Privacy Impact Assessment for the VA IT System called:

Veterans Service Network (VETSNET)
Benefits and Memorials Program Management
Office Compensation and Pension Product Line

Date PIA submitted for review:
3/3/2022

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Tonya Facemire</td>
<td><a href="mailto:Tonya.Facemire@va.gov">Tonya.Facemire@va.gov</a></td>
<td>202-632-8423</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Richard Tercero</td>
<td><a href="mailto:Richard.Tercero@va.gov">Richard.Tercero@va.gov</a></td>
<td>310-882-1091</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Gary Dameron</td>
<td><a href="mailto:Gary.Dameron2@va.gov">Gary.Dameron2@va.gov</a></td>
<td>202-492-1441</td>
</tr>
</tbody>
</table>
Abstract

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

Veterans Service Network (VETSNET) is a suite of applications that reside within the Department of Veterans Affairs, Benefits Application Infrastructure (BAI) environment and facilitates the Compensation & Pension (C&P) claims process. The minor applications that makeup VETSNET work together to provide the capability for: establishing a veteran’s claim, developing the claim, rating the claim, preparing the award, and paying the veteran. Within the application suite, the end user can: establish and develop veteran claims. They first obtain the rating decision, then if awarded, the award and notification letter are documented, and then payment information is transmitted to the Department of Treasury - accomplishing the necessary accounting.

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:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- 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.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes.
- Whether the completion of this PIA could potentially result in technology changes.
- 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 cover cloud usage or storage?

Veterans Service Network (VETSNET) is owned by the Department of Veterans Affairs, Infrastructure Operations (IO) at the Austin Information Technology Center (AITC) in Austin, Texas.

VETSNET is a suite of applications (with about 4 million users) that facilitates the entire C&P claims process. Within the suite, the end user can establish and develop Veterans’ claims; the rating decision, award and notification letter are documented; and payment information is transmitted to
Treasury, accomplishing the necessary accounting. Throughout these activities, data is shared and passed between the applications to support end-to-end claims processing, customer service and notification.

VETSNET has replaced most of the C&P functions of the Benefits Delivery Network (BDN), which is currently in maintenance phase. Oversight for the VETSNET investment is provided by the VETSNET Executive Team. The Executive Team is an interdisciplinary team led by a Senior Executive well-versed in C&P processes. The team is responsible for the day to day execution of the project. VETSNET is a fundamental component of VA’s Enterprise Architecture in providing critical C&P informational support to its customers through an integrated and technologically sound environment.

The following minor applications* are components of VETSNET:

- SHARE
- Search Participant Profile (SPP)
- Modern Awards Processing Development (MAP-D)
- Compensation and Pension Awards
- Statement of the Case/Supplemental SOC (SOC/SSOC)
- Finance and Accounting System (FAS)
- Request for Name and Address

Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55 provide the legal authority for operating VETSNET. VA gathers or creates these records in order to enable it to administer statutory benefits programs to Veterans, Service members, reservists, and their spouses, surviving spouses, and dependents, who file claims for a wide variety of Federal Veteran’s benefits administered by VA. Information is collected from Veterans (Name, SSN, date of birth, mailing address, zip code, phone number, email address, emergency contact information, financial account information, health insurance beneficiary numbers, current medications, previous medical records, service number, rank, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, service period, whether Veteran was discharged with a disability, reenlisted, received a Purple Heart or other military decoration) to determine Veteran eligibility for Compensation and Pension benefits.

The VA’s Beneficiary Identification and Records Locator System (BIRLS), Benefits Delivery Network (BDN) and the VBA Corporate Databases (CRP) are also used to determine Veteran eligibility for Compensation and Pension benefits. Data input are also provided from the SSA for income verification, SSN match; SSA benefit information or death file notices; DoD (DFAS) data input, e.g. DD Form 214; and information from the Internal Revenue Service for income verification. Verification with Department of Treasury payment history files; returned checks; Defense Manpower Data Center for military reserve status, verification of active duty date; and monthly interfaces from DoD, DFAS, Coast Guard, and DHHS. Data inputs are provided from State National Guard and Reserve Units to determine eligibility for Veterans Benefits.

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 Account Information
- Health Insurance Beneficiary Numbers
- Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Gender
- Integration Control Number (ICN)
- Military History/Service Connection
- Next of Kin
- Other Unique Identifying Information (list below)

Total amount of Active Service, Rank, Branch of Service, Character of Service, Pay Grade, Assigned Separation Reason, Service Period, Birth Certificates, Marriage Licenses, whether Veteran was discharged with a disability, reenlisted, received a Purple Heart or other military decoration

**PII Mapping of Components**

VETSNET resides on servers that are currently accredited under the VBA Corporate Database (CRP). The database function is provided by the VBA Corporate Database (CRP). Therefore, VETSNET does not have any components, itself, and refers to the CRP PIA regarding all component mapping.

**PII Mapped to Components**
Note: Due to the PIA being a public facing document, please do not include the server names in the table.

**PII Mapped to Components**

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is collected from Veterans to determine Veteran eligibility for Compensation and Pension benefits. The Benefits Delivery Network (BDN) and the VBA Corporate Databases (CRP) are also used to determine Veteran eligibility for Compensation and Pension benefits. Data inputs are provided from the Social Security Administration (SSA) for income verification, (SSN match; SSA benefit information or death file notices), Department of Defense (DoD) Department of Finance Administration Services (DFAS) (e.g. DD Form 214); the Internal Revenue Service (IRS) for income verification. Verification information is provided from the Department of Treasury regarding payment history files and returned checks, Defense Manpower Data Center for military reserve status, active duty date. The Federal Bureau of Prisons (BOP) provides Inmate Central Records System data to VETSNET to determine eligibility for those confined beneficiaries in receipt of VA compensation, pension, or dependency and indemnity compensation, or the amount of VA benefits, and to reduce overpayments. Monthly interfaces from DoD, DFAS, Coast Guard, and Department of Health and Human Services (DHHS) are also provided to VETSNET.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

There are a couple ways Veterans may reach out to the Veterans Benefits Administration (VBA) to apply for or adjust benefits. They may fill out the needed forms online or via the telephone.

- All VBA forms are located at http://www.va.gov/vaforms/ (The URL for the associated privacy statement is: http://www.va.gov/privacy/.) Veterans benefit information may also be obtained from https://www.ebenefits.va.gov.
- VBA forms can be downloaded, filled in and printed to be delivered in paper form.
- The VBA toll free number is 1-800-827-1000, upon calling, the veteran will be referred and transferred to the Regional Office of Jurisdiction, where they can provide a service representative with required information

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

If clarifying information is required for a claim for benefits a VBA employee may contact a Veteran directly.

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

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.

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.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

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.
1.5 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

- Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C. Section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55 provide the legal authority for operating VETSNET. VA gathers or creates these records in order to enable it to administer statutory benefits programs to Veterans, Service members, reservists, and their spouses, surviving spouses, and dependents, who file claims for a wide variety of Federal Veteran’s benefits administered by VA.”


- Per SORN 24VA10A7 https://www.oprm.va.gov/docs/Current_SORN_List_11_23_2021.pdf – Patient Medical Records Title 38, United States Code, Section 501(b) and 304. Memorandum of Understanding Between the Department of Defense (DOD) and the Department of Veterans Affairs (VA) for Sharing Personal Information, March 13, 2014

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.

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:
SPI (including personal contact information, service information and benefit information may be released to unauthorized individuals.

Mitigation:
VETSNET adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
- All employees with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- VA Regional Loan Center (RLC) staff, and VBA VACO Monitoring Unit staff also conduct audits of the lenders loan files (which included auditing funding fee information) as part of ongoing lender and RLC quality audits.

Section 2. Uses of the Information

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

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

*Identify and list each use (both internal and external to VA) of the information collected or maintained.*

*This question is related to privacy control AP-2, Purpose Specification.*

The information contained in the records, may include identifying information (e.g., name, address, social security number). Name and social security numbers are used to identify and track individual(s) in VA systems. The address is needed, so that VA can send correspondence to Veterans. Military service and active duty separation information (e.g., name, service number, date of birth, rank, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, service period, whether Veteran was discharged with a disability, reenlisted, received a Purple Heart or other military decoration) is used to verify the Veteran’s service information. Payment information (e.g., Veteran payee name, address, dollar amount of readjustment service pay, amount of disability or pension payments, any amount of indebtedness (accounts receivable) arising from title 38 U.S.C. benefits and which are owed to the VA) is kept for record purposes only. Intended use of information is to communicate with individuals regarding entitlement to VA compensation and pension benefits and deliver appropriate level of benefit programs, to determine, award, and pay eligible individuals VA compensation and pension benefits, to calculate monetary amount of VA pension benefits where entitlement is established, to determine eligibility for VA compensation and pension benefits.

2.2 What types of tools are used to analyze data and what type of data may be produced?

*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.

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

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

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

2.3 How is the information in the system secured?

2.3a What measures are in place to protect data in transit and at rest?
VETSNET shares data with external entities and protects data in transit using Secure Direct Connect.
The protection of Data at Rest falls on the VBA Corporate Database which is accredited under VBA Corporate Infrastructure (CRP-BEP).

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
All PII for VETSNET is maintained in the VBA Corporate Database which is accredited under VBA Corporate Infrastructure (CRP-BEP). Common Security Services (CSS) is used to restrict access.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest
All PII for VETSNET is maintained in the VBA Corporate Database which is accredited under VBA Corporate Infrastructure (CRP-BEP).

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?
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.

All PII that VETSNET access and exchanges is stored and maintained in the VBA Corporate Database that is accredited under VBA Corporate Infrastructure (CRP-BEP). All VA personnel that access both CRP-BEP and VETSNET must sign the VA Rules of Behavior and attend security awareness training annually. All certificates for training are maintained in VA’s Talent Management System (TMS). All system administrators that work on the system access it through the use of multifactor authentication via their Personal Identity Verification (PIV) card. All PII that is exchanged by VETSNET is done so through the means described in question 2.3, above.

### 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.

Compensation, pension, and vocational rehabilitation claims folders are retained at the servicing regional office until they are inactive for three years, after which they are transferred to the Records Management Center (RMC) for the life of the Veteran. Official legal documents (e.g., birth certificates, marriage licenses) are returned to the claimant after copies are made for the claimant’s file. At the death of the Veteran, these records are sent to the Federal Records Center (FRC) and maintained by the National Archives and Records Administration (NARA) in accordance with NARA policy. Some claims folders are electronically imaged; in which case, the electronic folder is maintained in the same manner as the claims folder. Once a file is electronically imaged and accepted by VBA, its paper contents (with the exception of documents that are the official property of the Department of Defense, and official legal documents), are destroyed in accordance with Records Control Schedule VB–1 Part 1 Section XIII, as authorized
by NARA. Documents that are the property of the DoD are either stored at the RMC or transferred to NARA and maintained in accordance with NARA policy.

Vocational Rehabilitation counseling records are maintained until the exhaustion of a Veteran’s maximum entitlement or upon the exceeding of a Veteran’s delimiting date of eligibility (generally, ten or twelve years from discharge or release from active duty), whichever occurs first, and then destroyed. Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA. Education electronic folders are retained at the servicing Regional Processing Office. Education folders may be destroyed in accordance with the times set forth in the Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA. Employee productivity records are maintained for two years after which they are destroyed by shredding or burning.

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

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

Compensation, pension, and vocational rehabilitation claims folders are retained at the servicing regional office until they are inactive for three years, after which they are transferred to the Records Management Center (RMC) for the life of the Veteran. Official legal documents (e.g., birth certificates, marriage licenses) are returned to the claimant after copies are made for the claimant’s file. At the death of the veteran, these records are sent to the Federal Records Center (FRC) and maintained by the National Archives and Records Administration (NARA) in accordance with NARA policy. Some claims folders are electronically imaged; in which case, the electronic folder is maintained in the same manner as the claims folder. Once a file is electronically imaged and accepted by VBA, its paper contents (with the exception of documents that are the official property of the Department of Defense, and official legal documents), are destroyed in accordance with Records Control Schedule VB–1 Part 1 Section XIII, as authorized by NARA. Documents that are the property of the Department of Defense are either stored at the RMC or transferred to NARA and maintained in accordance with NARA policy.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.
An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. This question is related to privacy control DM-2, Data Retention and Disposal.

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

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?

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

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

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

The VETSNET system does not use PII/PHI/SPI or production data for any testing or development 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.
While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

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

**Principle of Data Quality and Integrity:** Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

**Privacy Risk:**
As described herein, support systems retain information until that work in progress is completed and data is committed to master systems and records. The master systems retain data on a permanent basis (beyond the actual death of the veteran). If a master system is to be deactivated, critical information is migrated to the new system and the old system (along with associated data) is archived according to the application disposition worksheet. As such, SPI, PII or PHI may be held for long after the original record was required to be disposed. This extension of retention periods increases the risk that SPI may be breached or otherwise put at risk.

**Mitigation:**
Redaction of some information is required by law and protects the privacy interest of any individual who may have SPI, PII or PHI which may appear in the data and files collected.

**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**

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veterans Health Administration (VHA)</td>
<td>Determine eligibility for Veteran compensation.</td>
<td>Name: Social Security Number: Date of Birth: Mailing Address: Zip Code: Phone Numbers: Email Address: Emergency Contact Information: Financial Account Information: Health Insurance Beneficiary Numbers Current Medications: Previous Medical Records:</td>
<td>Electronic transmission methods in accordance with VA policy. Paper records are shared with the VHA to conduct medical examinations to determine Veteran’s eligibility for compensation. The VHA accesses Veteran’s information in VBMS and VIS to verify eligibility.</td>
</tr>
<tr>
<td>Veterans Benefits Administration (VBA) VBA Corporate Infrastructure (CRP)</td>
<td>VBA Corporate Database that stores and receives PII for several VBA applications.</td>
<td>Name, verify ssn, address info, disability info, service name/dates of service, competency, character of discharge, pct of disability 0-100</td>
<td>Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS).</td>
</tr>
<tr>
<td><strong>List the Program Office or IT System information is shared/received with</strong></td>
<td><strong>List the purpose of the information being shared/received with the specified program office or IT system</strong></td>
<td><strong>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</strong></td>
<td><strong>Describe the method of transmittal</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Veterans Benefits Administration (VBA)</td>
<td>Benefits Delivery Network (BDN)</td>
<td>Name, verify ssn, address info, disability info, service name/dates of service, competency, character of discharge, pct of disability 0-100</td>
<td>Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS).</td>
</tr>
</tbody>
</table>

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

Follow the format below:

**Privacy Risk:**
There is a risk that VETSNET data may be shared with unauthorized users or authorized users may share it with other unauthorized individuals.

**Mitigation:**
The VA provides Windows and Oracle access controls along with the following security controls: Audit and Accountability, Awareness Training, Security Assessment and Authorization, Incident Response, Personnel Security, and Identification and Authentication.

- All personnel with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- VETSNET adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).
- Information is shared in accordance with VA Handbook 6500.

### Section 5. External Sharing/Receiving and Disclosure

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

**5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?**
Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

### Data Shared with External Organizations

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Social Security Administration (SSA)</strong> (SSNECS), Title II Systems (Title II), Supplemental Security Income Record Maintenance Systems (SSIRMS) and Earnings Records Maintenance System (ERMS) and SSA Death Alert Control and</td>
<td>VBA uses information provided from SSA to verify and correct benefit records. VBA matches it’s benefit files with records provided by SSA, allowing VBA to ensure certain benefits will properly terminate when there is a record of death.</td>
<td>DOB SSN Master Earnings File Death indicator</td>
<td>Compensation, Pension, Education and Vocational Rehabilitation and Employment Records System of Record (58VA21/22/28)</td>
<td>Site to Site FIPS 140-2 validated VPN tunnel.</td>
</tr>
<tr>
<td><strong>List External Program Office or IT System</strong> information is shared/received with</td>
<td><strong>List the purpose of information being shared / received / transmitted with the specified program office or IT system</strong></td>
<td><strong>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</strong></td>
<td><strong>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</strong></td>
<td><strong>List the method of transmission and the measures in place to secure data</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Social Security Administration (SSA) US Department of Health and Human Services Administration for Children and Families Office of Child Support Enforcement</strong></td>
<td>Enables IRS to provide VA income information for purposes of verifying applicants eligibility and/or payment amounts to recipients under VA benefits programs</td>
<td>Name SSN</td>
<td>26 U.S.C. 6103 (1)(7) Privacy Act of 1974, 5 U.S.C. 552a 38 U.S.C. 5317</td>
<td>Two-way data exchange path. Data is encrypted and transferred using Connect: Direct Secure Plus File Transfer software through a VA Transport Layer Protocol site to site VPN tunnel, which is 140-2 compliant.</td>
</tr>
<tr>
<td><strong>Internal Revenue Service (IRS)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List External Program Office or IT System information is shared/received with</td>
<td>List the purpose of information being shared / received / transmitted with the specified program office or IT system</td>
<td>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</td>
<td>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</td>
<td>List the method of transmission and the measures in place to secure data</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>United States Coast Guard (USCG)</td>
<td>To deliver information between VA and the USCG in order to accurately calculate CG, National Oceanic and Atmospheric Administration (NOAA), and Public Health Service (PHS) and VA payment of veterans disability claims and military retiree entitlement. The data exchanged is “pay impactful” for both agencies.</td>
<td>VA’s rating percentage, monthly disability compensation, VA unemployable flag, Survivor Benefit Plan premiums, VARO number, diagnostic codes, combat-related information, and yearly cost of living adjustments</td>
<td>10 USC 1413a 10 U.S.C. 1414 10 U.S.C. 1450 38 U.S.C. 5305 38 U.S.C. 5721-5728 18 U.S.C. 641 18 U.S.C. 1905</td>
<td>One-way path from VA to USCG bi-monthly via a Combined Interface File (CIF)</td>
</tr>
<tr>
<td>Defense Manpower Data Center (DMDC)</td>
<td>To deliver respective computer matching agreement between VA and the State Public Assistance Agencies (SPAAs). The DMDC will provide the information to the SPAAs. The SPAAs report this data usage to comply with the requirements set by VA/DMDC joint strategic initiative issued by VA in November 2007 and Title 10 U.S.C.</td>
<td>Name SSN</td>
<td>VA/DMDC joint strategic initiative issued by VA in November 2007 and Title 10 U.S.C.</td>
<td>Cycle files are sent via a FIPS-140-2 approved encryption algorithms and products (Connect: Direct Secure Plus) from VA to DMDC quarterly, at the end of the month (February, May, August, and November</td>
</tr>
<tr>
<td><strong>List External Program Office or IT System</strong></td>
<td><strong>List the purpose of information being shared / received / transmitted with the specified program office or IT system</strong></td>
<td><strong>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</strong></td>
<td><strong>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</strong></td>
<td><strong>List the method of transmission and the measures in place to secure data</strong></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Administration for Children and Families (ACF), within the Department of Health and Human Services (HHS). They will use the data for their public assistance programs to determine eligibility and ensure fair and equitable treatment in the delivery of benefits attributable to funds by the Federal Government.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US Treasury Bureau of Fiscal Service (TWAI)</td>
<td>The interconnection is provided in order for the Fiscal Service to share data and information with VA. The interconnection will reduce government operating costs, provide greater functionality and improve efficiency.</td>
<td>SSN VA File Number Payment Address (EFT)</td>
<td>Compensation, Pension, Education and Vocational Rehabilitation and Employment Records- VA (58 VA 21/22/28)</td>
<td>The interconnection was established using guidance provided in the Fiscal Service Platform Services Division (PSD) Document Standards Document for External Network Communications General Edition 4.6 and TWAI System Security Plan. All</td>
</tr>
<tr>
<td>List External Program Office or IT System information is shared/received with</td>
<td>List the purpose of information being shared / received / transmitted with the specified program office or IT system</td>
<td>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</td>
<td>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</td>
<td>List the method of transmission and the measures in place to secure data</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Defense and Accounting Service (DFAS)</td>
<td>The purpose of the interconnection is to deliver information between VA and DFAS in order to accurately calculate DFAS and VA payment of Veterans' disability claims and military retiree entitlement. The data exchanged is “pay impactive” for both organizations.</td>
<td>Name, SSN</td>
<td>Compensation, Pension, Education and Vocational Rehabilitation and Employment Records- VA (58 VA 21/22/28)10 U.S.C. 1413a 10 U.S.C. 1414 10 U.S.C. 1450 38 U.S.C. 5305 38 U.S.C. 5721-5728 18 U.S.C. 641 18 U.S.C. 1905</td>
<td>Multiple files are sent from VETSNET via a FIPS 140-2 validated encryption when encryption is required. 3 exchanges are made from VETSNET: Combined Interface File (CIF) from VA to DFAS sent twice a week A monthly file of Survivor Benefit Plan (SBP) direct remittance payments, which DFAS applies to the members record to keep SBP premiums up to date. A CRSC recertification file 2 to 3 times a month, which DFAS uses to update retiree and annuitant records with current VA compensation information. Information transferred is FIPS 140-2 compliant.</td>
</tr>
<tr>
<td><strong>List External Program Office or IT System information is shared/received with</strong></td>
<td><strong>List the purpose of information being shared / received / transmitted with the specified program office or IT system</strong></td>
<td><strong>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</strong></td>
<td><strong>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</strong></td>
<td><strong>List the method of transmission and the measures in place to secure data</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>needed for retirees to receive accurate monthly payments. DFAS sends a monthly file payment to VA for CRSC/CRDP accounts that require additional retroactive payment from VA. DFAS sends a file of SSNs that require CRSC Recertification to VA, there times a month.</td>
</tr>
<tr>
<td>List External Program Office or IT System information is shared/received with</td>
<td>List the purpose of information being shared / received / transmitted with the specified program office or IT system</td>
<td>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</td>
<td>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</td>
<td>List the method of transmission and the measures in place to secure data</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| Department of Education (DoE) National Student Loan Data System (NSLDS) | NSLDS will receive transmitted data file from VBA of Post-9/11 GI Bill beneficiaries (Veterans) annually. The data file will be comprised of individual loan holder information NSLDS will return to VBA an aggregated file by using its current methodology for the CDR calculations which allows VA to post the aggregated institutional-level information on VA’s GI Bill Comparison Tool for the Service members, Veterans, to make informed decisions regarding higher education opportunities. | SSN, Date of Birth, Last Name, First Name | The Privacy Act of 1974 The E-Government Act of 2002 OMB Circulars and Memoranda:  
• OMB Circular A-130, Management of Federal Information Resources  
• OMB M-017-12, Preparing for and Responding to a Breach of Personally Identifiable Information  
• OMB M-08-05, Implementation of Trusted Internet Connections (TIC) Department of Education Policies and Procedures  
• OCIO 3-112, Cybersecurity Policy  
• Department of Education Handbook for Protection of Sensitive but Unclassified Confidential Information Freedom of Information Act, 5 U.S.C. § 552 | MOU/ISA |
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:**
There is a risk that VETSNET data may be shared with unauthorized users or authorized users may share it with other unauthorized individuals. Additionally, misspelling the veteran’s name could result in the wrong data to be displayed.

**Mitigation:**
Outside agencies provide their own level of security controls such as access control, authentication, and user logs in order to prevent unauthorized access.

- All personnel with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- VETSNET adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).

Information is shared in accordance with VA Handbook 6500.
• All personnel accessing Veteran’s information must first have a successfully adjudicated fingerprint check. This fingerprint check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. Individual users are given access to Veteran’s data through the issuance of a user ID and password, and/or a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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 question is 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.

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


2. This Privacy Impact Assessment (PIA) also serves as notice of the AITC VETSNET system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs “after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available.

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

Depending on the information required, some data collection is mandatory while others are voluntary. Failure to provide information may result in denial of access to the health care system. Veterans and their family or guardian (spouse, children, parents, grandparents, etc.) may not decline or request their information not be included as part to determine eligibility and entitlement for VA compensation and pension benefits and 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

While individuals may have the ability to consent to various uses of their information at the VA, they are not required to consent to the use of their information as part to determine eligibility and entitlement for VA compensation and pension benefits proceeding. The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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 Virtual VA 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, as discussed in detail in question 6.1, including the Privacy Act statement and a System of Record Notice.

Section 7. Access, Redress, and Correction

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

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

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.

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).

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. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Individual 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) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 (July 19, 2012). This SORN can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf.

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.

Individual wishing to obtain more information about access, redress and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records, they 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 Records – VA” 58VA21/22/28 (July 19, 2012).
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.

Individual 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) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 (July 19, 2012). This SORN can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf.

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. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Individual 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) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 (July 19, 2012). This SORN can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf.

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

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

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

**Principle of Individual Participation:** Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

*This question is related to privacy control IP-3, Redress.*

Follow the format below:

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

**Mitigation:**
By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications and 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?**

*Describe the process by which an individual receives access to the system.*

*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?*

*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.*

*This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.
OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed through the use of TMS.

Users of VA/VBA information systems gain access through a AITC LAN control domain. The AITC LAN uses Group Policy Objects (GPO) to manage accounts. GPO is a set of rules which control the working environment of user accounts and computer accounts. GPO provides the centralized management and configuration of operating systems, applications and users' settings in an Active Directory environment. GPO restricts certain actions that may pose potential security risks. Access must be approved by the Information Security Officer (ISO) at the Regional Office at which the employee is located. Access to the VETSNET suite of applications is authenticated through Common Security Services (CSS).

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.

OIT&T provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training for new users, when required by system changes and annually thereafter. VETSNET contracts are reviewed on a quarterly basis and accounts are disabled after 90 days of inactivity.

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

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

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

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

Yes

1. The Security Plan Status - Valid
2. The Security Plan Dated 5-21-2021
3. The Authorization Status – 1 Year ATO
4. The Authorization Date – 7-12-2021
5. The Authorization Termination Date - 7-12-2022
6. The Risk Review Completion Date – 9-15-2021
7. The FIPS 199 classification of the system (MODERATE).

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).

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.

No, VETSNET does not use cloud technology.

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)

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**

<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td><strong>Authority and Purpose</strong></td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td><strong>Accountability, Audit, and Risk Management</strong></td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td><strong>Data Quality and Integrity</strong></td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td><strong>Data Minimization and Retention</strong></td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
<tr>
<td>IP</td>
<td><strong>Individual Participation and Redress</strong></td>
</tr>
<tr>
<td>IP-1</td>
<td>Consent</td>
</tr>
<tr>
<td>IP-2</td>
<td>Individual Access</td>
</tr>
<tr>
<td>IP-3</td>
<td>Redress</td>
</tr>
<tr>
<td>IP-4</td>
<td>Complaint Management</td>
</tr>
<tr>
<td>SE</td>
<td><strong>Security</strong></td>
</tr>
<tr>
<td>SE-1</td>
<td>Inventory of Personally Identifiable Information</td>
</tr>
<tr>
<td>SE-2</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>TR</td>
<td><strong>Transparency</strong></td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System of Records Notices and Privacy Act Statements</td>
</tr>
<tr>
<td>TR-3</td>
<td>Dissemination of Privacy Program Information</td>
</tr>
<tr>
<td>UL</td>
<td><strong>Use Limitation</strong></td>
</tr>
</tbody>
</table>

Version Date: October 1, 2021
<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
Signature of Responsible Officials

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

Tonya L. Facemire 234776
Digitally signed by Tonya L. Facemire 234776
Date: 2022.03.23 13:03:20 -04'00'

Privacy Officer, Tonya Facemire

Richard Tercero 401041
Digitally signed by Richard Tercero 401041
Date: 2022.03.23 09:11:38 -07'00'

Information Systems Security Officer, Richard Tercero

Gary W. Dameron 101941
Digitally signed by Gary W. Dameron 101941
Date: 2022.03.23 13:26:15 -04'00'

Information Systems Owner, Gary Dameron
APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

The System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 (July 19, 2012). This SORN can be found online at