Privacy Impact Assessment for the VA IT System called:

Enrollment Database – Income Verification Matching

Veteran Experience Services – Eligibility and Enrollment

Date PIA submitted for review:

March 4, 2020

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Rita Grewal</td>
<td><a href="mailto:Rita.Grewal@va.gov">Rita.Grewal@va.gov</a></td>
<td>202-632-7861</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Howard Knight</td>
<td><a href="mailto:Howard.Knight@va.gov">Howard.Knight@va.gov</a></td>
<td>404-828-5340</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Doug Smith</td>
<td><a href="mailto:Doug.Smith2@va.gov">Doug.Smith2@va.gov</a></td>
<td>512-326-7845</td>
</tr>
</tbody>
</table>
Abstract

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

Enrollment Database – Income Verification Matching (EDB) uses Federal Tax Information (FTI) to conduct Means Testing and Income Verification Matching to determine the level of medical care benefits package from VA.

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.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- 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?
- Does the system use cloud technology? 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.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
- 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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?
Enrollment Database – Income Verification Matching (EDB) is a web-based application for the Health Eligibility Center (HEC) in Atlanta, Georgia. Analysts at HEC use the system to perform annual income verification of the Veteran for eligibility. HEC performs yearly Means Test on all Veterans whose eligibility is based on income. Each year analysts verify the income for an adjudicated decision to determine copay status. A message then goes to Enrollment System (ES, aka ESR) through the continuous enrollment rules engine to determine eligibility for enrollment. The results of the conversion are reported back to the Veteran’s VA Medical Center treating facility. The EDB application produces letter correspondence to assist the analysts in gathering information from the Veteran and to inform the Veteran of any changes in their eligibility status.

The expected number of individuals whose information is being used in the system is 10 million. The information is used to verify Veterans enrollment eligibility within the Veterans Health Administration (VHA) healthcare system.

Data Flow Description - EDB contains demographic and financial data in the database. EDB sends and receives Federal Tax Information (FTI) to/from the Internal Revenue Service and Social Security Administration. This FTI is used to conduct Means Testing and Income Verification Matching to determine level of medical care benefits package from VA. Information derived from FTI is used to support decisions information to the VA Medical Center facilities. HEC Atlanta and AITC generate the Communication Letters for the EDB system.

The system is a web-based application for the HEC facility staff in Atlanta, GA. Access is limited to the VA Intranet and customer use is controlled within the application. The data connection between Austin and the HEC is a VA line internal to the VA network. The servers accessing the data have server certificates issued through the VA Public Key Infrastructure (PKI) and VeriSign. Data passed from server to end customer is through secure client-server communications via the Secure Sockets Layer (SSL) protocol.

EDB shares data with the Social Security Administration (SSA) and the Internal Revenue Service (IRS). EDB also communicates with VA Medical Centers through Veterans Health Information Systems and Technology Architecture (VistA). Data from EDB is used by Enrollment System Redesign (ESR) as part of its Enrollment and Eligibility Service. Both ESR and VistA are internal VA systems.

Veterans' Health Care Eligibility Reform Act of 1996, Public Law 104-262; Title 38 U.S.C. Sections 1705, 1710, 1712 and 1722; Title 38 U.S.C Sections 5317 and 5319; Title 26 U.S.C. Section 6103 (I)(7) provide the legal authority for operating the EDB components. VA gathers or creates these records in order to enable it to administer statutory benefits programs to Veterans, Service members, reservists, and their spouses, surviving spouses, and dependents, who file claims for a wide variety of Federal Veteran’s benefits administered by VA. Applicable SORNs include 89VA10NB “Income Verification Records – VA” and 147VA10NF1 “Enrollment and Eligibility Records–VA.”

With the SSA, there is "Social Security Number Verification Information Exchange Agreement between the Social Security Administration and the Department of Veterans Affairs, Veterans Health Administration, Health Eligibility Center" which is Information Exchange Agreement #808. That agreement is extended through the use of SSA-1235 Reimbursable Agreements.
**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/](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.*

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
- Other Unique Identifying Number (list below)

Financial information [tax returns, net income and gross income for each year Veteran served], Military service information [branch of service, discharge type and discharge date], Veteran associates [next of kin, family members, their contact information and dependent information], Eligibility status, Enrollment status, Demographic information, Gender, Dependents and Employer information.

EDB Calculations [Means test, Means test threshold amount, income year of means test]

**PII Mapping of Components**

Enrollment Database (EDB) – Income Verification Matching (IVM) consists of five key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by EDB and the reasons for the collection of the PII are in the table below.
PII Mapped to Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database servers</td>
<td>Yes</td>
<td>Yes</td>
<td>Identification information [Name, Social Security Number (SSN), date of birth, address, phone and e-mail address] Financial information [Tax Identification Number (TIN), tax returns, net income and gross income for each year Veteran enrolled] Military Service information [branch of service, discharge type and discharge date] Veterans associates [next of kin, family members, their contact information and dependent information] Eligibility status, Enrollment status, Demographic information, Gender, Dependents and Employer information. EDB Calculations [Means test, Means test threshold amount, income year of means test]</td>
<td>Means Testing and Income Verification Matching</td>
<td>Restricted user access list, PIV authentication</td>
</tr>
<tr>
<td>Application servers</td>
<td>Yes</td>
<td>No</td>
<td>Identification information, Financial information, Military Service information, Veterans associates, Eligibility status, Enrollment status, Demographic information, Gender, Dependents and Employer information and EDB Calculations</td>
<td>Means Testing and Income Verification Matching</td>
<td>Restricted user access list, PIV authentication</td>
</tr>
</tbody>
</table>
### 1.2 What are the sources of the information in the system?

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

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

PII is pulled from VistA into Enrollment Database to ensure that the right information is being used to analyze and verify Veterans enrollment eligibility within the VHA healthcare system. More information is received from the Internal Revenue Service (IRS) and Social Security Administration (SSA) to determine an individual Veteran’s eligibility. EDB sends and receives Federal Tax Information (FTI) to/from the IRS and SSA. This FTI is used to conduct Means Testing and Income Verification Matching to determine level of medical care benefits package from VA. Information derived from FTI is used to support decisions information to the VA Medical Center facilities. Information is also gathered through letter correspondence with Veterans.

### 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.

Some information is received via electronic transmission from VistA, the IRS and the SSA. EDB creates its own data by conducting Means Testing and Income Verification Matching based on the FTI data from the IRS and SSA. Letter correspondence is used to gather information from Veterans.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose.

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

The purpose of the information being used is to analyze and verify Veterans enrollment eligibility within the VHA healthcare system. Each year analysts take the data reported by a Veteran and compare it to the information received from the IRS and SSA to determine an individual Veteran’s eligibility. The Means Test results are reported back to the Veteran’s VA Medical Center treating facility. EDB produces letter correspondence to assist the analysts in gathering information from the Veteran and also to inform the Veteran of any changes in their eligibility status.

1.5 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.

Information imported to EDB has its accuracy verified by the original source; VistA, IRS and SSA data is presumed to be accurate upon import by EDB. Information provided by individuals through correspondence is presumed accurate as it is from the authoritative source. Prior to any award or entitlement authorization(s) by EDB, the veteran record is manually reviewed and data validated to ensure correct entitlement has been approved.

1.6 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.

Veterans' Health Care Eligibility Reform Act of 1996, Public Law 104-262; Title 38 U.S.C. Sections 1705, 1710, 1712 and 1722; Title 38 U.S.C Sections 5317 and 5319; Title 26 U.S.C. Section 6103 (I)(7) provide the legal authority for operating the EDB components. VA gathers or creates these records in order to enable it to administer statutory benefits programs to Veterans, Service members, reservists, and their spouses, surviving spouses, and dependents, who file claims for a wide variety of Federal Veteran’s benefits administered by VA. With the SSA, there is "Social Security Number Verification Information Exchange Agreement between the Social Security Administration and the Department of Veterans Affairs, Veterans Health Administration, Health Eligibility Center" which is Information Exchange Agreement #808. That agreement is extended through the use of SSA-1235 Reimbursable Agreements.

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

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

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?
Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current? This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

**Privacy Risk:** EDB uses Personally Identifiable Information (PII) and Federal Tax Information (FTI). If this information were to be breached or accidentally leaked to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is being used in the EDB system.

**Mitigation:** Only information relevant to performing Means Testing and Income Verification Matching is collected. Correspondence with the Veteran may occur if additional details are needed. Only selected users have access to the information. The Department of Veterans Affairs is careful to only collect the information necessary to accomplish EDB’s mission. By only collecting the minimum necessary information, the VA is better able to protect the individual’s information.

Section 2. Uses of the Information

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

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

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

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

The information being used is to analyze and verify Veterans enrollment eligibility within the VHA healthcare system.

- Identification information [Name, Social Security Number (SSN), date of birth, address, phone and e-mail address] – identification – reporting - internal and external
- Demographic Data – reporting – statistical – internal and external
- Gender – identification – reporting – statistical data – internal and external
- Dependents – identification – reporting – statistical data – internal and external
- Employer information – reporting – statistical data – internal and external
- Eligibility Status - identification – reporting – statistical data – internal and external
• Enrollment Status: Success/Rejection - internal
• Military service information [branch of service, discharge type and discharge date] - statistical data – reporting – internal and external
• Veteran associates [next of kin, family members, their contact information and dependent information] - identification – reporting – statistical data – internal and external
• Financial Information [Tax Identification Number (TIN), tax returns, net income and gross income for each year Veteran enrolled] – statistical data – reporting – internal and external
• EDB Calculation [Means test, Means test threshold amount, income year of means test] – reporting – statistical data - internal

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

Analysts at HEC use the EDB system to perform annual income verification of the Veteran for eligibility. HEC performs yearly Means Test on all Veterans whose eligibility is based on income. Each year analysts verify the income for an adjudicated decision to determine copay status. A message then goes to Enrollment System (ES, aka ESR) through the continuous enrollment rules engine to determine eligibility for enrollment. The results of the conversion are reported back to the Veteran’s VA Medical Center treating facility. The EDB application produces letter correspondence to assist the analysts in gathering information from the Veteran and to inform the Veteran of any changes in their eligibility status. All code and algorithms are written by the VA.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?
Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

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

**Principle of Use Limitation:** Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

The System of Record Notice (SORN) defines the information collected from Veterans, use of the information and how the information is accessed and stored. The information collected is used for determining eligibility. The SORNs for the EDB system are:
89VA10NB SORN: Income Verification Records- VA

147VA10NF1 SORN: Enrollment and Eligibility Records-VA
https://www.govinfo.gov/content/pkg/FR-2016-07-14/pdf/2016-16640.pdf

The security controls for EDB’s high impact system cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The EDB application team has implemented the required security controls based on the tailoring guidance of National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4. VA Directives and Handbooks govern how Veterans’ information is used, stored, and protected.

**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.

- Identification information [Name, Social Security Number (SSN), date of birth, address, phone and e-mail address]
- Demographic Data
- Gender
- Dependents
- Employer information
- Eligibility Status
- Enrollment Status: Success/Rejection
- Military service information [branch of service, discharge type and discharge date]
- Veteran associates [next of kin, family members, their contact information and dependent information]
- Financial Information [Tax Identification Number (TIN), tax returns, net income and gross income for each year Veteran enrolled]
- EDB Calculation [Means test, Means test threshold amount, income year of means test]

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

Paper records are destroyed after they have been accurately scanned on optical disks. Optical disks or other electronic medium are deleted when all phases of the veteran’s appeal rights have ended (ten years after the income year for which the means test verification was conducted). Data received via Connect Direct from SSA and the IRS are destroyed 30 days after the data has been validated as being a good copy of the original data. Summary reports and other output reports are destroyed when no longer needed for current operation. Regardless of the record medium, no records are retired to a Federal records center.

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.

Record Control Schedule (RCS) 10-1 [https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf](https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf)


### 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

Per the Record Control Schedule (RCS) 10-1, Health Eligibility Center (HEC) Records, Code 1250:

1250.1; Health Eligibility Center (HEC) Records. Paper and electronic records of veterans who have applied for medical benefits at VA health care facilities, including data on the veterans’ spouses. The records contain identifying information including name, address, date of birth, social security number, current eligibility category, family information, including spouse and dependent(s) name, address, social security number; employment information on veteran and spouse including occupation, employer(s) name(s) and address(es); financial information including family income, assets, expenses, debts; and third-party health plan contract information including health insurance carrier name and address, policy number and time period covered by the policy; facility location(s) where treatment is provided, type of treatment provided, i.e., inpatient or outpatient, and length of stay or number of visits.

Temporary; destroy 7 year(s) after the income year for which the means test verification was conducted, when all phases of veteran’s appeal rights have ended. If an appeal is file retain records until all phases of the appeal have ended. (DAA-0015-2018-0001, item 0001)

1250.2; Tapes received from Social Security Administration (SSA) and Internal Revenue Service (IRS). Documents generated as a result of income verification by computer match with records from (IRS) and (SSA) and during the notification, verification and due process (appeals process) periods including initial verification letters, income verification forms, income difference/final letters, confirmation/due process letters, non-response confirmation letters, clarification letters, and all subpoena documentation.

Temporary; destroy 30 days after the data has been validated as being a true copy of the original data. (DAA-0015-2018-0001, item 0002)

1250.3; Summary Reports and other output records. All forms of individual correspondence generated during the process or provided to HEC by match participants include, but is not limited to, copies of death certification; discharge certification; DD 214, notice of separation; disability
award letter; IRS documents (i.e., forms 1040’s W-2’s, etc); State Welfare and food Stamp application; VA and other pension applicants; VA form 10-10, Application for Medical Benefits, and 10-10F, Financial Worksheet; workers compensation form; and various annual earnings statement as well as pay stubs.
Temporary; destroy when no longer needed (DAA0015-2018-0001, item 0003)

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

PII is not used for testing, research or training for the EDB system. Federal Tax Information (FTI) does not exist outside the Production environment.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

**Privacy Risk:** There is a risk that the information maintained by EDB could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.
Mitigation: To mitigate the risk posed by information retention, records are destroyed after they have been accurately scanned on optical disks. Optical disks or other electronic medium are deleted when all phases of the veteran’s appeal rights have ended (ten years after the income year for which the means test verification was conducted). Data received via Connect Direct to/from SSA and CD's/Tape from the IRS are destroyed 30 days after the data has been validated as being a good copy of the original data. Summary reports and other output reports are destroyed when no longer needed for current operation.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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.
### 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 privacy risk associated with maintaining PII is that sharing data within the Department of Veterans’ Affairs could happen and the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused or improperly disclosed.

**Mitigation:** The principle of need-to-know is strictly adhered to by EDB personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within. EDB will continue to maintain the requirement of proper credentials to communicate with these system interfaces. The system interfaces control the credentialing format and content. Access controls are in place at the wide area level through the CyberSecurity Operations Center (CSOC) gateways and firewalls. Authentication requires Personal Identify Verification (PIV) for two-factor authentication through the VA single-sign-on (SSOi) portal. Access is further controlled...
by the use of Active Directory (AD) thus making only VA-approved AD users able to be added as a user of the system. Further role-based security allows users to access only that data needed to accomplish their mission. All VA employees go through privacy and security training and system administrators must complete a system administration security course.

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: This question is #7 in the Privacy Threshold Analysis.

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 | List the purpose of information being shared / received / transmitted with | List the specific data element types such as PII/PHI that are shared/received with the Program or IT system | List the legal authority, binding agreement, SORN routine | List the method of transmission and the measures in |
Table:

<table>
<thead>
<tr>
<th>is shared/received with</th>
<th>the specified program office or IT system</th>
<th>use, etc. that permit external sharing</th>
<th>place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSA’s Enumeration Verification System (EVS)</td>
<td>Veteran eligibility determination</td>
<td>Social Security Number (SSN), Name, Date of Birth, Gender, annual income and Employer information.</td>
<td>Social Security Number Verification Information Agreement between SSA and VA VHA HEC #808 SSA-1235 Reimbursable Agreement</td>
</tr>
<tr>
<td>IRS’ Masterfile IBM Mainframe</td>
<td>Veteran eligibility determination</td>
<td>Social Security Number (SSN), Taxpayer Identification Number (TIN), Name and Financial Data [tax returns, net income, gross income for each year veteran enrolled]</td>
<td>VHA-IRS ISAMOU</td>
</tr>
</tbody>
</table>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

In order to protect veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:

1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a
Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments. Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing.

Follow the format below:

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

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

The VA provides policy stating sharing of information will only occur if there is a contract or agreement in place. EDB has signed agreements with the IRS and the SSA. Communications to these entities are via Connect:Direct site-to-site Virtual Private Network (VPN) connections. Access controls are in place at the wide area level through the CyberSecurity Operations Center (CSOC) and VA Trusted Internet Connection (TIC) gateways and firewalls. Additionally, all data is transferred using a FIPS 140-2 compliant encryption.

**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.

Public notice can be found in the SORN’s:
89VA10NB SORN: Income Verification Records- VA

147VA10NF1 SORN: Enrollment and Eligibility Records-VA
https://www.govinfo.gov/content/pkg/FR-2016-07-14/pdf/2016-16640.pdf

This Privacy Impact Assessment also serves as notice for the EDB system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs “after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.”

Many VA websites have a Privacy link at the bottom which links to the Privacy Service URL: https://www.oprm.va.gov/privacy/.

Privacy Notice statements exist in some letter correspondence as part of attached forms. The forms include:
- “HEC Form 410-1 VA National Income Thresholds,”
- “VA Form 21P-8049 Request for Details of Expenses,”
- “VA Form 21P-4185 Report of Income from Property or Business” and
- “VA Form 21P-4165 Pension Claim Questionnaire for Farm Income.”

See Appendix A-6.1 for the statements.

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 not decline or request that their information not be included as part of EDB’s process to determine eligibility and entitlement.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?
This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?

This question is related to privacy control IP-1, Consent

Individuals whose information is stored within EDB are not able to provide consent for specific uses of their information. Upon granting consent for the use of their information, that consent covers all uses within the system, both current and potential.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

**Principle of Use Limitation:** Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

**Privacy Risk:** There is a risk that members of the public may not know that the Enrollment Database (EDB) system exists within the Department of Veterans Affairs.

**Mitigation:** The VA mitigates this risk by providing the System of Record Notices (SORNs), the Privacy Impact Assessment, the Privacy link from most VA websites and the Privacy Notices included on individual forms included in correspondence.

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.

As outlined in SORN 89VA10NB Income Verification Records- VA (https://www.govinfo.gov/content/pkg/FR-2013-12-19/pdf/2013-30228.pdf) in the Record Access Procedures section, “Individuals seeking information regarding access to and contesting of income verification records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Suite 200, Atlanta, Georgia 30329.”

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.

As outlined in SORN 89VA10NB Income Verification Records- VA (https://www.govinfo.gov/content/pkg/FR-2013-12-19/pdf/2013-30228.pdf) in the Record Access Procedures section, “Individuals seeking information regarding access to and contesting of income verification records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Suite 200, Atlanta, Georgia 30329.”

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.
This Privacy Impact Assessment notifies users of the correction procedure as does the SORN 89VA10NB Income Verification Records - VA (https://www.govinfo.gov/content/pkg/FR-2013-12-19/pdf/2013-30228.pdf).

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

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

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

As outlined in SORN 89VA10NB Income Verification Records - VA (https://www.govinfo.gov/content/pkg/FR-2013-12-19/pdf/2013-30228.pdf) in the Record Access Procedures section, “Individuals seeking information regarding access to and contesting of income verification records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Suite 200, Atlanta, Georgia 30329.”

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 the individual accidentally provides incorrect information in their correspondence.

**Mitigation:** Individuals provide information directly to EDB. Any validation performed would merely be the individual personally reviewing the information before he/she provides it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indication to the VA that the new information supersedes the previous data.

### 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.

Users request access to the application through the HEC Access Request form and attest to being current on their annual VA Privacy, Information Security Awareness training and Rules of Behavior. The user’s supervisor must sign their approval on the form and the user’s Information Security Officer (ISO), after verifying the currency of the user training, signs their approval as well. The Health Eligibility Center (HEC) ISO must also give their approval for the user’s access. Then the HEC ISO forwards the user’s request to the EDB application administrator for their account to be created.

Per VA Directive and Handbook 0999 “Enterprise Directives Management (EDM)”, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains
individual training records for all personnel. This documentation and monitoring is performed through the use of VA’s Talent Management System (TMS).

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 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.

Contractors are prohibited from having access to the EDB Production system as part of the agreement with the IRS due to the presence of Federal Tax Information (FTI.)

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.

Annual Federal Tax Information (FTI) training is required by the IRS for those that work with FTI data. Users must watch a video and read two documents. Then, they must sign and turn in the IRS Tax Information Security Agreement.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA’s Talent Management System (TMS). After the user’s initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. System administrators are required to complete additional role- based training. Users with access to PHI are required to complete HIPAA privacy training annually.
8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. 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.

Enrollment Database has a full Authority to Operate (ATO) with an expiration date of January 15, 2021. The FIPS classification for EDB is High.
## Section 9. References

### Summary of Privacy Controls by Family

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

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

RITA K GREWAL
114938
Digitally signed by RITA K GREWAL 114938
Date: 2020.07.20 08:04:35 -04'00'

Privacy Officer, Rita Grewal

Knight, Howard
(HEC ISO)
Digitally signed by Knight, Howard (HEC ISO)
Date: 2020.07.20 08:19:06 -04'00'

Information Security Systems Officer, Howard Knight

Douglas W. Smith
364456
Digitally signed by Douglas W. Smith 364456
Date: 2020.07.20 10:11:55 -05'00'

Information System Owner, Doug Smith
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).

Veteran Final GMT/RX Letter and Veteran Final MT/RX Letter
On enclosure: HEC Form 410-1 VA National Income Thresholds

**HEC Form 410-1**

*Privacy Act Information:* VA is asking you to provide the information on this form under Title 38, United States Code, sections 1710, 1712, and 1722 in order to determine your eligibility for medical benefits. The information you supply may be verified through a computer matching program. VA may disclose the information that you put on the form as permitted by law. VA may make "routine use" disclosure for: 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. You do not have to provide the information to VA, but if you do not, we will be unable to process your request and serve your medical needs. Failure to furnish the information will not have any affect on any other benefits to which you may be entitled. If you give VA your Social Security Number, VA will use it to administer your VA benefits, to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.

Net Worth Letter
On enclosure: VA Form 21P-8049 Request for Details of Expenses

**Form 21P-8049 1**

*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, 5BVA21/22, Compensation, Pension, Education and Rehabilitation Records - VA, published in the Federal Register. You are required to respond to obtain or retain benefits. The requested information is considered relevant and necessary to determine entitlement to benefits. The responses you submit are considered confidential (58 U.S.C. 5701). Information submitted is subject to verifications through computer matching programs with other agencies. You are required to provide the Social Security number requested under 38 U.S.C. 5101(c)(1). VA may disclose Social Security numbers as authorized under the Privacy Act, and, specifically may disclose them for purposes stated above.

*Respondent Burden:* We need this information to determine entitlement to pension or parent's dependency and indemnity compensation (38 U.S.C. 1503 and 1315). Title 38, United States Code, allows us to ask for this information. We estimate that you will need an average of 15 minutes to review the instructions, find the information, and complete this form. VA cannot conduct or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed. Valid OMB control numbers can be located on the OMB Internet Page at www.reginfo.gov/public/do/PRAMain. If desired, you can call 1-800-827-1000 to get information on where to send comments or suggestions about this form.

On enclosure: VA Form 21P-4185 Report of Income from Property or Business
On enclosure: VA Form 21P-4165 Pension Claim Questionnaire for Farm Income