Privacy Impact Assessment for the VA IT System called:

Benefits Delivery Network (BDN)

Veterans Benefits Administration (VBA)

Office Of Business Integration

Date PIA submitted for review:

01/20/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jean-Claude Wicks	jean-claude.wicks@va.gov	(202) 502-0084
Information System Security Officer (ISSO)	Pedro Epting	*Pedro.epting@va.gov*	*708) 483-5096*
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.

Benefits Delivery Network (BDN) provides benefits and services to eligible Veterans, dependents, and beneficiaries. VBA uses BDN to process entitlements primarily for Education Service. BDN provides a supporting role for the Compensation Service and Pension and Fiduciary Service business lines.

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.

Benefits Delivery Network (BDN) and Veterans Benefits Administration owns the system

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

Benefits Delivery Network (BDN) provides benefits and services to eligible Veterans, dependents, and beneficiaries.

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

Veterans Benefits Administration

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.

Over a million records. These are veterans and their dependents for education benefit claim

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

Additionally, users leverage BDN to identify claimants, track claims, view records, process claims and generate computer letters for development, award, payment, and disallowance.

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

The VA Online Certification of Enrollment (VA-ONCE), Web Automated Verification of Enrollment (WAVE), Web Enabled Approval Management System (WEAMS) these applications provide the BDN system with data needed to process claims such as name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s), Email Address

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 information system has it disaster recovery site at the Philadelphia ITC. Data is used only when there a disaster recovery exercise is conducted.

3. Legal Authority and SORN

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

58VA21/22/28 80 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA: https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.

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?*

No

D. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

1.1 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)

Additional information collected is file number, family/dependents, marital status, and Veteran DD-214 service data to include the military personnel profile, component, service tours, rank, combat pay indicator(s), school information and character of discharge, School Information.VA Claim Number VA Claim Number, Payment Income Verification Matching Veterans disability ratings, Paid benefits, Military Branch and Service, Pension, Education and Burial Benefits, SSN's, BOP Inmate Central Records, Employment, and Education information, Veteran Rating information, Eligibility, Entitlement, Award data, VA Form 22-1999, VA Form 22-1111b WAVE, School Name, School Code, Enrollment Period Facility Code, Facility Names.

PII Mapping of Components (Servers/Database)

BDN consists of 1 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Benefits Delivery Network 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**
Corporate Database	Yes	Yes	Name, SSN, DOB	To identify individuals	Access Management, Least Privilege, Need to Know

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?

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.

The VA Online Certification of Enrollment (VA-ONCE) – a single system that allows school officials to enter enrollment and related information and transmits this information via secure Internet protocols or File Transfer Protocol (FTP).• Web Automated Verification of Enrollment (WAVE) – internet application allowing students to electronically complete and transfer monthly verifications of enrollment and student status changes to Education Regional Processing Offices to release monthly payments. Students can also submit changes of address and Direct Deposit information via this system in a secure environment using Secure Socket Layer (SSL).• Web Enabled Approval Management System (WEAMS) – repository of approved institutions, organizations, and training establishments for claimants receiving education benefits. Claims examiners use WEAMS to determine what institutions, organizations, and training establishments are approved. Data such as facility code and facility name for each institution, organization, and training establishment are captured in a batch mode and transferred into BDN

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

BDN does not create information but processes education claims

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?

BDN accepts claims from several sources including mail, fax, email, Vocational Rehabilitation and Employment (VR&E), and EDU Web Applications via the internet. Paper claims are also accepted. Documents are then scanned and stored into the appropriate Veteran's eFolder. The SPI information is collected via electronic transmissions from the master VBA repositories (Corporate and BDN Master Databases).

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.

BDN accepts claims from several sources including mail, fax, email, Vocational Rehabilitation and Employment (VR&E), and EDU Web Applications via the internet. Paper claims are also accepted. Documents are then scanned and stored into the appropriate Veteran's eFolder. The SPI information is collected via electronic transmissions from the master VBA repositories (Corporate and BDN Master Databases).

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.

BDN is hard coded to validate data for accuracy as it is entered. For example, when entering a social security number, BDN checks that 9 digits have been entered into the field. Additionally, data is checked for completeness by system audits, manual verifications, and annual questionnaires through automated Veteran letters. These letters ask specific questions for verification based on the existing entitlement or benefit the Veteran is receiving. The correspondence with each Veteran is then used to update the data. All collected data are matched against supporting claims documentation submitted by the Veteran, widow, or dependent. Certain data such as Social Security Number (SSN) is verified with the Social Security Administration. Prior to any award or entitlement authorization(s) by the VBA, the Veteran record is manually reviewed, and data validated to ensure correct entitlement has been approved.

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.

BDN does not access any 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

BDN operates under System of Record Notice (SORN) 58VA21/22/28; Title 10 U.S.C. chapters 106a, 510, 1606 and 1607; 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.

The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.

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: BDN collects SPI. If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offers assistance to the affected parties so that they may find the help they need to get through their crisis. Only authenticated users are permitted to have access to BDN and its resources. For BDN security administrators, the BDN supervisor or contract officer technical representative requests the administrative account that is established by the facility information security officer. BDN Section Chiefs review individual accounts to verify the access initially given is still required. Temporary and emergency accounts are not used within the BDN environment. User access is restricted to the minimum necessary to perform the job.

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 verify Veteran or subject's identification
Social Security Number: Used to verify Veteran or subject's identity
Date of Birth: Used to verify identity
Personal Mailing Address: Used for correspondence
Financial Account Information: Veteran or beneficiary's banking information
Marital Status: Used to determine rate of payment Veteran is eligible for
Family/Dependents: Relation to Veteran
Veteran DD-214 Data: Used to determine entitlement to benefits
File number, Family/dependents, Marital status, Veteran DD-214 Service data to include the military personnel profile, Component, Service tours, Rank, Combat pay indicator(s), School information and Character of discharge – Information collected are used to identify beneficiaries and process education claims.
School Information: Attendance verification
VA Claim Number: For identification
Payment: For money benefits
Income Verification Matching: to reconfirm claimant's identity
Veterans' disability ratings: Determines how of the benefits you deserve
Paid benefits: Monetary benefits for claimant
Military Branch and Service: Class of military service the veterans belongs to
Pension: The amount military pension
Education and Burial Benefits: The amount of money the veterans receive for education
BOP Inmate Central Records: Information from the Bureau of Prison if any
Employment and Education information: if the veteran is employed and the level of education
Veteran Rating information: The eligible or ineligible
Eligibility: Based on the percentage each veteran will receive
Entitlement: How many months of education can be claimed
Award data: The amount of money the veteran will receive
VA Form 22-1999: VA certified forms
School Name: Name of the school the veteran attends

School Code: Code number/ID of the school
Enrollment Period Facility Code: The semester in which veteran enrolled
Facility Names: the name associated with the facility code

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.

BDN processes entitlements primarily for the VBA Education Service business line, which is a collection of web-enabled applications delivering educational services. No data analysis tools are used within these applications.

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

BDN will update master record for each individual claim. The master record is maintained throughout the life of the claims.

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?

Secure File Transfer Protocol (SFTP), Electronic File Data is moved via Managed File Transfer and Encrypted data connection.

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

The information system only allows authorized person to view claimants' data

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

The BDN application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy and VA National Rules of Behavior in Talent Management System govern how Veterans' information is used, stored, and protected.

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?

The SORN defines the information collected from Veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a Veteran's burial and monument benefits.

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

The security controls for the BDN application cover 18 security areas with regards to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity

2.4c Does access require manager approval?

Yes

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

Yes

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

Hines Operations Center (HITC)

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*

Name, Social Security Number, Date of Birth, Personal Mailing Address, Financial Account Information, Marital Status, Family/Dependents, Veteran DD-214 Data

3.2 How long is information retained?

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

EDU Web Applications claim files are retained at the servicing regional office until they are inactive for three years. EDU files are transferred to the VA Records Management Center (RMC) in St. Louis, MO, for the life of the Veteran. At the death of the Veteran, these records are sent to a Federal Records Center (FRC), and maintained by the FRC for 60 years, and thereafter become the permanent possession of the National Archives and Record Administration (NARA) to be retained indefinitely as historical documents.

Education electronic file folders are retained at the servicing Regional Processing Office.

Employee productivity records are maintained for two years. File information for Credit Alert Interactive Voice Response System (CAIVRS) is provided to Department of Housing and Urban Development (HUD) by VA on magnetic tape. After information from the tapes has been read into the computer the tapes are returned to VA for updating. HUD does not keep separate copies of the tapes.

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?

Yes

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

The schedule is retained in accordance with the Records Control Schedules VB-1, Part 1, Section VII and XIII, approved by National Archives and Records Administration (NARA).

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

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.

Compensation, pension, and VR&E claim files are retained indefinitely as historical documents. Some claim file folders are electronically imaged, in which case the electronic file folder is maintained in the same manner as the claim file folder. Once a file is electronically imaged and established by VA as the official copy of record, its paper contents (with the exception of official legal documents, and service treatment records and other documents that are the property of DoD), are destroyed in accordance with Records Control Schedule VB–1 Part 1 Section XIII, as authorized by NARA.

Vocational Rehabilitation and Employment Counseling/Evaluation/Rehabilitation (CER) records, automated storage media containing temporary working information, and all other automated storage media are disposed of in accordance with disposition authorization approved by NARA. Education electronic file folders are destroyed in accordance with the times set forth in the VBA Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA.

Employee productivity records are destroyed by shredding or burning. The magnetic tapes sent to HUD for CAIVRS are returned to the VA and reused.

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.

BDN does not have PII/PHI/SPI in environments other than production. Live data is not used for testing or training purposes.

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: There is a risk that the information maintained by BDN could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, the BDN adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the VA will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information (SPI), which contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

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***
Benefits Identification Record	Cross reference for	Name, SSN, Dob, Mailing Address, Zip Code, Phone Number(s), Email Address	Secure File Transfer Protocol (SFTP)

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Locator System (BIRLS)	those with accounts for VA education benefits		
Common Security Services (CSS)	Authorization for various applications for education application processing	VA Claim Number	SFTP
Veterans Service Network (VETSNET	Cross reference for other VBA benefits	Name, SSN, DoB, Mailing Address, Phone Number(s), Email Address	Electronic File Data is moved via Managed File Transfer
VA DoD Identity Repository (VADIR)	The Veterans Affairs/Department of Defense Identity Repository VADIR) database is an electronic repository of military personnel's military history, payroll information and their dependents' data. The VADIR database repository is used in conjunction with Education applications to provide an electronic consolidated view of comprehensive eligibility and benefits utilization data from across VA and Department of Defense	Veteran DD-214	Encrypted data connection

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***
	(DoD). VA applications use the VADIR database to retrieve profile data, as well as address, military history, and information on benefits.		
EDU PITC Web Applications (EDU)	Education benefits entitlements	VA-ONCE: VA Form 22-1999, VA Form 22- 1999b WAVE: Name, Address, School Name, School Code, Enrollment Period WEAMS: Facility Code, Facility Names	SFTP

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining SPI is that sharing data within the Department of Veterans' Affairs could happen and the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

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

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

Defense Manpower Data Center	BDN system will match SSNs, and other data elements, with the SPAA's benefit information. DMDC will act as the intermediary in providing this matching information.	VA Claim Number	ISA/MOU	SFTP
Department of Treasury – Bureau of Fiscal Service	Two-way data exchange from BDN to Fiscal Service to send daily and monthly data files of payment information for Fiscal Service to disburse International Direct Deposit (IDD) payments.	VA Claim Number, Payment	ISA/MOU	VPN Tunnel using 3DES-encryption. Https (128-bit SSL)
Internal Revenue Service	Provides Compensation service and Pension & Fiduciary Service with and Electronic document management system designed to improve Veteran's Service representatives' access to claimant information.	Income Verification Matching (VETSNET/FAS function)	ISA/MOU	FIPS 140-2 Compliant VPN Tunnel (IPSEC) Tunnels

Social Security Administration	Transfers data about Veterans and their Beneficiaries who are receiving VA Benefits.	VETSNET & Death Alert Control and Update System (DACUS) share Veterans disability ratings, paid benefits, military branch and service, pension, education and burial benefits.	ISA/MOU	SFTP
Department of Justice (DOJ) - Federal Bureau of Prisons (BOP)	Matching of SSNs and other data elements from the BOP Inmate Central Records System against the “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” system of records.	SSN’s, BOP Inmate Central Records, Employment, and Education information.	ISA/MOU	VPN connection encrypted. Connect: Direct Secure Plus
BULL HN Information Systems Inc.	Mainframe computer system that contains ratings, eligibility, entitlement and award data for Veterans.	Veteran Rating information, Eligibility, Entitlement, and award data.	ISA/MOU	VPN Tunnel (IPSEC

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: The privacy risk associated with maintaining PII is that sharing data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by BDN personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system. Audit log for the BDN system will be maintained for authorization, authentication and regularly reviewed. Before sharing any information outside (external to VA) of the Department, Information Security Officer and Business Owner will validate and maintain all Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), contract, Computer Matching Agreement, legal binding agreement and SORN routine use, if applicable, that permit external sharing.

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.

The System of Record Notice (SORN) are as follows:
a. SORN 58VA21/22/28 "Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA.".

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

The Amended SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.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.

This Privacy Impact Assessment (PIA) also serves as notice. 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, or other means."

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.

Veteran and their family or guardian (spouse, children, parents, grandparents, etc.) may not decline or request that their information not be included as part of BDN to determine eligibility and entitlement for VA compensation and pension benefits and may also designate a guardian to manage the VA compensation and pension benefits.

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.

Individuals have the right to decline providing information to VA personnel. However, failure to provide needed information may result in denial of access to or delays in obtaining health care and other VA benefits. Veterans and their family or guardian (spouse, children, parents, grandparents, etc.) may not decline or request their information not be included to determine eligibility and entitlement for VA compensation and pension benefits and may also designate a guardian to manage the VA compensation and pension benefits.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that members of the public may not know that the BDN system exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists; the Privacy Impact Assessment and the System of Record Notice.

Section 7. Access, Redress, and Correction

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

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

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

*7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. **For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals wishing to obtain more information about access, redress and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records should contact the Department of Veteran's Affairs regional office as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment

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).

Individuals can request to his or her information pertaining to education claim at any Veterans Affairs regional office

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 system is a privacy act system.

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

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

If incorrect information was collected, then the education claim will be denied.

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 VA regional office will send denied mails to claimant.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1, as directed in the System of Record Notice (SORN)

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:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:

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

<u>Mitigation:</u> By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

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.

BDN depends on the Computer Access Request System (CARS) requirements to provide the standard for establishing and maintaining security profiles, permissions, applications, roles, and functions for OIT BDN administrators and developers. The purpose of CARS is to validate, coordinate, monitor, and restrict access to sensitive data. Only authenticated user IDs are permitted to have access to BDN and its resources. For BDN security administrators, the BDN supervisor or COR requests the administrative account that is established by the facility ISO. The CARS is used to request BDN administrative access.

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?

The Super Migration Gateway (SMGW) security administrator provides application level access to the Regional Offices (ROs). BDN Section Chiefs review individual accounts to verify the access initially given is still required. Temporary and emergency accounts are not used within the BDN environment. User access has been restricted (least privilege) to data files and processing capability (i.e., read, write, execute, delete) to the minimum necessary to perform the job.

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.

BDN security administrator and BDN regional office supervisor

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.

Yes, VA contractors can have access to BDN. VA contract employee access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

8.4a If Yes, provide:

1. *The Security Plan Status: Completed*
2. *The System Security Plan Status Date:* 3/14/2022
3. *The Authorization Status:* Full ATO
4. *The Authorization Date:* 2/18/2022
5. *The Authorization Termination Date:* 2/17/2025
6. *The Risk Review Completion Date:* 9/27/2022
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.***

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)*

No. BDN is a COBOL/Mainframe application and does use the 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.*

N/A

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**

ID	Privacy Controls
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

JEAN-CLAUDE WICKS

Digitally signed by JEAN-CLAUDE WICKS
Date: 2023.03.02 07:50:39 -07'00'

Privacy Officer, Jean-Claude Wicks

Thomas J. Orler 178546

Digitally signed by Thomas J. Orler 178546
Date: 2023.02.22 10:14:02 -06'00'

Information System Security Officer, Pedro Epting

Timothy M. Allgeier 264256

Digitally signed by Timothy M. Allgeier 264256
Date: 2023.02.22 09:15:55 -06'00'

Information System Owner, Timothy Allgeier

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).

System Of Records Notice:

58VA21/22/28 80 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

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

HELPFUL LINKS:

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