Privacy Impact Assessment for the VA IT System called:

Education LAN Applications (ELA)

Veterans Benefits Administration (VBA)

Program Office: Education Veteran Readiness and Employment

Date PIA submitted for review:

August 22, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Bertha L. Brown	Bertha.brown@va.gov	(202) 461-9740
Information System Security Officer (ISSO)	Mark Ingold	Mark.ingold@va.gov	(918) 781-7520
Information System Owner	Timothy Allgeier	Timothy.allgeier@va.gov	(708) 483-5247

Abstract

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

Education LAN Applications (ELA) provides financial assistance for education, training, certification, etc. in the form of monthly benefit payments to veterans, active-duty service persons, reservists, and eligible dependents of disabled or deceased veterans.

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.

Education LAN Applications (ELA) is owned by the Department of Veterans Affairs, Veterans Benefits Administration and is located at the Hines Information Technology Center (HITC) in Chicago, Illinois.

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

The purpose of ELA is to provide financial assistance for education, training, certification, etc. in the form of monthly benefit payments to veterans, active duty services persons, reservists, and eligible dependents of disabled or deceased veterans.

C. Indicate the ownership or control of the IT system or project.

ELA is VA-owned and 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 75,000 with the data stored at the Buffalo and Muskogee Regional Processing Offices (RPOs), and the HITC.

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

The ELA boundary houses The Image Management System (TIMS) which houses general information such as name and personal contact information, service information, education information, and benefit information. TIMS contains claim folders and provides electronic storage, retrieval, and workflow processing for all VA education benefit claims (Chapters 30, 31, 32, 33, 34, 35, 1606, 1607 Work Study, On the Job Training and Veterans Retraining Assistance Program).

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

TIMS shares information with the following internal VA systems: The Digital GI Bill (DGI), Web Automated Verification of Enrollment (WAVE), Vets.gov, Enrollment Certification Automated Processing (eCAP), Performance Analysis and Integrity (PA&I), Benefits Delivery Network (BDN), and Veterans Service Network (VET). These systems receive Name, SSN and other identifiers from Veterans to assist with verification purposes.

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.

ELA is housed at the Hines Information Technology Center and operated in the Buffalo and Muskogee Regional Processing Offices. PII is maintained consistently in both sites, and the same controls are used. The system makes use of an encrypted Oracle database, uses SSH for communication, and is internal to the VA.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.
(https://www.oprm.va.gov/privacy/systems_of_records.aspx)

The legal authority for ELA is Title 10 United States Code (U.S.C.) chapters 106a, 510, 1606, and 1607, and Title 38, U.S.C. section 501(a), and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55, as well as SORN: System of Records 58VA21/22/28 – Compensation, Pension, Education, and Rehabilitation Records – VA.

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

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

There are no modifications taking place that would require an amendment to the SORN.

D. System Changes

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

Completion of this PIA will not result in circumstances that require changes to the business processes.

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

Completion of this PIA will not result in technology changes.

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)

ELA also collects Service information, Education information, and Benefit information.

PII Mapping of Components (Servers/Database)

Education LAN Applications (ELA) consists of three key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Education LAN Applications (ELA) 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. The first table of 3.9 in the PTA should be used to answer this question.

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
Office of Equipment Management (OEM)	**Yes**	**Yes**	**Full Name, SSN**	To identify the proper individual that is going to receive the benefit	TIMS has an encrypted Oracle database, uses SSH for communication, and is internal to the VA.
Buffalo	**Yes**	**Yes**	**Full Name, SSN**	To identify the proper individual that is going to receive the benefit	TIMS has an encrypted Oracle database, uses SSH for communication, and is internal to the VA.
Muskogee	**Yes**	**Yes**	**Full Name, SSN**	To identify the proper individual that is	TIMS has an encrypted Oracle

				going to receive the benefit	database, uses SSH for communication, and is internal to the VA.

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?

The Veteran or eligible dependent provides the information identified in Section 1.1 when applying for educational benefits via the VBA Education Benefits Website (http://www.benefits.va.gov/gibill/apply.asp), in person at a VA Regional Office, or via telephone at 1-888-442-4551.

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.

ELA does not require information from sources other than the individual.

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

ELA does not create information.

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?

There are many forms used by Veterans to apply for and/or make adjustments to pending benefits. All VBA forms are located at http://www.va.gov/vaforms/. The URL of the associated privacy statement is http://www.va.gov/privacy/. Veterans can also apply for Education Benefits at http://www.benefits.va.gov/gibill/apply.asp. Information can also be collected verbally from the

Veteran. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury.

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 are completed and submitted online and are not subject to the Paperwork Reduction Act.

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.

The information is verified by the Veteran when he/she is contacted regarding the Education Benefits application. Some of the information can be verified from other VBA systems such as eBenefits, Digital GI Bill (DGI), and Benefits Delivery Network (BDN) if the Veteran is receiving VBA benefits. The information is not checked for accuracy on regular intervals once it has been initially verified as the information collected typically does not change. However, any time the Veteran has to be contacted regarding the Education Benefits application, all of his/her information will once again be verified. Additionally, if any information for the Veterans does change, he/she may initiate an update via internal VA electronic 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.

The system does not access a commercial aggregator of information.

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 legal authority for ELA is Title 10 United States Code (U.S.C.) chapters 106a, 510, 1606, and 1607, and Title 38, U.S.C. section 501(a), and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55, as well as SORN: System of Records 58VA21/22/28 – Compensation, Pension, Education, and Rehabilitation Records – VA.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Personally Identifiable Information such as name and SSN may be release to unauthorized individuals.

Mitigation:

- ELA 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.
- VA Regional Loan Center (RLC) staff and VBA VACO Monitoring Unit staff also conduct audits of the lenders loan files (which included auditing funding fee information) as part of ongoing lender and RLC quality audits.

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.

- Name: Used to identify and track individual(s) in VA systems
- SSN: Used to identify and track individual(s) in VA systems
- Mailing Address: Used to identify and track individual(s) in VA systems
- Phone Number: Used to identify and track individual(s) in VA systems
- Email Address: Used to identify and track individual(s) in VA systems
- Service Information: Used to determine benefit eligibility
- Education Information: Used to determine benefit eligibility
- Benefit Information: Used to determine benefit eligibility

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

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

The system does not conduct analysis. There are no tools used to analyze the data. The data is compared to previous elements to ensure the correct record and submitted by the proper person.

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

individual? If so, explain fully under which circumstances and by whom that information will be used.

The system does not create or make available any new or previously unutilized information about an individual.

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?

ELA utilizes SSH File Transfer Protocol (SFTP) to transfer data via encrypted tunnels. When data is at rest, it is protected by being stored on encrypted volumes.

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

SSNs and other data are protected through assigned user roles, responsibilities, and need-to-know designation.

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

ELA runs on a least-privilege model, and only users of the system with a need-to-know will have access. Users login using Security Assertion Markup Language (SAML). There are no login IDs or passwords.

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?

Access to PII is granted on a need-to-know basis for individuals filling a role to assist veterans and eligible dependents with gaining access to benefits. It is also dependent on individual completing all required trainings.

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

Yes, all employees with access to Veterans' information must complete the mandatory VA Privacy and Information Security Awareness training and Rules of Behavior. At the end of this course, users read and attest they understand the VA Rules of Behavior. This course is required upon new employment and annually thereafter.

2.4c Does access require manager approval?

Yes, as PII is accessed within ELA, manager approval is required to gain access to the system.

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

Yes, users are required to use PIV credentials to log into the system, and their actions within the system are documented in system logs which can be reviewed as needed.

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

ELA users are responsible for assuring safeguards for PII as noted in the training they are required to take. Failure to do so could result in disciplinary actions, such as counseling, loss or access, suspension, or termination. Additionally, ELA limits users (based on roles) to only access information that is required to perform their jobs.

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*

ELA retains name and SSN as database tables. Additionally, ELA stores full name, full SSN, mailing address, phone number, email address, service information, education information, and benefit information in an imaging file.

3.2 How long is information retained?

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

The information is retained following the policies and schedules of VA's Records Management Service and NARA. Records are retained for 7 years.

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. This is detailed in 3.3b.

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

ELA follows the Records Control Schedule VB-1 Part 1, Section XIII, Veterans Benefits Administration Records Management, Records Control Schedule VB-1 Part 1 Section VII as approved 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.

Records/digital information will be eliminated following the sanitization procedures in VA 6300 Records and Information Management and VA 6500.1 Electronic Media Sanitization. Paper records are destroyed on-site weekly. Paper records are shredded using an approved National Security Agency (NSA) High Security Crosscut Shredder from the NSA High Security Crosscut Shredder List.

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.

All data is stored in encrypted tablespace and is redacted in lower environments. PII is not used for any testing, training, or research.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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:

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

<u>Principle of Data Quality and Integrity:</u> 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: There is a risk that the information contained in the system will be retained for longer that is necessary to fulfill the VA mission.

Mitigation: Paper records are shredded weekly. To mitigate the risk posed by information retention, ELA adheres to VBA Records Management Records Control Schedule VB-1 Part 1 for each category of data it maintains.

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***
Digital GI Bill (DGI)	Document, verify and update Veteran information	Name and SSN	Internal VA electronic transmission
Web Automated Verification of Enrollment (WAVE)	Document, verify and update Veteran information	Name and SSN	Internal VA electronic transmission
Vets.gov	Document, verify and update Veteran information	Name and SSN	Internal VA electronic transmission
Enrollment Certification Automated Processing (eCAP)	Document, verify and update Veteran information	Name, SSN, Mailing Address, File Number, Email Address	Internal VA electronic transmission
Performance Analysis and Integrity	Document, verify and update Veteran information	Name and SSN	Internal VA electronic transmission
Benefits Delivery Network (BDN)	Document, verify and update Veteran information	Name, SSN, File Number, Mailing Address	Internal VA electronic transmission
Veterans Service Network (VET)	Document, verify and update Veteran information	Name, Mailing Address, DoB, SSN, Phone Number	Internal VA electronic transmission

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: Privacy information may be released to unauthorized individuals.

Mitigation:

• All personnel with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

• ELA adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).

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

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

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

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

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

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

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

Data Shared with External Organizations

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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: If ELA communicated with external partners, there would be a risk that data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification and authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, and planning and maintenance.

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.

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 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.

Notice can be found here: https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf

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?

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.

Yes, Veterans have the right to refuse to disclose their information to VBA. The individual shall not be denied any right, benefit, or privilege provided by law because of the refusal to disclose to VBA an SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(a)).

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.

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 information is only access when requested by the Veteran. While individuals may have the ability to consent to various uses of their information at the VA, they must consent to the use of their information to determine eligibility and entitlement for VA compensation and pension benefits proceedings. The Privacy Act and VA policy require that PII only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

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: Privacy information may be collected prior to providing the written notice.

Mitigation: The VA mitigates this risk by providing Veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. The three main forms of notice are discussed in detail in question 6.1 and include the Privacy Act statement, a System of Record Notice, and the publishing of this Privacy Impact Assessment. The VA also mitigates this risk by providing the public with one form of notice that the Education LAN Application exists through the Privacy Impact Assessment (PIA) which is posted for public access.

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).

ELA 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.

ELA is a Privacy Act system and follows the procedures detailed in 7.1a.

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.

1. An individual may request amendment of a record pertaining to him/her contained in a specific VA system of record by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the requirements in paragraph 3b (3) of the handbook. It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requestor should be advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired.

2. Not later the 10 days, excluding Saturdays, Sundays, and legal public holidays, after the date of the receipt of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a determination has not been made, the acknowledgement will inform the individual when he/she may expect to be advised of action taken on the request. VA will

complete a review of the request to amend or correct a record as soon as reasonably possible, normally within 30 days form receipt of the request (excluding Saturdays, Sundays, and legal public holidays).

3. Where VA agrees with the individual's request to amend his/her record(s), the requirements of 5 U.S.C. 552a(d) will be followed. The records(s) will be corrected promptly, and the individual will be advised promptly of the correction. Amendment consists of adding information to the record, altering information in the record, or deleting information in the record. Under the Privacy Act, if information is altered or deleted, the previous version must be obliterated and illegible after amendment. The amendment should be annotated "Amended, Privacy Act, (date), (signature and title of amending official)."

4. If the record has previously been disclosed to any person or agency, and an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. An approved VA notification of amendment form letter may be used for this purpose.

5. If it is determined not to grant all or any portion of the request to amend a record, the official will promptly notify the individual in writing. The individual will be advised of his/her right to file a concise statement of reasons for disagreeing with the refusal to amend. The notice will specify the reason(s) for denying the request, identify the VA regulations or statutes upon which the denial is based, and advise that the denial may be appealed in writing to the General Counsel (024), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington DC, 20420. An approved VA notification of refusal to amend form letter may be used for this purpose.

6. The determination on an appeal will be made not later than 30 days, excluding Saturdays, Sundays, and legal public holidays, from the date the individual's letter of appeal is received unless the Secretary or Deputy Secretary, for good cause shown, extends such 30-day period. If the 30-day period is so extended, the individual will be notified promptly of the reasons for the extension and the date on which a final determination may be expected. The final determination in such appeals will be made by the General Counsel or Deputy General Counsel.

7. If the General Counsel or Deputy General Counsel finds that the adverse determination should be reversed, he/she will notify the VA office or station of the remedial action to be taken. The VA office or station will promptly carry out that action. The General Counsel or Deputy General Counsel will promptly notify the individual in writing of the corrective action. The field station or Central Office organization that provided the initial decision will inform previous recipients of the record that a correction has been made.

8. If the General Counsel or Deputy General Counsel determines that the adverse determination will not be reversed, the individual will be notified promptly in writing of that decision, the reasons therefor, and of his/her right to see judicial review of the decision pursuant to section 3 of the Privacy Act (5 U.S.C 552a(g)).

9. If the adverse determination is sustained by the General Counsel or Deputy General Counsel, the individual will also be advised promptly of his/her right to file a concise statement of reason for

disagreeing with the refusal to amend. The statement may contain information that the individual believes should be substituted.

10. When an individual files a statement disagreeing with VA's decision not to amend a record, the record will be clearly annotated so that the fact that the record is disputed is apparent to anyone who may subsequently access, use, or disclose it. When the disputed record is disclosed to persons or other agencies, the fact of the dispute will be clearly noted. Copies of the statement of disagreement will be provided, and, when appropriate, copies of a concise statement of VA's reasons for not making the amendment(s) requested will also be provided.

11. A decision by either the General Counsel or Deputy General Counsel pursuant to paragraph 3f(7) of the handbook is final. It is subject to judicial review in the district court of the United States in which the complainant resides, or has his/her principal place of business, or in which the VA records are located, or in the District of Columbia.

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.

Veterans and other beneficiaries are notified of the procedures for correcting their records is outlined in this PIA and VA SORN 58VA21/22/28 Compensation, Pension, Education and Vocational Rehabilitation and Employment Records, which states: "Records Access Procedures: Individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA Regional Office.

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

Mitigation: The privacy risk is mitigated by information provided by VA SORN 58VA21/22/28 – Compensation, Pension, Education and Vocational Rehabilitation and Employment Records 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.

Physical and logical access is limited to those individuals who have a need to access the information and who have completed the security requirements. This includes a correct level background investigation and US citizenship. Physical access controls include security guards, keycard locked doors, and closed-circuit television monitoring. Logical access is enforced by PIV authentication; authorization levels are assigned based on roles. These authorization levels employ the best practices of least privilege and separation of duties.

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?

Non-VA users do not have access to ELA.

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.

Role	**Access Level**
Windows System Administrator	Administrator
Linux System Administrator	Root/Administrator
Database Administrator	Database Administrator
Software Developer	User
Quality Assurance	User

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.

Contractors may have roles such as Database Administrator or System Architect. All PII is encrypted and requires encryption keys for direct access. Contracts are reviewed monthly and at the end of the Period of Performance (POP) by the Program Manager (PM) and Contracting Officer's Representative (COR). Contractors require a High/Tier 4 clearance. A Tier 4/Background Investigation (BI) is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

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 who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA 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 ELA user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:

- VA 10176: Privacy and Information Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics Training

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:* 19-May-2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 16-Jul-2023
5. *The Authorization Termination Date:* 28-Jun-2025
6. *The Risk Review Completion Date:* 31-May-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

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

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

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

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

There is no cloud technology being used in the ELA environment.

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).

ELA does not utilize Robotics Process Automation.

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

ID	Privacy Controls
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.

BERTHA BROWN Digitally signed by BERTHA BROWN
Date: 2023.08.29 11:19:10 -04'00'

Privacy Officer,

Mark L. Ingold 187982 Digitally signed by Mark L. Ingold 187982
Date: 2023.08.30 08:55:08 -05'00'

Information System Security Officer,

Timothy M. Allgeier 264256 Digitally signed by Timothy M. Allgeier 264256
Date: 2023.08.29 10:57:17 -05'00'

Information System Owner,

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).

The notice or verbiage referred to in Section 6 can be found here.

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