Privacy Impact Assessment for the VA IT System called:

# BIP Compensation and Pension User Interface (CPUI)

# Benefits, Appeals and Memorials

# Veterans Benefits Administration (VBA)

Date PIA submitted for review:

3/2/2022

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Simon Caines | Simon.Caines@va.gov | 202-461-9468 |
| Information System Security Officer (ISSO) | Joseph Facciolli | Joseph.Facciolli@va.gov | 215-842-2000x2012 |

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Information System Owner | Gary Dameron | Gary.Dameron2@va.gov | 202-492-1441 |

## Abstract

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

The purpose of the BIP Compensation and Pension UI (CPUI) application is to increase the efficiency and quality of Claims Processors while working in VBMS. This application provides User Interface microservice front-ends for three components of VBMS Core:

1) Interactive Development Banner (IDB) UI – makes recommendations to Claims processors of work that needs to be done before moving the claim along to the next phase.
2) Interactive Development Banner Admin – manages the recommendations that are made in IDB
3) STR Assist – Based on Veteran and Period of Service information makes recommendations on which STR repository to request STR from.

Each of these UI components interface with various backend services to retrieve and modify data from the sources of record and then display that data in their UIs.

## 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 for the system cover cloud usage or storage?*

The CPUI application consists of three User Interface microservice applications that are hosted on the Benefits Integration Platform (BIP) and are components of VBMS Core. The CPUI is owned by the Benefits, Appeals and Memorials Program Office. The business purpose of these applications is to increase the speed with which claims for Veteran benefits are processed while also reducing errors in the claims processing workflow. By reducing these errors we further increase the speed with which claims can be approved for our Veterans. This system is VA owned and VA operated.

The three UI components that make up CPUI are listed and described below:

1) Interactive Development Banner (IDB) UI – displays recommendations of work that needs to be done during the Claim development process before moving Claim to the next processing phase. This application is dependent on BIP BSS and BIP CFAPI to support authentication and to provide the pre-calculated recommendations that will be displayed in IDB. This system does not display of process any PII or PHI.
    a. Since this capability is available to all users of VBMS Core there could be as many as 20,000 users per day. These individuals are standard Claims processors.
2) Interactive Development Banner (IDB) Admin – manages the recommendations that are made in IDB. This system is dependent on BIP BSS and BIP CFAPI to provide authentication and to store the rules that are created in the IDB Admin UI. This system does not display or process and PII or PHI.
    a. There likely be less than 20 users of this application. These individuals will be advanced users with specific credentials that are well trained in creating rules to determine which recommendations will be displayed in IDB.
3) STR Assist – This application is responsible for collecting PII and Service Period information about a Veteran so that it can calculate a recommendation on the most likely source system that the claim processor will find the Veteran's Service Treatment Records (STRs) in. This system is dependent on BIP BSS, BIP CFAPI and Benefits Gateway System (BGS) services to provide the data needed for calculations as well as to calculate recommendations, store the information used to calculate the recommendations, and maintain the status of what recommendations have been made previously. Additionally, this system will submit digital requests to VA National Personnel Records Center (NPRC) and Department of Defense (DoD) Healthcare Artifacts and Images Management Solution (HAIMS) systems for STRs through the BIP CFAPI.
    a. Since this capability is available to all users of VBMS Core there could be as many as 20,000 users per day. These individuals are standard Claims processors.

IDB and STR Assist are both accessed via the VBMS Core User Interface. IDB Admin is accessed directly by a very small number of properly authorized users.

While there is data that passes through CPUI, none of the data is stored long-term in this system. All log data is stored in the BIP log-aggregation solution. All application data is stored in the CFAPI application security boundary. Requests for Service Treatment Records first go to CFAPI before being routed to other systems such as the NPRC and HAIMS. The only data stored by CPUI is transient log data that is deleted every time a new application version is deployed or every time a pod on the BIP is restarted.

CPUI is hosted on BIP as a Web Application meaning that is hosted in only one site as a primary source. BIP provides some disaster recovery failover capabilities but they are still hosted in the VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) environment.

VA Enterprise Cloud Solutions group partnered with Amazon Web Services (AWS) a FedRAMP provider to offer VA programs the opportunity to host cloud applications. The BIP CPUI application will be deployed onto the Benefits Integrated Platform (BIP) production environment hosted in AWS under VA Enterprise Cloud Solutions Office (ECSO) General Support System (GSS) and accredited as FISMA "HIGH" categorization. Custody and ownership of PII and PHI are solely the responsibility of the VA as a tenant of AWS, in accordance with VA policy and NIST 800-144. Both AWS and the VA have a tremendous interest in maintaining security of PII and PHI, including (but not limited to) HIPAA Enforcement Rule of 2006, HIPAA Omnibus, and HITECH. AWS is responsible for physical security, infrastructure security, network and communications for the facility. VA is responsible for the maintaining application, data and system security for the program. VA is the sole owner of all data stored within the system.

As many of the controls for this application are inherited from systems that are already accredited it is not expected that any changes will come about based on the results of this PIA. There is no SORN for this system as we simply read and update data in other systems.

## 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)

Additional: Veteran Service Number, First and Last Name, Filenumber, Employee ID, Employee Station and Claim Data

**PII Mapping of Components**

CPUI consists of 0 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CPUI and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

**Note**: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

*PII Mapped to Components*

| Database Name of the information system collecting/storing PII | Does this system collect PII? (Yes/No) | Does this system store PII? (Yes/No) | Type of PII (SSN, DOB, etc.) | Reason for Collection/ Storage of PII | Safeguards |
|---|---|---|---|---|---|
| N/A | N/A | N/A | N/A | N/A | N/A |
| | | | | | |
| | | | | | |

### 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.*

1) IDB UI retrieves data from the BIP CFAPI IDB API.
2) IDB Admin retrieves data from the BIP CFAPI IDB Admin API and the BIP BSS Service.
3) STR Assist retrieves data from the BIP CFAPI STR Assist API and the BIP BSS Service.

### 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.*

All components of CPUI collect data via REST Web Service calls to the source systems. All service calls are secured using SSL/TLS encryption.

### 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.*

All three components of the BIP CPUI application will be dependent on users informing us if the data that we have retrieved form VA systems is accurate.

**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*

CPUI does not actually collect data. CPUI calls Web Services in the CFAPI application to retrieve data to be displayed but that data is not stored in the CPUI application.

**1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>**

*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:*

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

*<u>Principle of Minimization:</u> Is the information directly relevant and necessary to accomplish the specific purposes of the program?*

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

*<u>Principle of Data Quality and Integrity:</u> 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:** CPUI retrieves PII and other delicate information through secure web service calls to APIs from the CFAPI minor application hosted on BIP. This information is not stored in the CPUI application beyond transient logs that are deleted with every restart of the CPUI application pods. If someone were to gain access to one of the CPUI application Pods hosted on BIP then there would be limited data of a sensitive nature available in the logs.

**Mitigation:** CPUI will utilize different log levels for the application to ensure that sensitive data is only printed to the transient logs on the Pods when explicitly requested for application triage purposes. The security controls for protecting access to the application infrastructure is inherited from VAEC AWS and the BIP. Application access is controlled by the BIP CSS application to ensure that only authorized users are able to login to the system.

## 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.*

All uses of the data displayed by the CPUI application are for VA internal use only.

1) BIP IDB UI is imported into VBMS and displayed on top of the VBMS Core Claim Details page. VBMS retrieves IDB using a REST webservice that is secured with a secret key and the traffic is encrypted using TLS/SSL. IDB UI displays a list of recommended actions required on the current Claim in VBMS Core to complete the Development phase of Claim processing. These recommendations do not contain any PII/PHI or other sensitive information. User ID is included in the logs, when certain logging levels are utilized, for triage purposes. These recommendations are intended to prevent Claim processors from missing actions that often result in errors and cause delays in processing Claims for our Veterans. All IDB UI data is retrieved from BIP IDB API, which is a component of CFAPI application.
2) BIP IDB Admin UI provides properly authorized users to configure the rules that represent the recommendations that are displayed in IDB. Aside from User ID this application does not display any sensitive data. Users of IDB Admin are allowed to create rules based off of Veteran and Claim data that BIP IDB Admin API, which is a

component of CFAPI application, will utilize to determine if that rule should be displayed for each Claim.

3) BIP STR Assist UI is accessed from VBMS Core. This application displays Veteran identity data and service history data to allow users to request recommendations on which Service Treatment Record repository to request records from. This application also maintains a history of the requests submitted as a result of the recommendation made in the system. All data is retrieved from and stored by BIP STR Assist API, which is a component of CFAPI application.

**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*

None of the components of CPUI perform any complex analytical tasks.

**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?*

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

*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*

CPUI does not store any data but does retrieve data from CFAPI APIs via REST webservices. That data is encrypted in transit using SSL/TLS encryption.

**2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> 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. <u>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.</u>*

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

*<u>Principle of Transparency:</u> Is the PIA and SORN, if applicable, clear about the uses of the information?*

*<u>Principle of Use Limitation:</u> 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.*

Add answer here:

1) BIP IDB UI – no PII/PHI
2) BIP IDB Admin UI – no PII/PHI
3) BIP STR Assist UI uses BIP BSS for Authentication to the application. This enforces multi-factor authentication utilizing VA PIV and requires VBMS credentials be registered with the VA Common Security Service (CSS). Manage approval is required prior to a user being granted VBMS credentials to gain access to this data. Viewing data is not tracked through this application as all data access is controlled and monitored by the BIP STR Assist component of the CFAPI application.

## Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

### 3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is retained by the system.*
*This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

CPUI does not retain any data. All data for CPUI applications is retrieved from and managed by APIs within the CFAPI application.

### 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.*

CPUI does not retain any data. All data for CPUI applications is retrieved from and managed by APIs within the CFAPI application.

### 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.*

CPUI does not retain any data. All data for CPUI applications is retrieved from and managed by APIs within the CFAPI application.

### 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*

N/A as CPUI does not retain any data. All data for CPUI applications is retrieved from and managed by APIs within the CFAPI application.

**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*

CPUI only uses test data for research, testing and training.

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

*Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.*

*While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.*

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

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

*<u>Principle of Data Quality and Integrity:</u> Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?*
*This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.*

Follow the format below:
**<u>Privacy Risk:</u>** There is no Risk from data retention as CPUI does not retain any data. All data for CPUI applications is retrieved from and managed by APIs within the CFAPI application.

**<u>Mitigation:</u>** N/A

## 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*** |
|---|---|---|---|
| CFAPI – BIP IDB API | This information is retrieved in order to display the recommended actions for the active Claim in VBMS Core | • Filenumber<br>• Claim data (Established Date, Type, Status, Other Claims for the Vet)<br>• Contention Name and Type<br>• Military Service Separation Reason and Character of Discharge | REST Web Service over TLS |
| CFAPI – BIP IDB Admin API | The information shared here is data about rules that will | N/A | REST Web Service over TLS |

| ***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*** |
|---|---|---|---|
| | be executed on the data that is stored by the CFAPI BIP IDB API application component. There is no PII exchanged with this application. | | |
| CFAPI – STR Assist API | Retrieving Veteran Identity Information and Service History information so that the user can validate the information and then submit to STR Assist API to receive a recommendation for which repository to request STRs from. For some repositories the user can request that STR Assist API request the STRs for them. | • Filenumber<br>• Participant ID<br>• SSN<br>• Open Claim Types<br>• Military Service Dates, Branches, Periods of Service, Separation Reason and Character of Discharge | REST Web Service over TLS |
| | | | |
| | | | |

## 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:** The primary risk in the sharing of this data is only for data in transit. The data is not stored in the CPUI application beyond potentially being stored in transient CPUI application logs which are deleted with every pod restart.

**Mitigation:** All data transmission is encrypted via TLS/SSL.

## 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 /*** | ***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*** | ***List the method of transmission and the measures in*** |
|---|---|---|---|---|

|  | ***transmitted with the specified program office or IT system*** |  | ***routine use, etc. that permit external sharing (can be more than one)*** | ***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.*

*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:
**<u>Privacy Risk:</u>** N/A

**<u>Mitigation:</u>** N/A

## 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 VBMS system does exist from which the CPUI application is accessible. CPUI application is not publicly accessible, only via the VBMS system. When Veterans apply for benefits, The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for benefits. A signed statement acknowledging that the individual read and understood the NOPP is scanned into each applicant's electronic file. When updates are made to the NOPP copies are mailed to all Veteran's beneficiaries. Additionally, new NOPPs are mailed to beneficiaries on a yearly basis and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records. Additional notice is provided through this Privacy Impact Assessment, which is available online, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs and the following VA System of Record Notices (SORNs) which are published in the Federal Register and available online: The System of record Notice (SORN) "Compensation, Pension, Education, and Rehabilitation Records-VA" 2019 58VA21/22/28 SORN located at https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.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*

Veterans and Service members may decline or request that their information not be included as part to determine eligibility and entitlement for benefits. No penalty or denial of service is attached with not providing needed information; however, services may be delayed.

**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 benefits.

**6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>**

*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:*

*<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?*

*<u>Principle of Use Limitation:</u> 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:
**<u>Privacy Risk:</u>** There is a risk that members of the public may not be aware of the additional features within the VBMS Core application that CPUI provide.

**<u>Mitigation:</u>** 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 Impact Assessment and the System of Record Notice.

## Section 7. Access, Redress, and Correction

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

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

*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.*

Members of the public are not allowed access to VBMS Core, which is where the CPUI Application components are displayed for VA users only. An individual who wishes to determine whether a record is being maintained under his or her name in VBMS Core or wishes to determine the contents of such records should submit a written request or apply in person to the VA facility where the records are located. For a directory of VA facilities and phone numbers by region, see https://www.benefits.va.gov/benefits/offices.asp.

**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.*

Veterans and authorized parties have a statutory right to request a copy of or an amendment to a record in VA's possession at any time under the Freedom of Information Act (FOIA) and the Privacy Act (PA). VA has a decentralized system for fulfilling FOIA and PA requests. The type of information or records an individual is seeking will determine the location to which a request should be submitted. For records contained within a VA claims folder (Compensation and Pension claims), or military service medical records in VA's possession, the request will be fulfilled by the VA Records Management Center. Authorized requestors should mail or fax their Privacy Act or FOIA requests to: Department of Veterans Affairs, Claims Intake Center, P.O. Box 4444, Janesville, WI 53547–4444, Fax: 844– 531–7818, DID: 608–373–6690."

### 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 are not notified if there is missing or inaccurate information in their record. An individual who wishes to determine whether a record is being maintained under his or her name in VBMS Core or wishes to determine the contents of such records should submit a written request or apply in person to the VA facility where the records are located. Requests should contain the full name, address and telephone number of the individual making the inquiry. (Per 58VA21/22/28 SORN)

### 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.*

Veterans and other beneficiaries may contact their supporting VA regional office or VHA center to learn how to access, correct, or contest their information. VBMS-Fiduciary receives information from other systems therefore veterans instead would have to go through the source system's protocols to correcting the data.

### 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.*

1) Access to BIP IDB UI is controlled within VBMS Core and limited to users that are able to view the Claim Details page in VBMS Core.
2) Access to BIP IDB Admin UI is controlled by BIP BSS. Users are required to have a VA PIV and must have the 'IDA Administrator' assigned to them in the VA Common Security Service (CSS) application.
3) Access to BIP STR Assist UI is controlled by BIP BSS. All users with access to VBMS are granted access to STR Assist and can access STR Assist from within VBMS Core on the Development Plan screen or from the Veteran context drop down menu.

All users of the VBMS Core application are required to complete annual information system security training activities including security awareness training and specific information system security training. Annual training on VA Privacy and Information Security Awareness is tracked on the VA TMS.

Access controls to the BIP infrastructure that the CPUI application is hosted in are inherited from the BIP Platform Major Application ATO.

Access controls to the VAEC AWS infrastructure and the AWS Gov Cloud infrastructure is inherited from those teams and their ATOs.

**8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?**

*If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.*

*This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

Yes, the VBMS program contractors who provide support to the system are required to complete a Moderate Background Investigation (MBI), complete annual VA Privacy and Information Security Version Date: February 27, 2020 Page 26 of 30 and Roles of Behavior training via the VA's Talent Management System TMS. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. VA contract employee system/application access is verified through VA Contract Officers Representative (COR) before access is granted to any contractor

**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.*

Users are required to complete information system security training activities including annual security awareness training, Privacy training and specific information system security training.

The training records are retained for 7 years. This documentation and monitoring are performed using the Talent Management System (TMS).

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

*If Yes, provide:*

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

Yes, as a minor application on BIP, CPUI inherits the BIP Authority to Operate from the "BIP Assessing" major application.

1. *The Security Plan Status: Approved*
2. *The Security Plan Status Date: December 18, 2020*
3. *The Authorization Status: Authorization to Operate (ATO)*
4. *The Authorization Date: January 6, 2022*
5. *The Authorization Termination Date: January 6, 2023*
6. *The Risk Review Completion Date: January 7, 2021*
7. *The FIPS 199 classification: High*

## 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.*

The system is hosted on BIP, which is hosted in VAEC AWS GovCloud, a FedRAMP approved Cloud Service Provider.

**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

*Summary of Privacy Controls by Family*

| ID | Privacy Controls |
|---|---|
| **AP** | **Authority and Purpose** |
| AP-1 | Authority to Collect |
| AP-2 | Purpose Specification |
| **AR** | **Accountability, Audit, and Risk Management** |
| AR-1 | Governance and Privacy Program |
| AR-2 | Privacy Impact and Risk Assessment |
| AR-3 | Privacy Requirements for Contractors and Service Providers |
| AR-4 | Privacy Monitoring and Auditing |
| AR-5 | Privacy Awareness and Training |
| AR-7 | Privacy-Enhanced System Design and Development |
| AR-8 | Accounting of Disclosures |
| **DI** | **Data Quality and Integrity** |
| DI-1 | Data Quality |
| 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** |

| ID | Privacy Controls |
|---|---|
| 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.**

Simon K. Caines 3430973

Digitally signed by Simon K. Caines 3430973
Date: 2022.03.25 11:15:24 -04'00'

**Privacy Officer, Simon Caines**

Joseph Facciolli 148552

Digitally signed by Joseph Facciolli 148552
Date: 2022.03.25 07:14:12 -04'00'

**Information System Security Officer, Joseph Facciolli**

Gary W. Dameron 101941

Digitally signed by Gary W. Dameron 101941
Date: 2022.03.25 06:41:05 -04'00'

**Information System 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).

https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf

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