

**Privacy Impact Assessment - 2009 (Form) / VBA Rules Based Claims Processing - 2009 (Item)**

**PIA SECTIONS 1 - 4**

**Part I. Project Identification and Determination of PIA Requirement**

**1. PROJECT IDENTIFICATION:**

**1.1) Project Basic Information:**

*1.1.a) Project or Application Name:*

VBA Rules Based Claims Processing - 2009

*1.1.b) OMB Unique Project Identifier:*

029-00-01-14-01-1266-00.

*1.1.c) Project Description*

*Project description is pre-populated from Exhibit 300 Part I.A.8. You will not be able to edit the description on this form.*

The Veterans Benefit Administration (VBA) will invest in a web-enabled, Rules-Based Claims Processing (RBCP) initiative to improve claims processing and enhance customer service. RBCP will use business rules engine (BRE) technology and business process reengineering to support the delivery of business line benefits. BREs promote standardized decision making when the rules being assessed are grounded on objective, finite criteria. Many VA benefits are derived from objective law and regulation, making them ideal for RBCP. Automating the claims process with BRE technology will promote standardized decision making, reduce variances, and improve accuracy and claims processing timeliness, which should result in reduced claims inventory and administrative costs while improving productivity. VBA adjudicators will only need to work those claims that do not meet defined business rules. The RBCP solution will be fully compatible with service-oriented architecture to support the requirements of business processes and users, while satisfying VA enterprise architecture standards. RBCP will start with the following Education and Compensation & Pension (C&P) projects:

1. The Education Expert System (TEES) for adjudicating education claims.
2. The Burial Rules Based Claims Processing (Burial RBCP) application for adjudicating C&P burial benefits claims.
3. The Rating Veterans Service Representative Medical Evidence Rating Tool (MERT) for evaluating medical evidence related to C&P claims.

RBCP aligns with the following VA strategic Goals:

VA Goal 1, Objective 1.2 – Provide timely and accurate decisions on disability compensation claims to improve the economic status and quality of life of service-disabled veterans.

VA Goal 1, Objective 1.4 – Improve the standard of living and income status of eligible survivors of service members and service-disabled veterans through compensation, education, and insurance benefits.

VA Goal 2, Objective 2.2 – Enhance the ability of veterans and service members to achieve educational and career goals by providing timely and accurate decisions on education claims and continuing payments at appropriate levels.

VA Goal 3, Objective 3.2 – Provide eligible veterans and their survivors a level of income that raises their standard of living and sense of dignity by processing pension claims in a timely manner.

VA Goal 3, Objective 3.4 – Ensure that the burial needs of veterans and eligible family members are met.

*1.1.d) Additional Project Information (Optional)*

*The project description provided above should be a concise, stand-alone description of the project. Use this section to provide any important, supporting details.*

**1.2) Contact Information:**

**1.2.a) Person completing this document:**

**Title:**

Ivan Labombarbe

<b>Organization:</b>	OI&T OED VBIT Programs Plans and Control (PPC)
<b>Telephone Number:</b>	202-461-9980
<b>Email Address:</b>	ivan.labombarbe@va.gov
<b>1.2.b) Project Manager:</b>	
<b>Title:</b>	Rebecca Wells
<b>Organization:</b>	OI&T OED VBIT, Business Program Management Office (BPMO)
<b>Telephone Number:</b>	202-461-9135
<b>Email Address:</b>	rebecca.wells@va.gov
<b>1.2.c) Staff Contact Person:</b>	
<b>Title:</b>	Rhonda Jones
<b>Organization:</b>	VBA, Education Service (EDU)
<b>Telephone Number:</b>	202-461-9821
<b>Email Address:</b>	rhonda.jones1@va.gov

*ADDITIONAL INFORMATION: If appropriate, provide explanation for limited answers, such as the development stage of project.*

The Staff contact person for VBA, Compensation and Pensions, Brian Stephens phone 727-319-5807 and email brian.stephens@va.gov. The staff person for VBA Requirements is Kim Graves, phone 202-461-9374, email kim.graves@va.gov

## 2. DETERMINATION OF PIA REQUIREMENTS:

*A privacy impact assessment (PIA) is required for all VA projects with IT systems that collect, maintain, and/or disseminate personally identifiable information (PII) of the public, not including information of Federal employees and others performing work for VA (such as contractors, interns, volunteers, etc.), unless it is a PIV project. All PIV projects collecting any PII must complete a PIA. PII is any representation of information that permits the identity of an individual to be reasonably inferred by either direct or indirect means. Direct references include: name, address, social security number, telephone number, email address, financial information, or other identifying number or code. Indirect references are any information by which an agency intends to identify specific individuals in conjunction with other data elements. Examples of indirect references include a combination of gender, race, birth date, geographic indicator and other descriptors.*

2.a) Will the project collect and/or maintain personally identifiable information of the public in IT systems?

Yes

2.b) Is this a PIV project collecting PII, including from Federal employees, contractors, and others performing work for VA?

No

*If "YES" to either question then a PIA is required for this project. Complete the remaining questions on this form. If "NO" to both questions then no PIA is required for this project. Skip to section 14 and affirm.*

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

## Part II. Privacy Impact Assessment

<b>3. PROJECT DESCRIPTION:</b>
<i>Enter the information requested to describe the project.</i>
<i>3.a) Provide a concise description of why personal information is maintained for this project, such as determining eligibility for benefits or providing patient care.</i>
The mission of the Education Service is to provide financial assistance for education, training, certification, etc. generally in the form of monthly benefit payments, to veterans, active duty service persons, reservists, and certain eligible dependents of disabled or deceased veterans in recognition of their military service to this nation. The mission of C&P Service is to provide various monetary benefits to veterans, eligible dependents, and authorized claimants. There are three categories of C&P Service benefits: compensation benefits for veterans; income-based pension benefits for veterans and survivors; and non-income based benefits for survivors. RBCP will extract data from the VBA corporate database, collect additional data, and upload data to the VBA corporate database for the purpose of determining entitlement eligibility to VBA Education and C&P Service benefits.
<i>3.b) What specific legal authorities authorize this project, and the associated collection, use, and/or retention of personal information?</i>
Title 38, United States Code, Chapters 11, 13, 15, 30, 31, 32, and 35; U.S.C Section 3845; 10 U.S.C Chapter 1606 and 1607; Sections 901 and 903 Title 38 USC, Chapters 11 (Compensation), 15 (Pension) 23, (Burial); 38 CFR, Parts 3 (Adjudication) and 4(Schedule for Rating Disabilities).
<i>3.c) Identify, by selecting the appropriate range from the list below, the approximate number of individuals that (will) have their personal information stored in project systems.</i>
10,000,000 - 19,999,999
<i>3.d) Identify what stage the project/system is in: (1) Design/Planning, (2) Development/Implementation, (3) Operation/Maintenance, (4) Disposal, or (5) Mixed Stages.</i>
(1) Design/Planning
<i>3.e) Identify either the approximate date (MM/YYYY) the project/system will be operational (if in the design or development stage), or the approximate number of years that the project/system has been in operation.</i>
09/2011
<i>ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)</i>

<b>4. SYSTEM OF RECORDS:</b>
<i>The Privacy Act of 1974 (Section 552a of Title 5 of the United States Code) and VA policy provide privacy protections for employee or customer information that VA or its suppliers maintain in a System of Records (SOR). A SOR is a file or application from which personal information is retrieved by an identifier (e.g. name, unique number or symbol). Data maintained in a SOR must be managed in accordance with the requirements of the Privacy Act and the specific provisions of the applicable SOR Notice. Each SOR Notice is to be published in the Federal Register. See VA Handbook 6300.5 "Procedures for Establishing &amp; Managing Privacy Act Systems Of Records", for additional information regarding Systems of Records.</i>
<i>4.a) Will the project or application retrieve personal information on the basis of name, unique number, symbol, or other identifier assigned to the individual?</i>
If "No" then skip to section 5, 'Data Collection'.
Yes
<i>4.b) Are the project and/or system data maintained under one or more approved System(s) of Records?</i>
IF "No" then SKIP to question 4.c.
Yes
<i>4.b.1) For each applicable System of Records, list:</i>
<i>(1) The System of Records identifier (number),</i>
58VA21/22/28
<i>(2) The name of the System of Records, and</i>
Compensation, Pension, Education and Rehabilitation Records-VA
<i>(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL).</i>
VBA Records Control Schedule (RCS) at <a href="http://www.va.gov/oit/cio/foia/systems_of_records.asp">http://www.va.gov/oit/cio/foia/systems_of_records.asp</a>

**IMPORTANT:** For each applicable System of Records Notice that is not accessible via a URL: (1) Provide a concise explanation of why the System of Records Notice is not accessible via a URL in the "Additional Information" field at the end of this section, and (2) Send a copy of the System of Records Notice(s) to the Privacy Service.

4.b.2) Have you read, and will the application comply with, all data management practices in the System of Records Notice(s)?

Yes

4.b.3) Was the System(s) of Records created specifically for this project, or created for another project or system?

Created for another project or system

If created for another project or system, briefly identify the other project or system.

Created for multiple business lines to include Compensation & Pension, Vocational Rehabilitation & Employment and Education Service

4.b.4) Does the System of Records Notice require modification?

If "No" then skip to section 5, 'Data Collection'.

Modification of the System of Records is NOT Required.

4.b.5) Describe the required modifications.

4.c) If the project and/or system data are not maintained under one or more approved System(s) of Records, select one of the following and provide a concise explanation.

Explanation:

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## PIA SECTION 5

### Project Name

VBA Rules Based Claims Processing - 2009

### 5. DATA COLLECTION:

#### 5.1 Data Types and Data Uses

Identify the types of personal information collected and the intended use(s) of that data:

a) Select all applicable data types below. If the provided data types do not adequately describe a specific data collection, select the "Other Personal Information" field and provide a description of the information.

b) For each selected data type, concisely describe how that data will be used.

**Important Note:** Please be specific. If different data types or data groups will be used for different purposes or multiple purposes, specify. For example: "Name and address information will be used to communicate with individuals about their benefits, while Name, Service, and Dependent's information will be used to determine which benefits individuals will be eligible to receive. Email address will be used to inform individuals about new services as they become available."

Yes

**Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc.)**

Specifically identify the personal information collected, and describe the intended use of the information.

Name, Address, Social Security Number, Family/Dependents, Marital Status, Medical Status, Birth Information, Death Information, Telephone, Email, Financial is used to communicate with the Veteran about his/her benefits, to notify of change in account status and advise about new options.

No	<b>Other Personal Information of the Veteran or Primary Subject</b>
----	---

*Specifically identify the personal information collected, and describe the intended use of the information.*

Yes	<b>Dependent Information</b>
-----	------------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

Veteran Dependent Data (personal information including name and address, age, school status, relationship to the veteran, medical status, Social Security Number, Telephone) is used to (1) communicate with the Veteran about his/her benefits, to notify of change in account status and advise about new options and (2) to determine eligibility and process entitlement.

Yes	<b>Service Information</b>
-----	----------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

Department of Defense provides (1) Service Data: reserve and guard participation, retired pay or severance pay, hazardous agent exposure, branch of service, active duty date, released date, type of discharge, separation reason. This information is used to determine eligibility and process entitlement.

Yes	<b>Medical Information</b>
-----	----------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

The Department of Defense provides military clinical records and government health records.  
 The Veterans Health Administration provides VA medical records.  
 Claimants submit private medical information.  
 VBA uses the medical information to determine entitlement to various VBA benefits, including Education and C&P Service benefits.  
 This information is used to determine eligibility and process entitlement.

Yes	<b>Criminal Record Information</b>
-----	------------------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

State Police Records: Incarceration at state or local facility, fugitive felon status, investigative reports for some accident. These records are used to determine if eligible for benefits during imprisonment at local and Federal facilities

Yes	<b>Guardian Information</b>
-----	-----------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

Guardianship Information may include name ,address, telephone number, court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accountings. This information is used to communicate with guardians regarding the veteran or his/her dependent and court proceedings, field examinations, appointments and annual accountings.

Yes	<b>Education Information</b>
-----	------------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

Education program approval information on approved courses, effective dates, types of training, training type is used during administering education benefits to ensure veterans are in compliance with applicable laws and regulations required to receive benefits.

No	<b>Rehabilitation Information</b>
----	-----------------------------------

*Specifically identify the personal information collected, and describe the intended use of the information.*

No	<b>Other Personal Information (specify):</b>
----	--

*The "Other Personal Information" field is intended to allow identification of collected personal information that does not fit the provided categories. If personal information is collected that does not fit one of the provided categories, specifically identify this information and describe the intended use of the information.*

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

## 5.2 Data Sources

*Identify the source(s) of the collected information.*

*a) Select all applicable data source categories provided below.*

*b) For each category selected:*

*i) Specifically identify the source(s) - identify each specific organization, agency or other entity that is a source of personal information. ii) Provide a concise description of why information is collected from that source(s). iii) Provide any required additional clarifying information.*

*Your responses should clearly identify each source of personal information, and explain why information is obtained from each identified source. (Important Note: This section addresses sources of personal information; Section 6.1, "User Access and Data Sharing" addresses sharing of collected personal information.)*

*Note: PIV projects should use the "Other Source(s)" data source.*

Yes	<b>Veteran Source</b>
-----	-----------------------

*Provide a concise description of why information is collected from Veterans. Provide any required additional, clarifying information.*

Veteran Personal data (Name, Address, Social Security Number, Family/Dependents, Marital Status, Medical Status, Birth Information, Death Information, Financial, Telephone, Email) and Veteran Dependent Data (personal information including name and address, age, school status, relationship to the veteran, medical status, Telephone, Social Security Number) is used to (1) communicate with the Veteran about his/her benefits, to notify of change in account status and advise about new options and (2) to determine eligibility and process entitlement.

Yes	<b>Public Source(s)</b>
-----	-------------------------

*i) Specifically identify the Public Source(s) - identify the specific organization(s) or other entity(ies) that supply personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.*

Educational institutions (schools) provide information on veterans' enrollment and attendance. Veterans Service Organizations (VSO), Attorneys, Funeral Home Directors, claimants, and other designated claimant VA representatives holding a valid VA power of attorney submit information on behalf of a claimant. Information is used to process claims for education and C&P benefits.

Yes	<b>VA Files and Databases</b>
-----	-------------------------------

*i) Specifically identify each VA File and/or Database that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.*

Information such as Account History (case/account number, identity of beneficiary, eligibility determination information, benefit information), Education Program Approval Information (approved courses, effective dates, types of training, training type), and Rehabilitation Program Approval Information (institution certifications, licenses, approval information) is used to determine eligibility and process entitlement.

Yes	<b>Other Federal Agency Source(s)</b>
-----	---------------------------------------

*i) Specifically identify each Federal Agency that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.*

National Service Life Insurance, Veterans Mortgage Life Insurance, Veterans Government Life Insurance, and Social Security Administration (verifies if Veteran is deceased), Department of Defense provides (1) Service Data: reserve and guard participation, retired pay or severance pay, hazardous agent exposure, branch of service, active duty date, released date, type of discharge, separation reason; and (2) Medical Records: Military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations. Other Federal agencies that provide information that is used to determine eligibility and to process entitlements are the Department of Labor, Department of Treasury, Federal Parent Locator Service, General Accounting Office, Office of Inspector General, Office of Personnel Management, and Bureau of Census, Federal Housing Administration, Internal Revenue Service, Department of Housing and Urban Development. Bureau of Prisons provide Police Records: Incarceration at federal state or local facility, fugitive felon status, investigative reports for some accident. Benefits are suspended for incarcerated veterans.

Yes	<b>State Agency Source(s)</b>
-----	-------------------------------

*i) Specifically identify each State Agency that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.*

Bureau of Prisons provide Police Records: Incarceration at federal state or local facility, fugitive felon status, investigative reports for some accident. Benefits are suspended for incarcerated veterans. State Veterans Service Organization, State operated nursing homes to determine entitlement to VA benefits.

No	<b>Local Agency Source(s)</b>
----	-------------------------------

*i) Specifically identify each Local Agency (Government agency other than a Federal or State agency) that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.*

Yes	<b>Other Source(s)</b>
-----	------------------------

*i) If the provided Data Source categories do not adequately describe a source of personal information, specifically identify and describe each additional source of personal information. ii) For each identified data source, provide a concise description of why information is collected from that source. iii) Provide any required additional, clarifying information.*

American Red Cross and Blind American Veterans provide information that is used to determine eligibility and to process entitlements. Blind American Veterans also exchange information in their capacity as fiduciaries for the veteran or the veteran's dependents. Guardianship Information may include court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accountings. It may also include Veteran Dependent Data: Personal information including name and address, age, school status, relationship to the veteran, medical status, telephone, email, Social Security Number.

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

### 5.3 Collection Methods

*Identify and describe how personal information is collected:*

*a) Select all applicable collection methods below. If the provided collection methods do not adequately describe a specific data collection, select the "Other Collection Method" field and provide a description of the collection method. b) For each collection method selected, briefly describe the collection method, and provide additional information as indicated.*

Yes	<b>Web Forms:</b>	Information collected on Web Forms and sent electronically over the Internet to project systems.
-----	-------------------	--

*Identify the URL(s) of each Web site(s) from which information will be submitted, and the URL(s) of the associated privacy statement. (Note: This question only applies to Web forms that are submitted online. Forms that are accessed online, printed and then mailed or faxed are considered "Paper Forms.")*

The VBA website is <http://www.vba.va.gov>; with the specific online form located at

<http://vabenefits.vba.va.gov/vonapp/main.asp>. The available forms located at this site are: V A Form 22-1990, Application for Education Benefits, VA Form 22-1995, Request for Change of Program or Place of Training, VA Form 22-5490, Application for Survivors' and Dependents' Educational Assistance, VA Form 22-5495, Request for Change of Program or Place of training Survivors' and Dependents' Educational Assistance. Applicants are required to complete form 21-4142, Authorization and Consent to Release Information to the Department of Veterans Affairs (V A). All VBA benefit forms are located at <http://www.va.gov/vaforms/>

The URL of the associated privacy statement is: <http://www.va.gov/privacy/>

The Veterans Online Application (VONAPP) is used to electronically submit claims for Education and C&P Service benefits. The VONAPP website is: <http://vabenefits.vba.va.gov/vonapp/main.asp>

Yes	<b>Paper Forms:</b>	Information collected on Paper Forms and submitted personally, submitted via Postal Mail and/or submitted via Fax Machine.
-----	---------------------	--

*Identify and/or describe the paper forms by which data is collected. If applicable, identify standard VA forms by form number.*

VA Form 22-1990, Application for Education Benefits; Form 21-4142, Authorization and Consent to Release Information to the Department of Veterans Affairs (V A), VA Form 22-8800, Request for VA Forms and Publications, VA Form 21-674, Request for Approval of School Attendance, VA Form 21-674b, School Attendance report, VA Form 21-686c, Declaration of status of dependents, VA Form 21-4138, Statement in Support of Claim, VA Form 22-1990, Application for VA Educational Benefits, VA Form 22-1990t, Application and Enrollment Certification for Individualized Tutorial Assistance, VA Form 22-1995, Request for Change of Program or Place of Training, VA Form 22-1999, VA Form 22-1999b, Notice of Change in Student Status; Correspondence Courses, VA Form 22-1999c, Certificate of Affirmation of Enrollment Agreement, VA Form 22-5490, Application for Survivors' and Dependents' Educational Assistance, VA Form 22-5495, Request for Change of Program or Place of training Survivors' and Dependents' Educational Assistance, VA Form 8690, Work-Study, VA Form 8691, Application for Work Study Allowance, VA Form 22-8794, School Officials Form, VA Form 22-8873, Supplemental Information for Change of Program or Reenrollment After Unsatisfactory Attendance, Conduct or Progress, VA Form 22-8889, Application for Educational Assistance Test Program Benefits, VA Form 24-0296, Direct Deposit Enrollment, VA Form 24-5281, Application for Refund of Educational Contributions, VA Form 21-530, Application for Burial Benefits, VA Form 21-526, Application for C&P Benefits, VA Form 21-4138, Statement in Support of Claim.

Yes	<b>Electronic File Transfer:</b>	Information stored on one computer/system (not entered via a Web Form) and transferred electronically to project IT systems.
-----	----------------------------------	--

*Describe the Electronic File Transfers used to collect information into project systems. (Note: This section addresses only data collection – how information stored in project systems is acquired. Sharing of information stored in project systems and data backups are addressed in subsequent sections.)*

VADIR - VA DOD Data Identification Repository issued to transfer data on veterans from DOD to VA. Interchange of data between new project IT systems and the following IT systems is anticipated: VETSNET, BDN, BIRLS/VADS, and VVA.

Yes	<b>Computer Transfer Device:</b>	Information that is entered and/or stored on one computer/ system and then transferred to project IT systems via an object
		or device that is used to store data, such as a CD-ROM, floppy disk or tape.

*Describe the type of computer transfer device, and the process used to collect information.*

Educational institutions submit electronic information (via the VA-ONCE program) to the VA on veterans' enrollment, attendance, credits, term, and courses using VA Form 22-1999, Request for Change of Program or Place of Training and VA Form 22-1999b, and Notice of Change in Student Status. The veterans can also submit electronic information (via the

WAVE program) certifying their school attendance. SSA, DoD (Defense Finance and Accounting Service (DFAS) and Defense Manpower Data Center (DMDC)) and Department of Treasury matching systems is used for verifying veteran data and income. This information is used to process claims for Education and C&P Service benefits.

Yes	<b>Telephone Contact:</b>	Information is collected via telephone.
-----	---------------------------	---

*Describe the process through which information is collected via telephone contacts.*

The VBA toll free number for veterans is 1-800-827-1000. They can verify their benefits. 1-877-823-2378 and 1-888-442-4551 is Education IVR. Veterans can certify their school attendance as well as provide any other information VBA needs to process their claim. Veterans can provide information about their claim on the telephone; VBA representatives will record the information on VA Form 119, Report of Contact. This data is used to process claims for Education and C&P Service benefits.

No	<b>Other Collection Method:</b>	Information is collected through a method other than those listed above.
----	---------------------------------	--

*If the provided collection method categories do not adequately describe a specific data collection, select the "Other Collection Method" field and specifically identify and describe the process used to collect information.*

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

#### 5.4 Notice

*The Privacy Act of 1974 and VA policy requires that certain disclosures be made to data subjects when information in identifiable form is collected from them. The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.*

**5.4.a) Is personally identifiable information collected directly from individual members of the public and maintained in the project's IT systems?**

Yes

*Note: If you have selected NO above, then SKIP to Section 5.5, 'Consent'.*

**5.4.b) Is the data collection mandatory or voluntary?**

Voluntary

**5.4.c) How are the individuals involved in the information collection notified of the Privacy Policy and whether provision of the information is mandatory or voluntary?**

Privacy policy is provided on the website (<http://www.va.gov/privacy/index.htm>). The site specifically states, "You do not have to give us personal information to visit our site. We will collect personally identifiable information (name, email address, Social Security number, or other unique identifier) only if specifically and knowingly provided by you."

Individuals provide consent through the use of signed consent forms, through notarized indication of a Power of Attorney or through authorized or verified signature. Regardless of the media, consent is collected through submission of electronic forms marking consent approval, verbal authorization, or through Memorandums of Understanding with business partners. VA requires that all consent forms be documented and authorized or verified signatures are required. In addition, limited consent is provided as part of routine use as specified in various Privacy Act System of Record notifications.

The collection site provides a link to VA's privacy and security statement located at <http://www.va.gov/privacy/>. This statement discloses that "the privacy of our customers has always been of utmost importance to the Department of

Veterans Affairs." It also explains the VA's Internet privacy policy.

The collection site also provides a link to VA's information on the Freedom of Information Act located at <http://www.va.gov/foia/>. The site also provides a link to VA Form 21-4142, Authorization and Consent to Release Information to the Department of Veterans Affairs (VA), which is a requirement.

5.4.d) Is the data collection new or ongoing?

Ongoing

5.4.e.1) If personally identifiable information is collected online, is a privacy notice provided that includes the following elements? (Select all applicable boxes.)

No	<b>Not applicable</b>
No	<b>Privacy notice is provided on each page of the application.</b>
Yes	<b>A link to the VA Website Privacy Policy is provided.</b>
Yes	<b>Proximity and Timing: the notice is provided at the time and point of data collection.</b>
Yes	<b>Purpose: notice describes the principal purpose(s) for which the information will be used.</b>
Yes	<b>Authority: notice specifies the legal authority that allows the information to be collected.</b>
Yes	<b>Conditions: notice specifies if providing information is voluntary, and effects, if any, of not providing it.</b>
Yes	<b>Disclosures: notice specifies routine use(s) that may be made of the information.</b>

5.4.e.2) If necessary, provide an explanation on privacy notices for your project:

5.4.f) For each type of collection method used (identified in Section 5.3, "Collection Method"), explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

Note: if PII is transferred from other projects, explain any agreements or understandings regarding notification of subjects.

Yes	<b>Web Forms:</b>
-----	-------------------

Explain:

a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.

The subjects will be told in electronic notice:

PRIVACY ACT INFORMATION: No allowance of compensation or pension may be granted unless this form is completed fully as required by law (38 U.S.C. 5101). The responses you submit are considered confidential (38 U.S.C. 5701). VA may disclose the information that you provide, including Social Security numbers, outside VA if the disclosure is authorized under the Privacy Act, including the routine uses identified in the VA system of records, 58VA21/22 Compensation, Pension, Education, and Rehabilitation Records - VA. The requested information is considered relevant and necessary to determine maximum benefits under the law. Information submitted is subject to verification through computer matching programs with other agencies. VA may make a "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. The requested information is

considered relevant and necessary to determine maximum benefits under the law. Information that you furnish may be utilized in computer matching programs with other Federal or state agencies for the purpose of determining your eligibility to receive VA benefits, as well as to collect any amount owed to the United States by virtue of your participation in any benefit program administered by the Department of Veterans Affairs.

**Income and employment information:** The income and employment information furnished by you will be compared with information obtained by VA from the Secretary of Health and Human Services or the Secretary of the Treasury under clause (viii) of section 6103 (1)(7)(D) of the Internal Revenue Code of 1986.

**Social Security information:** You are required to provide the Social Security number(s), 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 the purposes stated above.

You do not have to give us personal information to visit our site. We will collect personally identifiable information (name, email address, Social Security number, or other unique identifier) only if specifically and knowingly provided by you. Personally identifying information you provide will be used only in connection with VA programs and services or for such other purposes as are described at the point of collection. Information is collected for statistical purposes and VA sometimes performs analyses of user behavior in order to measure customer interest in the various areas of our site. We do not give, sell or transfer any personal information to a third party. We may enable "cookies." A "cookie" is a file placed on your personal computer's hard drive by a Web site that allows it to monitor your use of the site.

Yes	<b>Paper Forms:</b>
-----	---------------------

*Explain:*

*a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.*

The subjects will be told in writing:  
**Privacy Act Notice:** 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 5, Code of Federal Regulations 1.526 for routine uses (i.e., allowing VA to send educational forms or letters with a veteran's identifying information to the veteran's school or training establishment to (1) assist the veteran in the completion of claims forms or (2) for VA to obtain further information as may be necessary from the school for VA to properly process the veteran's education claim or to monitor his or her progress during training) as identified in the VA system of records, 58VA21/22, Compensation, Pension, Education and Rehabilitation Records - VA, and published in the Federal Register. Your obligation to respond is required to obtain or retain education benefits. 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 benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a 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 the maximum benefits under the law. Payment of education benefits cannot be made unless the information is furnished as required by existing law (38 U.S.C. 3471). 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.

**Important Notice About Information Collection:** We need this information to determine your eligibility to education benefits (38 U.S.C. 3471). Title 38, United States Code, allows us to ask for this information. We estimate that you will need an average of 54 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.whitehouse.gov/library/omb/OMBINVC.html#VA](http://www.whitehouse.gov/library/omb/OMBINVC.html#VA) . If desired, you can call 1-888-GI-BILL1 (1-888-442-4551) to get information on where to send comments or suggestions about this form.

Yes	<b>Electronic File Transfer:</b>
-----	----------------------------------

*For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to notify subjects regarding:*

*a) What they will be told about the information collection? b) How the message will be conveyed (e.g. written notice, electronic notice if web-based collection, etc.)? c)How a privacy notice is provided?*

Interchange occurs between various VA IT applications, including VETSNET, BDN, BIRLS/VADS, and VVA. The data is protected under the Privacy Act. All VBA users with access to the applications complete a Rules of Behavior and annual privacy training that describes the protection afforded the data under the Privacy Act.

Yes	<b>Computer Transfer Device:</b>
-----	----------------------------------

*For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to notify subjects regarding:*

*a) What they will be told about the information collection? b) How the message will be conveyed (e.g. written notice, electronic notice if web-based collection, etc.)? c) How a privacy notice is provided?*

Subjects are told that information to be collected is voluntary and protected under the Privacy Act. The data will be shared only for routine purposes to process a VA claim; non-routine disclosures require the veteran's consent.

**Privacy Act and Paperwork Reduction Act Notice**

When asking people for personal information, the Department of Veterans Affairs (VA) must follow the Privacy Act of 1974, the Paperwork Reduction Act of 1995, and Office of Management and Budget (OMB) regulations.

Why do we need this information? We need this information to determine your continuing eligibility for education benefits and the proper amount payable.

What authority do we have to collect this information? Title 38 United States Code, section 3684 authorizes us to collect this information. You don't have to complete this form and we can't require you to respond unless this form's OMB Control Number (2900-0465) is valid. The OMB Internet Home Page ([www.whitehouse.gov/OMB/index.html](http://www.whitehouse.gov/OMB/index.html)) shows the OMB Control Numbers for VA approved forms.

What happens if you don't give us this information? If you don't give us this information, we may be unable to give you the benefit you're asking for. Giving this information is required for receiving a benefit.

Can we give this information to people outside VA? We can release information outside VA only when the Privacy Act of 1974 or our confidentiality law (38 USC 5701) allows it. These laws allow us to release the information you put on this form to people outside VA in certain situations. You can find the situations and information when we can release your information in the description of VA's systems of records in the Federal Register. In some cases, the law allows us to release information even if you don't agree to it.

Some examples of situations where information might be released to people outside VA include:  
communicating with members of Congress or other representatives to answer an inquiry you requested  
collecting debts owed the Federal Government  
enforcing civil or criminal law  
comparing with information kept by other Federal agencies

The information we receive may be used to establish or verify your eligibility for VA benefits and debt collection. In all other cases, we must get your written permission before we give information to people outside VA.

Yes	<b>Telephone:</b>
-----	-------------------

**Explain:**

*a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.*

Subjects are told information to be collected is voluntary and that a VA Report of Contact form will be completed to document the conversation and exchange of data. Subjects are told that the information provided is protected under the Privacy Act and shared only for routine purposes to process their VA claim; non-routine disclosures for other than normal VA business require the veteran's consent.

Guidance concerning Privacy notice and acceptable methods of authentication are included in Veterans Service Representative training materials.

No	<b>Other Method:</b>
----	----------------------

*Explain:*

*a) What the subjects will be told about the information collection. b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.). c) How a privacy notice is provided.*

*ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)*

**5.5 Consent For Secondary Use of PII:**

*The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.*

*5.5.a) Will personally identifiable information be used for any secondary purpose?*

*Note: If you have selected No above, then SKIP to question 5.6, "Data Quality."*

No

*5.5.b) Describe and justify any secondary uses of personal information.*

*5.5.c) For each collection method identified in question 5.3, "Collection Method," describe:*

*1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.*

*Some examples of consent methods are: (1) Approved OMB consent forms and (2) VA Consent Form (VA Form 1010EZ). Provide justification if no method of consent is provided.*

	<b>Web Forms:</b>
--	-------------------

*Describe:*

*1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.*

	<b>Paper Forms:</b>
--	---------------------

*Describe:*

*1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.*

	<b>Electronic File Transfer:</b>
--	----------------------------------

*For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to provide the following:*

a) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. b) The opportunities individuals have to grant consent for particular uses of the information. c) How individuals may grant consent.

	<b>Computer Transfer Device:</b>
--	----------------------------------

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to provide the following:

a) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. b) The opportunities individuals have to grant consent for particular uses of the information. c) How individuals may grant consent.

	<b>Telephone Contact Media:</b>
--	---------------------------------

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

	<b>Other Media</b>
--	--------------------

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 5.6 Data Quality

5.6.a) Explain how collected data are limited to required elements:

The VA Forms, electronic and hardcopy, referenced in Section 5.3, that veterans use to submit data are reviewed by the Departments OIG and the General Accounting Office to ensure that only data that is permissible by law and that only data necessary to process benefits is collected. The web sites privacy statements (<http://www.va.gov/privacy/index.htm>) certify that personally identifying information provided by the veteran will be used only in connection with VA programs and services or for such purposes as are described at the point of collection. Information is collected primarily on defined forms and entered to specific fields of database records.

5.6.b) How is data checked for completeness?

Original submission of data is verified for completeness by the Regional Office Veterans Claims Examiners. There are also internal program controls, edits, and checks to ensure that the data submitted is complete. Data is checked for completeness manually and by system edits.

5.6.c) What steps or procedures are taken to ensure the data are current and not out of date?

Veterans who participate in VBA education programs must certify their enrollment monthly. The School certifying official must also certify the same enrollment information. Data is also verified through computer matching programs with other agencies. Data is checked for completeness manually and by system edits with existing VBA IT systems.

5.6.d) How is new data verified for relevance, authenticity and accuracy?

Veterans must provide supporting documentation that verifies their claims such as marriage, birth, and death certificates, DD-214's and other documentation. These documents are reviewed by the Regional Office Veterans Claims Examiners to certify authenticity and accuracy. New income data is verified where possible against computer matching programs with other Federal agencies.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)


**PIA SECTIONS 6 - 13**

**Project Name**

VBA Rules Based Claims Processing - 2009

**6. Use and Disclosure**

**6.1 User Access and Data Sharing**

Identify the individuals and organizations that have access to system data.

--> *Individuals - Access granted to individuals should be limited to the data needed to perform their assigned duties. Individuals with access to personal information stored in project system must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to prevent as well as detect unauthorized access and browsing.*

--> *Other Agencies – Any Federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.*

--> *Other Systems – Information systems of other programs or projects that interface with the information system(s) of this project must be identified and the transferred data must be defined. Also, the controls that are in place to ensure that only the defined data are transmitted must be defined.*

6.1.a) Identify all individuals and organizations that will have access to collected information. Select all applicable items below.

Yes	<b>System Users</b>
-----	---------------------

Yes	<b>System Owner, Project Manager</b>
-----	--------------------------------------

Yes	<b>System Administrator</b>
-----	-----------------------------

Yes	<b>Contractor</b>
-----	-------------------

If contractors to VA have access to the system, describe their role and the extent of access that is granted to them. Also, identify the contract(s) that they operate under.

RBCP is in the planning and initiation stages. It is planned that during RBCP design and development that an Independent Verification and Validation contractor, Business Rules Engine contractor, and system integrator contractor will have access to RBCP. No contracts have been let for RBCP because no funding has been approved; funding is requested for FY 2009.

Yes	<b>Internal Sharing: Veteran Organization</b>
-----	---

If information is shared internally, with other VA organizations identify the organization(s). For each organization, identify the information that is shared and for what purpose.

RBCP will utilize information from existing VBA IT systems to process claims for Education and C&P Service benefits. RBCP entitlement decisions are routinely shared within VBA and VHA for purposes of determining continuing entitlement to current and potential new VA benefits. The VA IG will also have access to RBCP system data.

Yes	<b>Other Veteran Organization</b>
-----	-----------------------------------

If information is shared with a Veteran organization other than VA, identify the organization(s). For each organization, identify the information that is shared and for what purpose.

Veterans Service Organizations, who represent veterans and their eligible dependents, and other designated representatives with VA power of attorney may have read-only access to benefit determinations processed through RBCP.

Yes	<b>Other Federal Government Agency</b>
-----	--

If information is shared with another Federal government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

Congress, GAO, and other Federal entities responsible for oversight of VBA benefits.

Yes	<b>State Government Agency</b>
-----	--------------------------------

If information is shared with a State government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

State Veterans Service Organizations that hold valid VA power of attorney to represent veterans and eligible dependents for claims seeking entitlement to VBA may have read-only access to RBCP system data.

No	<b>Local Government Agency</b>
----	--------------------------------

If information is shared with a local government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

Yes	<b>Other Project/ System</b>
-----	------------------------------

If information is shared with other projects or systems:

1) Identify the other projects and/or systems, and briefly describe the data sharing. 2) For each project and/or system with which information will be shared, identify the information that will be shared with that project or system. 3) For each project and/or system with which information will be shared, describe why information is shared. 4) For each project and/or system with which information will be shared, describe who will be responsible for protecting the privacy rights of the individuals whose data will be shared across this interface.

Data is primarily shared with the Benefits Delivery Network (BDN), specifically for the processing of and payment of educational benefits. RBCP will interface with VVA and VETSNET, and as such will share system data with the VBA corporate database and the VETSNET suite of IT applications, including SHARE, SPP, MAP-D, RBA 2000, Awards, and FAS for purposes of processing and paying C&P Service benefits.

Yes	Other User(s)
-----	---------------

*If information is shared with persons or organization(s) that are not described by the categories provided, use this field to identify and describe what other persons or organization(s) have access to personal information stored on project systems. Also, briefly describe the data sharing.*

Authorized institution or school officials that perform the duty of certifying officials are designated as other users. Their function is to process and certify enrollments, attendance, credits, terms, and courses.

*6.1.a.1) Describe here who has access to personal information maintained in project's IT systems:*

Department of Defense, Social Security Administration, educational institutions, Federal Housing Administration, Internal Revenue Service, Department of Housing and Urban Development, Department of Labor, Department of Treasury, Federal Parent Locator Service, General Accounting Office, Office of Inspector General, Office of Personnel Management, Bureau of Census, Department of Housing and Urban Development. VA employees who process the benefits have access.

*6.1.b) How is access to the data determined?*

This system has documented Memorandums of Understanding/Agreement with all of its business partners, including veteran organizations, federal agencies, state agencies, and local agencies in regard to confidential business information, Privacy Act, and certain information that is subject to confidentiality protections. Access by VA employees is restricted by a security control module to that data they need to do their job. There are also internal controls limits that record a user and reviewing or updating individual records.

*6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents.*

The information that will be processed on TEES is sensitive data because it contains personal information associated with veterans of all the armed services and their family members. This information includes names, social security numbers, and dates of birth, marriage, and death as well as information describing the financial status of veterans. VBA has emplaced strict control measures to prevent the inadvertent or deliberate release of information to non-authorized personnel. Criteria, procedures, controls, and responsibilities regarding access are documented in the Security Plan. Ensuring that protection of data to only authorized persons has been identified as a low risk. It is a defined system requirement.

The information processed on the EDU Maintenance and Operations applications is sensitive data because it contains personal information associated with veterans of all the armed services and their family members. This information includes names, social security numbers, and dates of birth, marriage, and death as well as information describing the financial status of veterans. VBA has emplaced strict control measures to prevent the inadvertent or deliberate release of information to non-authorized personnel. Criteria, procedures, controls, and responsibilities regarding access are documented in the Security Plan. Ensuring that protection of data to only authorized persons has been identified as a low risk. It is a defined system requirement.

Security programs and procedures have been developed to ensure: (1) the protection of veterans, beneficiary, and employee data; (2) the privacy of personal data; (3) the prevention of system operation disruptions; and (4) the elimination of negligent and/or fraudulent misuse of VBA information resources. The protection requirements for this application's data have been reviewed and identified according to relative importance of protection needs for the system, based upon the degree of security needed for the data being processed in terms of confidentiality, integrity, availability, and accuracy.

Internal controls are currently being investigated, and will be documented in the future.

*6.1.d) Will users have access to all data on the project systems or will user access be restricted? Explain.*

User access is restricted. Access is granted on the principles of least privilege and separation of duties. A sensitive file is used to control further access to selected veteran records, which contain "sensitive" information not generally disclosed to all the VBA users.

Internally, station directors may authorize access to the system for any employee that requires access to the network, providing the employee meet the appropriate personnel security requirements as outlined in the VBA IT Handbook No. 5.00.02 HB2. Non-VBA employees, such as Veterans Service Organization (VSO) representatives and student interns, are not considered employees of the United States for the purpose of laws administered by the Office of Personnel Management. Since these individuals do not meet the requirement for employee security review, their access to veterans benefits data is limited to inquiry commands only. These individuals must go through a certification process in order to gain access to the system.

RBCP users will have access to all data in the project systems required to process Education and C&P Service claims. Additional controls are being investigated, and will be documented in the future.

6.1.e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by those having access? (Please list processes and training materials that specifically relate to unauthorized browsing)

Internal controls are in place that disallows unauthorized browsing. A security violation is generated if an employee attempts unauthorized browsing and the event is investigated by the Security Officers. Incident handling capability has been incorporated into the system, including intrusion detection monitoring, and audit log reviews.

The Department has centralized all component incident response capabilities into a single VA-CIRC. Associated guidelines and procedures require that all VA computer security incidents be reported to the VA-CIRC through the facility or office ISO within one business day of the first observation of the incident. VA-CIRC policy requires that, upon identification of an incident/suspected incident, a preliminary report is generated. For incidents that affect critical systems and/or may have adverse global effects on the VA network, the VA-CIRC will dispatch a fly-away team of technical and forensic experts to assist facility personnel in impact containment. A complete incident report, including a full description of the final incident resolution, is submitted to the VA-CIRC no more than five business days after the incident is resolved by the reporting entity.

The VA-CIRC is also responsible for supplying incident reports to OCIS, the primary organizational contact for the affected organization, and to other VA organizations as appropriate; providing a quarterly report summarizing all incidents to the FedCIRC as provided for in a letter of agreement between VA and the FedCIRC; and, responding directly to FedCIRC inquiries. If an individual incident appears to constitute criminal activity, the facility ISO coordinates the incident with local area law enforcement authorities; and, the VA-CIRC notifies the VA OIG. The OIG provides the necessary federal law enforcement coordination (i.e. Federal Bureau of Investigation, Bureau of Alcohol, Tobacco, and Firearms) although the VA-CIRC does respond directly to federal law enforcement inquiries concerning specific incidents upon request.

Additional controls are being investigated, and will be documented in the future.

6.1.f) Is personal information shared (is access provided to anyone other than the system users, system owner, Project Manager, System Administrator)? (Yes/No)

Yes

Note: If you have selected No above, then SKIP to question 6.2, "Access to Records and Requests for Corrections".

6.1.g) Identify the measures taken to protect the privacy rights of the individuals whose data will be shared.

Data included in transfers will be restricted to the minimum necessary for a specific task, e.g., to locate a veteran address or to pay a claim.

6.1.h) Identify who is responsible, once personal information leaves your project's IT system(s), for ensuring that the information is protected.

Other systems will not access RBCP data on-line.

6.1.i) Describe how personal information that is shared is transmitted or disclosed.

Rules for transmission and disclosure are currently being determined and will be documented in the future.

6.1.j) Is a Memorandum of Understanding (MOU), contract, or any other agreement in place with all external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If an MOU is not in place, is the sharing covered by a routine use in the System of Records Notice? If not, explain the steps being taken to address this omission.

This system has documented Memorandums of Understanding/Agreement with all of its business partners, including veteran organizations, federal agencies, state agencies, and local agencies in regard to confidential business information, Privacy Act, and certain information that is subject to confidentiality protections. This includes all the entities mentioned previously within this document and includes the Department of Defense, the Social Security Administration, Educational Institutions, Federal Housing Administration, Internal Revenue Service and the Department of Housing and Urban Development. A detailed listing of all business partners is available from the project manager. VBA has emplaced strict control measures to prevent the inadvertent or deliberate release of information to non-authorized personnel.

6.1.k) How is the shared information secured by the recipient?

Shared information will be required to be secured, how this will be done has not yet been determined. This will be done in the system development phase.

6.1.l) What type of training is required for users from agencies outside VA prior to receiving access to the information?

Training needs will be determined in the project development phase.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 6.2 Access to Records and Requests for Corrections

The Privacy Act and VA policy provide certain rights and mechanisms by which individuals may request access to and amendment of information relating to them that is retained in a System of Records.

6.2.a) How can individuals view instructions for accessing or amending data related to them that is maintained by VA? (Select all applicable options below.)

No	The application will provide a link that leads to their information.
No	The application will provide, via link or where data is collected, written instructions on how to access/amend their information.
Yes	The application will provide a phone number of a VA representative who will provide instructions.
Yes	The application will use other method (explain below).
Yes	The application is exempt from needing to provide access.

6.2.b) What are the procedures that allow individuals to gain access to their own information?

This application has implemented a multi level information access control system. This control system is based upon information sensitivity, access requirements based on individual or group roles and responsibilities. Individual PII access requires admin or supervisory roles above the individual. PII for the admin or supervisory levels must be obtained by another peer admin or supervisory level.

Individuals can submit requests for release of records under the Freedom of Information Act, 5 USC 552, the Privacy Act, 5 USC 552a, the VA Claims Confidentiality statute, 38 USC 5701, and HIPAA.

6.2.c) What are the procedures for correcting erroneous information?

Edit capabilities for PII of an individual can only be changed by admin or supervisory levels. VBA personnel can correct erroneous C&P information after verification of the requestor's identity.

6.2.d) If no redress is provided, are alternatives available?

There is no specific redress beyond direct intervention of a system administrator or database administrator. This would involve remove and recreate of individual records.

6.2.e) Provide here any additional explanation; if exempt, explain why the application is exempt from providing access and amendment.

The position sensitivity ratings and levels are established on a need to access basis, sensitivity of the information and assigned to group or individual permissions as established by the systems administrator.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 7 Retention and Disposal

By completing this section, you provide documented assurance that proper data retention and disposal practices are in place.

The "Retention and disposal" section of the applicable System of Records Notice(s) often provides appropriate and sufficiently detailed documented data retention and disposal practices specific to your project.

VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures.

**System of Records Notices may be accessed via:**

<http://vaww.vhaco.va.gov//privacy/SystemofRecords.htm>

or

[http://vaww.va.gov/foia/err/enhanced/privacy\\_act/privacy\\_act.html](http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html)

For VHA projects, VHA Handbook 1907.1 (Section 6j) and VHA Records Control Schedule 10-1 provide more general guidance.

**VHA Handbook 1907.1 may be accessed at:**

[http://www1.va.gov/vhapublications/ViewPublication.asp?pub\\_ID=434](http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=434)

For VBA projects, Records Control Schedule (RCS) VB-1 provides more general guidance. VBA Records Control Schedule (RCS) VB-1 may be accessed via the URL listed below.

[Start by looking at the http://www.warms.vba.va.gov/20rcs.html](http://www.warms.vba.va.gov/20rcs.html)

7.a) What is the data retention period? Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Active records are retained at servicing Regional Office (RO) for the life of the veteran; inactive records may be transferred to the VA Records Processing Center (RPC) for storage. Electronic records are maintained indefinitely. At the death of the veteran, paper records maintained at the servicing RO are sent to the Federal Records Center (FRC) and maintained by FRC for 75 years.

7.b) What are the procedures for eliminating data at the end of the retention period?

After 75 years retention at the FRC, paper records are destroyed by shredding or burning.

Regarding electronic information, support systems retain data that is work in process until the data is committed to the master system of record (VBA corporate database). If a master system is deactivated, critical data is migrated to the new system, and data from the old system is archived per the application disposition worksheet. Once archived, existing application code and files are deleted. Data elimination procedures are currently being updated. In Education Service, which has electronic folders, paper that is scanned into the system is kept for 1 year and then destroyed. Reference is RPO Letter 22-03-14 Dated March 14, 2003.

7.c) Where are procedures documented?

VA Handbook 6300.5 and Records Control Schedule (RCS) VBA-1, Part 1, Section 8.

These procedures are available online at <http://www.warms.vba.va.gov/admin23/part1/sec08.doc> and in the Systems of Records 58VA21/22/28 and 38VA23.

7.d) How are data retention procedures enforced?

The Director of each RO enforces retention procedures at his/her station. Management oversight and review enforces data retention policies.

7.e) If applicable, has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 8 SECURITY

OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, (OMB M-03-22) specifies that privacy impact assessments must address how collected information will be secured.

### 8.1 General Security Measures

8.1.a) Per OMB guidance, citing requirements of the Federal Information Security Management Act, address the following items (select all applicable boxes.):

Yes	The project is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured.

Yes	The project has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.
Yes	Security monitoring, testing, and evaluating are conducted on a regular basis to ensure that controls continue to work properly, safeguarding the information.

**8.1.b) Describe the security monitoring, testing, and evaluating that is conducted on a regular basis:**

A standardized Department methodology based on the direction in National Institute of Standards and Technology (NIST) guidance is used to continuously monitor, test and evaluate security for this major application. The approximately 60 common security controls provided by the Office of Information and Technology (OIT), or other respective VA Program Office, are tested every year. Application-specific security testing evaluates approximately one-third of the remaining 90 controls on an annual basis, with the entire respective application NIST Special Publication (SP) 800-53 security control baseline—at the Federal Information Processing Standard (FIPS) 199 level of moderate--being tested over each three-year period. The testing supports certification and re-accreditation requirements, as well as Federal Information Security Management Act (FISMA) requirements to annually test the operational, management, and technical controls of each Department system. The specific controls identified for testing are selected by OIT Operations, with advice from the VA Office of Cyber Security (OCS), and include key controls that provide integrity and confidentiality (such as access, authentication, configuration management, and media controls). The tests are conducted using the criteria in NIST SP 800-53A, Second Public Draft, Guide for Assessing the Security Controls in Federal Information Systems, and tailored to the VA operational environment. Testing of operational systems is primarily conducted by the OIT Compliance and Inspection Management Office, which was chartered to conduct security control assessments across the VA enterprise, as well as independent contractors.

For test results that indicate a security control is not operating as intended, a Plan of Action and Milestones (POA&Ms) is developed and entered into the Department's Security Management and Reporting Tool (SMART). The POA&Ms identifies the activities and timelines for correction of the security weakness, and is managed by the respective application information security officer, with progress monitored by the application program manager. The VA Chief Information Officer receives quarterly reporting on the status of all POA&Ms, with that information also being included in required updates to the Office of Management and Budget as part of the FISMA reporting process.

On an annual basis, the VA Chief Information Officer (CIO), in conjunction with system owners and information owners, and with advice from the VA Office of Inspector General (OIG), evaluate the Department's overall IT security posture. This evaluation includes identification of significant security performance gaps, the prioritization of key POA&M weakness areas for immediate remediation action, as well as the designation of certain security areas that would benefit from enterprise-wide management of a single security solution, thereby effectively targeting those areas for action that would most improve the Department's security posture in the near-term.

**8.1.c) Is adequate physical security in place to protect against unauthorized access?**

Yes

**8.2 Project-Specific Security Measures**

**8.2.a) Provide a specific description of how collected information will be secured.**

- A concise description of how data will be protected against unauthorized access, unauthorized modification, and how the availability of the system will be protected.
- A concise description of the administrative controls (Security Plans, Rules of Behavior, Procedures for establishing user accounts, etc.).
- A concise description of the technical controls (Access Controls, Intrusion Detection, etc.) that will be in place to safeguard the information.
- Describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses. For example, are audit logs regularly reviewed to ensure appropriate use of information? Are strict disciplinary programs in place if an individual is found to be inappropriately using the information?

*Note: Administrative and technical safeguards must be specific to the system covered by the PIA, rather than an overall description of how the VA's network is secured. Does the project/system have its own security controls, independent of the VA network? Is so, describe these controls.*

All information stored in VBA databases is secured in agreement with VA strategy. This strategy implements Federal Regulations, VA IT security policy and guidelines, NIST Guidelines and industry best practices. Security is implemented in compliance with VA's Office of Cyber and Information Security (OCIS) guidelines, policies, and mandates. With guidance from OCIS, the VBA administers and monitors security controls on multiple operating levels including the managerial, operational and technical levels. This System uses strong passwords. Access is granted on the principles of least privilege and separation of duties. Users have completed ethics training, annual cyber security training, and have signed rules of

behavior. All security controls are implemented through a cohesive security structure and are geared to maintaining risk to information and information resources to acceptable levels. In addition to documented risk management, other management level controls such as system security planning, certification and accreditation and security reviews are also implemented to assure that controls reflect management policies at operational levels including at the enterprise, business line and project level. Operational and technical controls such as contingency planning, input/output settings, data integrity and validation measures and logical access controls, are implemented on the various network, system, server and application levels to assure that information is secured in transit, process and storage. For example, the VA employs a virtual private network to assure the privacy of information in transit. This system works in conjunction with strong authentication measures to ensure and authenticate the identification of VA network users. System interconnection agreements (SIA)s are a system level measure to ensure that all interconnected systems meet minimum VA access policies for interconnected systems from within and outside the VA wide area network (WAN) boundaries. Moreover, the VA employs a comprehensive incidence response unit to respond to unwanted incursions and institutes enterprise level anti-virus system to protect mission critical applications on the desktop. Finally, the VA security program is an iterative program with repeatable processes that, in an ongoing basis, will mitigate vulnerabilities, minimize security exposures and maintain security and operating risk at acceptable levels. A security plan will be developed that documents the procedures required ensuring the integrity, confidentiality, and availability to VA information. Specifically, personnel security, physical protection, production input/output controls, contingency planning, system hardware and software maintenance controls, security awareness and training, and incident response capabilities are discussed in detail. The details contained within these sections include specific activities and procedures, which ultimately ensure that the integrity, confidentiality, and availability to VA information contained within the system is protected as required by Federal policy. All files, records, reports, and other papers and documents pertaining to any claim under any of the laws administered by the Department of Veterans Affairs and the names and addresses of present or former members of the Armed Forces, and their dependents, in the possession of the Department shall be confidential and privileged. This specifically includes all individually identifiable health information of a veteran, which is stored electronically and in hard copy form. All works or items of intellectual property used, transmitted, stored, or disseminated by the Department as part of this initiative, in any form, including electronic or physical, will be used in conformance with laws and regulations applicable to copyright, patent, trademark, or licensing of such works.

8.2.b) Explain how the project meets IT security requirements and procedures required by federal law.

This project implements all applicable Federal Regulations, VA IT security policy and guidelines, NIST Guidelines and industry best practices. Security is implemented in compliance with VA's Office of Cyber and Information Security (OCIS) guidelines, policies, and mandates.

## 9. CHANGE RECORD

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, mandates that PIAs address any project/ system changes that potentially create new privacy risks. By completing this section, you provide documented assurance that significant project/ system modifications have been appropriately evaluated for privacy-related impacts.

9.a Since the last PIA submitted, have any significant changes been made to the system that might impact the privacy of people whose information is retained on project systems? (Yes, No, n/a: first PIA)

N/A

If no, then proceed to Section 10, "Children's Online Privacy Protection Act."

If yes, then please complete the information in the table below. List each significant change on a separate row. 'Significant changes' may include:

Conversions - when converting paper-based records to electronic systems;

Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;

Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:

- For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.

Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:

- For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.

New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;

Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

*Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:*

• For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.

*Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information);*

List All Major Project/System Modification(s)	State Justification for Modification(s)	*Concisely describe:	Modification Approver	Date

\* The effect of the modification on the privacy of collected personal information

\* How any adverse effects on the privacy of collected information were mitigated.

## 10. CHILDREN'S ONLINE PRIVACY PROTECTION ACT

10.a) Will information be collected through the Internet from children under age 13?

No

If "No" then SKIP to Section 11, "PIA Considerations".

10.b) How will parental or guardian approval be obtained.

Not applicable

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 11. PIA CONSIDERATIONS

11) Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA. Examples of choices made include reconsideration of: collection source, collection methods, controls to mitigate misuse of information, provision of consent and privacy notice, and security controls.

As a result of performing the PIA, continual emphasis and attention will be applied to addressing security and privacy concerns including assuring that collection of data and personal information contains appropriate consent and release information and that all information stored in VBA databases are secured per VA security standards.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

## 12. PUBLIC AVAILABILITY

The Electronic Government Act of 2002 requires that VA make this PIA available to the public. This section is intended to provide documented assurance that the PIA is reviewed for any potentially sensitive information that should be removed from the version of the PIA that is made available to the public.

The following guidance is excerpted from M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," Section II.C.3, "Review and Publication": iii. Agencies must ensure that the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).

1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment<sup>9</sup>. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).

2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

12.a) Does this PIA contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

12.b) If yes, specify:

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

### 13. ACCEPTANCE OF RESPONSIBILITY AND ACKNOWLEDGEMENT OF ACCOUNTABILITY:

13.1) I have carefully reviewed the responses to each of the questions in this PIA. I am responsible for funding and procuring, developing, and integrating privacy and security controls into the project. I understand that integrating privacy and security considerations into the project may affect the development time and cost of this project and must be planned for accordingly. I will ensure that VA privacy and information security policies, guidelines, and procedures are followed in the development, integration, and, if applicable, the operation and maintenance of this application.

Yes

13.2) Project Manager/Owner Name and Date (mm/dd/yyyy)

Rebecca Wells 08/24/2007

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)