Privacy Impact Assessment for the VA IT System called:

Benefits Processing Data Service (BPDS)

Benefits and Memorials Services

Veterans Benefits Administration

eMASS ID# 2070

Date PIA submitted for review:

6/11/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.harvey@va.gov	202-461-8401
Information System Security Officer (ISSO)	Joseph Facciolli	Joseph.Facciolli@va.gov	215-983-5299
Information System Owner	Lindsay Tucker	Lindsay.Tucker@va.gov	512-364-1176

Abstract

The abstract provides the simplest explanation for "what does the system do?".

The Benefits Process Data Service (BPDS), hosted by the Benefits Integration Platform (BIP) within the VA Enterprise Cloud (VAEC), allows the VA to store and request raw data received by non-VBA systems via web-based forms as Benefits Process Data (BPD). BPDS provides the ability to store BPDs (JSON documents identifiable by UUID) and the ability to wholly retrieve this data. Submitted BPDs are given an ID and can be associated with other VBA data such as claim IDs or File Numbers. These BPD IDs and other VBA data may be utilized to retrieve target BPDs.

The primary use case for BPDS is to enable a service consumer to post raw structured data to BPDS in a way that allows Process Automation to read, Operations to troubleshoot, and Performance Analysis & Integrity (PA&I) to report.

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. What is the IT system name and the name of the program office that owns the IT system?

- Benefits Processing Data Service (BPDS) is owned by the VBA Office of Business Integration (OBI) and operated by Benefits Integration and Administration (BIA) Product Line which is situated within the Benefits and Memorials (BAM) Portfolio.

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

- BPDS is a storage repository for scanning vendors to upload VA Form data; e.g. VA Form 530. BPDS allows Pension Automation and Mail Automation to look at the data submitted by Veterans and their delegates to assist with pension analysis.

C. Who is the owner or control of the IT system or project?

- BPDS is owned by the VBA OBI and operated by the BIA Product Line, which is situated within the BAM Portfolio.

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?

- BPDS will store Veteran and non-Veteran claimant data for approximately 50001-75000 individuals. BPDS processes information regarding Veterans, Dependents, VA Employees and VA Contractors.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

- BPDS is a repository of scanned VA Form data; e.g. VA Form 530. BPDS allows Pension Automation and Mail Automation to look at the data submitted by Veterans and their delegates to assist with pension analysis.

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

- BPDS receives VA Form data containing PII via Benefit Request Intake, completed by the Veteran, from VBA systems. VBA Automation Platform extracts data from the subject VA forms and uploads it to BPDS. BEP stores and shares readable data stored with Pension Automation. Pension Automation utilizes this data for Veteran pension analysis.

G. Is 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?

- BPDS is a minor, assess only tenant application of BIP. The BIP resides on the VA Enterprise Cloud (VAEC) GovCloud High. BIP operated within a single instance of the VAEC AWS GovCloud, deployed across three Availability Zones.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

BPDS operates under the following legal authority:

- VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records— VA'' (58VA21/22/28)
  - https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf
- Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
- SORNs: 38 U.S.501(a)C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E
- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,
- VA Directive and Handbook 6502, Privacy Program

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

- The SORN will not require revision and approval.
- The SORN for BPDS does cover cloud usage and storage.

4. System Changes

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

- Completion of this PIA is not anticipated to result in circumstances that require changes to business processes.

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

- Completion of this PIA is not anticipated to result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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[1]
- ☒ 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)

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

Account Numbers

The following are all selected, as VA Form data is specific to each form and could change outside of BPDS knowledge. Each item has the potential for use however use is not guaranteed.

PII Mapping of Components (Servers/Database)

BPDS 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 BPDS 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 server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
Oracle Database/Restful API	Yes	Yes	Name SSN Date of Birth (DOB) 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)	The database stores data retrieved by consumers of BPDS	Safeguards are determined by the VBA

			Financial Information Account numbers Certificate/License numbers Vehicle License Plate Number Internet Protocol (IP) Address Numbers Race/Ethnicity Tax Identification Number Gender Integrated Control Number (ICN) Other Unique Identifying Number		

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?

- BPDS receives data, listed in Section 4.1, from BPDS integration partners for the purpose of digital document storage.

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.

- There is no data required other than data received by scanning vendors.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

- BPDS does not create information.

1.3 How is the information collected?

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

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

- BPDS collects information, listed above in Section 1.1, from the internal VA integration partners via electronic submission through the BPDS API. The information provided to BPDS is collected by our integration partners from VA Form data.

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

- N/A

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.

- BPDS does not manage the data validation processes and assumes that the original source data has been reviewed for accuracy before being provided to BPDS. BPDS will ensure that the design requirements for data storage are valid.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

- BPDS is not responsible for accuracy of the data requested for storage by integrated systems but will ensure the data requested for storage is valid and is stored against the design requirements.

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

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048

- VA Compensation, Pension Education, and Vocational Rehabilitation Employment Records -VA SORN 58VA21/22/28 86 FR 61858
- 38 U.S.501(a)C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- Privacy Act of 1974; U.S Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 &Title38, US Code section 7301 (a) and Executive Order 9397
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws
- The legal authority is 38 U.S.C 7601-7604 and U.S.C 7681-7683 and Executive Order 93

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: No current identified privacy risks.

Mitigation: There are no current identified privacy risks BPDS, no mitigation is required.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
• 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 • Account Numbers • Certificate/License numbers • Vehicle License Plate Number • Internet Protocol (IP) Address Numbers • Race/Ethnicity • Tax Identification Number • Gender • Integrated Control Number (ICN) • Other Unique Identifying Number	File Identification purposes	Not used

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?

- BPDS does not perform data analysis, it accepts JSON versions of scanned VA Forms.

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.

- BPDS does not create information.

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?

- BPDS encrypts data at rest and data in transit (SSL, TLS). FIPS 140-2 compliant.
- Uses automated tools to validate and enforce data at rest controls are utilized continuously.
- Encryption keys and certificates are stored securely and rotated at appropriate times with strict access control.
- BIP protects the confidentiality and integrity of the transmitted information within the system boundary.
- BIP Platform utilizes Amazon Elastic Block Storage (EBS) for platform component storage, including platform operational state from the distributed state model, as well as for log files and log aggregators that could contain PII/PHI from BIP minor applications.

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

- Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system. Further, SPI will be encrypted in transit and at rest.
- While in transit, the systems utilize Mutual SSL authentication and encryption protocols.
- All data is encrypted at rest in the database.

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

- BPDS does not share data with third parties.
- All Users, employees and contractors, are required to take VA Privacy and Rules of Behavior, which includes training on how to safeguard PII/PHI.

- BIA Benefits Services is a tenant system of BIP. Security and privacy data held by a cloud provider is required to meet the requirements under the privacy act. Federal agencies must identify and assess the risk to their PII, and to ensure security controls are implemented to provide adequate safeguards. Section C MM. of the contract references OMB Memorandum "Security Authorization of Information Systems in Cloud Computing Environments" FedRAMP Policy Memorandum.

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?

- To receive access to BPDS, a partner (i.e. client system) will need approval from the BPDS Information System Owner. A unique application key will be created for the partner to access the API. The key is provided for every request to access the API.

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

- Yes, BPDS has onboarding documents and processes for new consumers.

2.4c Does access require manager approval?

Yes.

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

- All operations are audited as well as the data is immutable once persisted.

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

- Safeguards are determined by the VBA.

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*

1.Name
2.Social Security Number
3.Date of Birth
4.Mother's Maiden Name
5.Personal Mailing Address
6.Personal Phone Number(s)
7.Personal Fax Number
8.Personal Email Address
9.Emergency Contact Information (Name, Phone Number, etc. of a different individual)
10.Financial Information
11. Account Numbers
12.Certificate/License numbers
13.Vehicle License Plate Number
14.Internet Protocol (IP) Address Numbers
15.Race/Ethnicity
16.Tax Identification Number
17. Gender
18. Integrated Control Number (ICN)
19.Other Unique Identifying Number

3.2 How long is information retained?

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

- VA Form Data held by BPDS is retained indefinitely.

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?

- All records are stored within BPDS as the system of record for scanned documents utilized by Pension and Mail Automation; however, because BPDS does not process physical forms, the responsibility of obtaining an approved retention schedule is out of scope.
- National Archives and Records Administration (NARA) https://www.archives.gov/records-mgmt/grs.html

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

- All records are stored within BPDS as the system of record for scanned documents utilized by Pension and Mail Automation; however, because BPDS does not process physical forms, the responsibility of obtaining an approved retention schedule is out of scope.

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.

- All records are stored within BPDS as the system of record for scanned documents utilized by Pension and Mail Automation; however, because BPDS does not process physical forms, the responsibility of obtaining an approved retention schedule is out of scope.

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

- All research, testing and/or training is conducted in lower environments that do not contain PII.

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: BPDS is designed to retain digital data indefinitely. There is a risk that information will be stored in the system longer than necessary.

Mitigation: Digital data indefinite retention is mandated by the following System of Record Notice (SORN): SORN 58VA21/22/28 86 FR 61858 Compensation, Pension Education, and Vocational Rehabilitation Employment Records-VA. 2021-24372.pdf (govinfo.gov)

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***
Pension Automation, eMASS ID# 2062	Pension Automation receives data submitted by Veterans and their delegates for pension analysis	Name, Social Security Number (SSN), Date of Birth (DOB), 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, Certificate/License Numbers, Vehicle License Plate Number, Internet Protocol (IP) Address Numbers, Race/Ethnicity, Tax Identification Number, Gender, Integrated Control Number (ICN), Other Unique Identifying Number	HTTPS Request/Response (JSON data format)
VBA Automation Platform (VBAAP), eMASS ID# 1143	VBA Automation Platform uploads JSON versions of Pension Automation relevant documents to BPDS for Pension Automation to consume.	Name, Social Security Number (SSN), Date of Birth (DOB), 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, Certificate/License Numbers, Vehicle License Plate Number, Internet Protocol (IP) Address Numbers, Race/Ethnicity, Tax Identification Number, Gender, Integrated Control	HTTPS Request/Response (JSON data format)

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*
		Number (ICN), Other Unique Identifying Number	

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: Sharing of protected Veteran data is necessary to support VA benefits processing/ensure eligible Veterans receive the VA benefits to which they are entitled however sharing of any information carries with it a risk of unauthorized disclosure.

Mitigation: The risk of improperly disclosing protected Veteran data to an unauthorized internal VA entity and/or VA personnel is mitigated by limiting access only those VA entities and personnel with approved access and clear business purpose/need to know. Additionally, consent for use of PII data is signaled by the completion of benefits forms by the Veteran. The principle of need to know is strictly adhered to. Information is shared in accordance with VA Handbook 6500.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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 no external sharing.

Mitigation: There is no 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.

- VA consistently publishes all SORNS to the Federal Register as dictated by law and VA Policy. VA requires the Administration and Staff Offices to put forth for approval and publication all notice for their respective Privacy Act system of records. VBA routinely updates SORN for altered system of record that include major changes or changes in the routine use. VBA ensuring that the required notice is given with requests for Social Security Numbers, and that a Privacy Act statement appears on each applicable form or accompanying instruction sheet collecting information that is going into a Privacy Act system of records (see 5 USC 552a(e)(3)).

- (SORN) SORN 58VA21/22/28 86 FR 61858 Compensation, Pension Education, and Vocational Rehabilitation Employment Records-VA. 2021-24372.pdf (govinfo.gov)

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

- A notice was not provided. BPDS does not collect information directly from the Veteran, but instead from the applications listed in section 4.1 of this PIA. The source systems collecting the information would provide the notice. The System of Record Notice (SORN) SORN 58VA21/22/28 86 FR 61858 Compensation, Pension Education, and Vocational Rehabilitation Employment Records-VA. 2021-24372.pdf (govinfo.gov) indicates all purposes of use and records categories stored in the BPDS system.

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.

- http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf

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

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

- This is not applicable to BDPS as the systems does not engage directly with the Veteran. All data processed by BPDS is provided by systems, as noted in Section 1.1, that integrate with BPDS. Veterans may have the opportunity or notice of the right to decline to provide information to the source systems that collects the information from the Veteran.

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.

- This is not applicable to BDPS as the systems does not engage directly with the Veteran. All data processed by BPDS is provided by systems, as noted in Section 1.1, that integrate with BPDS. Veterans may have the opportunity or notice of the right to decline to provide information to the source systems that collects the information from the Veteran.

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 an individual may not receive notice that the BPDS API is utilizing their information.

Mitigation: The VA mitigates this risk by providing Veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. The main forms of notice are discussed in the Privacy Act statement, a System of Record Notice, and the publishing of this Privacy Impact Assessment as well as the PIA's for our partner systems.

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 seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/28(July 19, 2012).

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)?

- BPDS is not exempt from the access provisions of the Privacy Act.

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

- BPDS is not a Privacy Act system. Procedures and regulations in place that covers an individual gaining access to their information is beyond the scope of BPDS.

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.

- Individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 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.

- Individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/28(July 19, 2012).

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. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/28(July 19, 2012).

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individual 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 files. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and 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?

- In order to receive access to BPDS, a partner (i.e., client system) will need approval from the Information System Owner. A unique application key will be created for the partner to access the API.

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?

- Users from other non-VA agencies do not have access to BPDS.

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.

- Users from other non-VA agencies do not have access to BPDS.

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 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.
- VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, ISSO, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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 ROB or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. VA employees and contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). 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. All VA employees must complete annual Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

- All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, ISSO, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders

required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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

- This is not applicable to BPDS as the system is a minor, assess only, tenant application of BIP. BIP's authorization information is provided below.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 03/26/2024
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 06/30/2024
5. *The Authorization Termination Date:* 06/30/2026
6. *The Risk Review Completion Date:* 06/30/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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

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

Section 9 – Technology Usage

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

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

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

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

- Yes, BPDS is a minor, assess only, tenant application of BIP. The BIP resides on the Federal Risk and Authorization Management Program (FedRAMP) approved VA Enterprise Cloud (VAEC) GovCloud High.

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.

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.

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.

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).

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

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

MARVIS HARVEY

Digitally signed by MARVIS HARVEY
Date: 2024.08.20 10:43:34 -05'00'

Privacy Officer, Marvis Harvey

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2024.08.20 13:29:45 -04'00'

Information System Security Officer, Joseph Facciolli

LINDSAY TUCKER

Digitally signed by LINDSAY TUCKER
Date: 2024.08.20 12:02:33 -05'00'

Information System Owner, Lindsay Tucker

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; screen shot of a website collection privacy notice).

Notice of Privacy Practices
This system is intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA; all use is considered to be understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms. Unauthorized attempts or acts to either (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties. PRIVACY ACT INFORMATION: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA Programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is required to obtain or retain benefits. VA uses your SSN to identify your claim file. Providing your SSN will help ensure that your records are properly associated with your claim file. Giving us, your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefit for refusing to provide his or her SSN unless the disclosure of the SSN is required by Federal Statute of law in effect prior to January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine maximum benefits under the law.

The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies.

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

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