



Privacy Impact Assessment for the VA IT System called:

**Salesforce-Education Development  
Management System (EDMS)  
Education Service  
Veterans Benefits Administration (VBA)**

Date PIA submitted for review:

04/19/2023

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)	James Boring	James.Boring@va.gov	215-852-2000 ext 46
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	202-461-8484

## Abstract

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

Salesforce - Education Development Management Systems (EDMS) is a national database for tracking and managing Education Service requests to DOD for additional information in support of eligibility and education claims decisions. EDMS provides a standardized method for capturing and reporting the status of information requests sent to DOD. DOD users have authenticated access via CAC card and now respond directly to the request within Salesforce.

EDMS is tracking tool for “requests presented to the DoD, it is a standalone database for tracking status of the requests. When the requested information has been received, the VA user captures it to “The Image Management System” (TIMS).

## 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 Development Management System (EDMS) owned by Education Services

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

The information is collected to address claims under Section 38 USC Ch 33 - Post 9/11 Educational Assistance Program. All Veterans Claims Examiners are required to use EDMS to request information from DoD service components. DoD users log in and respond within the application to eliminate PII exposure via email. VA utilizes the information provided to complete processing the education benefit claims.

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

EDMS is a VA/VBA owned, Salesforce controlled application built on Salesforce Government Cloud Plus (SFGCP) for VA Education Service Division.

### 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.*

Each client is either a Veteran or a beneficiary, therefore there is a potential of up to 2 social security numbers (SSNs) associated to each record. As of the January 2023, EDMS has been in use for 5 years and 3 months. During the window of activity, we have generated 120,582 requests or records, 105,548 have one SSN, the remaining 15,034 have two SSN associated with the request. We average 1,914 requests from per month and expect the trend to continue until

VA and Department of Defense improve the quality of information sharing required to establish Education eligibility for Veteran or beneficiaries applying for education benefits.

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

EDMS began as a way of electronically tracking and managing the email requests submitted to the Department of Defense (DOD) relating to service dates required to establish eligibility for education benefits. In FY22, our DOD partners (service components) began logging into Salesforce using their CAC cards to review and respond to VA inquires. This has eliminated the need for any email correspondence containing PII.

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

No information sharing.

*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 system operates on one site which is accessed only by VA Employee users and DOD users that have access to EDMS via PIV or CAC card single sign on access.

### *3. Legal Authority and SORN*

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

Department of Veterans Affairs, Privacy Act of 1974; System of Records “Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA (58/VA21/22/28)

Link: <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?*

The Salesforce – Education Development Management System (EDMS) is currently in sustainment; it is not being modified.

### *D. System Changes*

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

DoD users are now set up as authenticated users with CAC cards logging into Salesforce Community. The Business process improvement eliminates risk of exposure of PII by eliminating email inquiries and responses.

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

No changes are required.

## 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://vawww.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:

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

No Additional Information Collected.

## PII Mapping of Components (Servers/Database)

Salesforce – Education Development Management System does not connect with other databases.

**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*

<b>Database Name of the information system collecting/storing PII</b>	<b>Does this system collect PII? (Yes/No)</b>	<b>Does this system store PII? (Yes/No)</b>	<b>Type of PII (SSN, DOB, etc.)</b>	<b>Reason for Collection/ Storage of PII</b>	<b>Safeguards</b>
NA	NA	NA	NA	NA	NA

### **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?*

VA Veterans Claims Examiner enters the information

*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.*

VA user must have validated service data to establish eligibility. If the information is not provided by the claimant or available in other VA systems, the VA user will request claimant specific service data from the applicable service component to expedite the claim.

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

The system does not create a score, analysis or report.

### **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?*

On an as-needed basis. When there is an Education claim that requires additional development to DoD components, VA employees use the EDMS module.

*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.*

Information is not collected on a form.

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

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

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

The information is collected to address claims under Section 38 USC Ch 33 - Post 9/11 Educational Assistance Program. All DoD users are required to use EDMS to provide military service information so that VA requests are tracked and addressed in timely manner.

*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.*

VA users are responsible for entering the correct information. Salesforce is not validating claimant SSN or other details for accuracy.

#### **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*

Authority to collect and maintain the information is found in 38 USC Ch 33 - Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. § 501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.

### **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:** The internal VA Education Service users collect and enter Personally Identifiable Information (PII) to address Education benefits eligibility. The DoD user provide military service dates to ensure Veterans receive the appropriate benefits they are entitled. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

**Mitigation:** The data is secured in Salesforce Shield which utilizes FIPS 140-2 encrypted connection. Only authorized internal VA users and DoD users login via single sign on to the application.

## 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 information is collected to address claims under Section 38 USC Ch 33 - Post 9/11 Educational Assistance Program. All external users are required to use EDMS to provide required details for VA to complete processing the education benefit claim.

### **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 data is not used for any other analytical purposes. The data is used to process education claims in a timely manner.

*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 data is not used for any other analytical purposes. The data is used to process education claims in a timely manner.

### **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?*



The application utilizes Salesforce Shield protect adhering to FIPS 140-2 encrypted connection protects data at rest. SSN are encrypted within Salesforce. Data is not in transit.

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

Sames as above, encryption within Salesforce

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

Users accessing Salesforce Application must be Authenticated during login and granted access based on role.

## **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 fields storing PII information is determined by the Role the user is setup in module. User Roles based on the job function determines the access to PII. Once Business owner who is a VA Program Manager approves the user to access the system in a certain role that grants required Permissions to module. The module is configured with various Permission setting that decides who can access what. These settings are documented in Technical Design document which is reviewed by Digital Transformation Center (DTC). Business owner is responsible for requesting User Step based on the Role the User will be playing in the module. If there are any changes to Role (resource movement), Business reaches out to DTC to remove access for that specific user by submitting a User access request. Business Owner monitors all Users to ensure they have access only to what they are supposed to have. Business owner is responsible for safeguarding PII by utilizing features Salesforce provides – Permission sets and User activity logs.

-

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

Yes, all requests for access to Salesforce are submitted by Management, Approved by System Administrator and completed by governing help desk, Digital Transformation Center Contractor.

2.4c Does access require manager approval?

Yes, a member of management must request access to the application for new or reactivation of accounts disabled due to inactivity of 90 days.

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

All electronic records with PII are stored within Salesforce for authorized users. All workflows are completely electronic.

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

Salesforce Encryption has been established and maintained since inception of the application.

## 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*

Retention policy applicable to VA's Salesforce platform is applicable for this module, Name and SSN noted in 1.1 is retained.

### 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 schedules of VA's "Records Control Schedule VB-1 Part II, Central Office" found at the following link:

[https://www.benefits.va.gov/warms/docs/regs/rcs\\_ii.doc](https://www.benefits.va.gov/warms/docs/regs/rcs_ii.doc)

The SORN provides the retention/destruction times set forth in the VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII, as authorized by NARA.

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

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

*This question is related to privacy control DM-2, Data Retention and Disposal.*

*3.3a Are all records stored within the system of record indicated on an approved disposition authority?*

The retention schedule for the Salesforce Government Cloud Plus (SFGCP) is also applied to CCQMS application. SFGCP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFGCP records are retained according to [VBA Records Control Schedule, VB-1, Part II](#) & [VBA Records Control Schedule, VB-1, Part I](#).

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

VBA records are governed by Records Control Schedule (RCS) VB-1, Part II Revised for VBA <http://www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/VB-1PartII.doc> and by Records Control Schedule (RCS) VB-1, Part I <http://www.benefits.va.gov/WARMS/docs/admin20/rcs/part1/VB-1Part-I.doc>

Public Customer Service Operations Records, Item number: 1925.1. Disposition Authority, GRS 6.5, item 020. DAA-GRS-2017-0002-0001 ([Records Control Schedule 10-1 \(va.gov\)](#))

### **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 moved to another backup server post retention period. VA's Salesforce Platform policy for data backup is applicable for this module.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. [https://www.va.gov/vapubs/search\\_action.cfm?dType=1](https://www.va.gov/vapubs/search_action.cfm?dType=1)

### **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.*

No training or testing is conducted using PII data.

### **3.6 PRIVACY IMPACT ASSESSMENT: Retention of information**

*Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System 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:** Depending on the retention time, PII and sensitive information of the individual is at risk of exposure to unauthorized individuals. The information retained by the system is stored for adjudication of eligibility for Education Benefits.

**Mitigation:** All data at rest in Salesforce platform is encrypted with Salesforce Shield which utilizes FIPS 140-2, in addition to being protected by FedRAMP security controls under the FedRAMP ATO.

## **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.*

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
Veteran Benefits Administration – The Image Management System (TIMS).	The receipt is sent to TIMS so that the information related to the Veteran claiming Education benefits is saved.	TIMS File Claimant Last Name TIMS File Claimant Full Name TIMS File Claimant SSN TIMS File Veteran SSN Veteran First Name Veteran Middle Name Veteran Last Name Veteran Full Name Veteran SSN	User choses to capture screenshot of EDMS data into TIMS by user of button that “prints page to pdf and then the pdf is manually saved to TIMS.

**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:** There is a risk of information may be shared with unauthorized VA personnel.

**Mitigation:** Safeguards are implemented including assignment of appropriate User Roles and Module access settings in Salesforce (Automated Controls) and Operational Processes (Manual Controls). All VA users must login using PIV or CAC cards, EDMS PII is encrypted and the platform is protected with Salesforce Shield. Users access data on need-to-know-basis.

**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*

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

## **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.

**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.*

Veterans and/or beneficiaries applying for Education benefits must complete an application, VA FORM 22-1990, MAR 2023. The aforementioned form includes the following 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

Version Date: October 1, 2022

**Page 16 of 30**



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 Veteran Readiness and Employment Records - VA, published in the Federal Register. Your response 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. VA FORM 22-1990, MAR 2023 (B) If you haven't selected a school or training establishment: Step 1: Mail the completed application to the VA Regional Processing Office for the state or region of your home address. See the addresses below for VA Regional Processing Offices. Step 2: Wait for VA to process your application and notify you of its decision concerning your eligibility for education benefits. Respondent Burden: We need this information to determine your eligibility for education benefits (38 U.S.C. 3471). Title 38, United States Code, allows us to ask for this information. We estimate that you will need an average of 15 minutes to review the instructions, find the information, and complete this form. VA cannot conduct or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed. Valid OMB control numbers can be located on the OMB Internet Page at [www.reginfo.gov/public/do/PRAMain](http://www.reginfo.gov/public/do/PRAMain). If desired, you can call 1-800-827-1000 to get information on where to send comments or suggestions about this form. The Harry W. Colmery Veterans Educational Assistance Act of 2017 (Public Law 115-48), also known as the "Forever GI Bill," requires the Department of Veterans Affairs (VA) to make available to educational institutions information about the amount of educational assistance to which a veteran or other eligible individual is entitled. If you are eligible for the post-9/11 GI Bill (Chapter 33), Montgomery GI Bill-Active Duty (Chapter 30), Montgomery GI Bill - Selected Reserve (Chapter 1606), or the Survivors' and Dependents Educational Assistance Program (DEA) (Chapter 35), you may elect to "opt-out" of these disclosures and have VA withhold this information instead. To request an opt-out, or for information about how to opt-out, please refer to our website at [va.gov](http://va.gov), or click <https://www.va.gov/find-forms/> to complete the VA Form 22-0993, Request to Opt-Out of Information Sharing with Educational Institutions. REQUEST TO OPT OUT OF INFORMATION SHARING WITH EDUCATIONAL INSTITUTIONS WV WY APO / FPO AA FOREIGN SCHOOLS US VIRGIN ISLANDS NJ NY OH PA RI SD TN VA VT WI MD ME MI MN MO MT NC ND NE NH CO CT DC DE IA IL IN KS KY MA SERVES THE FOLLOWING STATES Eastern Region: VA Regional Office P.O. Box 4616 Buffalo, NY 14240-4616 APO / FPO AP GUAM PHILIPPINES MARIANA ISLANDS MS NM NV OK OR PR SC TX UT WA AK AL AR AZ CA FL GA HI ID LA SERVES THE FOLLOWING STATES Western Region: VA Regional Office P.O. Box 8888 Muskogee, OK 74402-8888 AMERICAN SAMOA PAGE

*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.*

All Veterans and/or beneficiaries applying for Education benefits must complete an application, VA FORM 22-1990, MAR 2023, a Privacy Notice which informs information that will be collected to process their benefits. Screenshot for the privacy notice is attached in Appendix section or connect to the VA Form at the following link:

<https://www.vba.va.gov/pubs/forms/VBA-22-1990-ARE.pdf>

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

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

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.*

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:** EDMS is a secondary application, so the user is not directly aware of the internal system to request DoD information. The risk is associated with the Veteran is not aware of the internal application.

**Mitigation:** The Veteran consents to the user of their information by applying for Education benefits, basic PII is a part of the data collection on the application.

## **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 request for access must be delivered to and reviewed by the System Manager for concerned VBA system records, Regional Office Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access is 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).*

The application is not exempt from 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.*

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.*

The Privacy Act of 1974 affords Veterans the right to amend their records by submitting their request in writing. The request must be in writing and adequately describes 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 outline in this PIA, and SORN 58 VA21/22/28. 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 ensure 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.*

As a part of the onboarding process, after the User is set up in the Active Directory, the Supervisor submits a request to the Education Service Operations team. They review, validate and prepare the appropriate request with the DTC helpdesk, the team managing Salesforce Platform access. DTC reviews the details and grants appropriate access (ensuring the users are granted only the lowest privilege(s) needed to use EDMS).

*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?*

Currently, we have approximately 40 Department of Defense employees logging in as authenticated users (using CAC card). They have read only access to PII, the DoD user reviews their systems and respond to the request for information directly in Salesforce. The DOD users do not have access to reporting functions in Salesforce.

*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.*

VA internal users are granted read/write access to data within Salesforce. DOD users have read only access to the Salesforce data and may contribute information in a read/write section of the application.

### **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.*

The development of the application was completed under the COE contract, Office of Business Integration (OBI) were the COR. The application is now in sustainment under O&M contract with Accenture Federal Service (AFS). AFS only access the application when logging in as authenticated users.

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 system 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 ECC 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 acknowledgement is tracked through the TMS system. All VA employees and contractors must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:

- VA Privacy and Information Security Awareness and Rules of Behavior
- Privacy and Health Insurance Portability and Accountability Act (HIPPA)

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

**Yes**

*8.4a If Yes, provide:*

1. *The Security Plan Status:* Approved
2. *System Security Plan Status Date:* March 15, 2023
3. *The Authorization Status:* ATO
4. *The Authorization Date:* January 20, 2022
5. *The Authorization Termination Date:* December 17, 2023
6. *The Risk Review Completion Date:* January 20, 2022

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 (ITMAaaS). 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)

Government Cloud, Provider - Salesforce Government Cloud

### 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.

Service Provider: Contract entitled: “Salesforce Subscription Licenses, Maintenance and Support”, Contract Number: NNG15SD27B, Order Number: 36C10B9F0460

### 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.*

Yes, VA has full ownership of the ancillary data stored in the system.

**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.*

The cloud service provider does not collect ancillary data.

**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).*

The system does not utilize RPA

## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

<b>ID</b>	<b>Privacy Controls</b>
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>

<b>ID</b>	<b>Privacy Controls</b>
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

**Signature of Responsible Officials**

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

---

**Privacy Officer, Bertha L. Brown**

---

**Information Systems Security Officer, James Boring**

---

**Information Systems Owner, Michael Domanski**

## **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).

Department of Veterans Affairs, Privacy Act of 1974; System of Records "Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA (58/VA21/22/28)

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

Document Link: <https://www.vba.va.gov/pubs/forms/VBA-22-1990-ARE.pdf>

## **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](#)