

Privacy Impact Assessment - 2009 (Form) / VBA Application Migration Program-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 Application Migration Program-2009

1.1.b) OMB Unique Project Identifier:

029-00-03-00-01-1015-00

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 mission of the Veterans Benefits Administration (VBA) is to provide benefits and services to veterans and their families in a responsive, timely and compassionate manner in recognition of their service to the Nation. VBA has identified five lines of business to accomplish its mission;

- (1) Compensation and Pension
- (2) Education
- (3) Vocational Rehab and Employment
- (4) Insurance
- (5) Loan Guaranty

Each business line utilized a stove pipe approach to fulfilling an identified business need and implemented a disparate set of applications to meet those needs. So in many cases the solution developed is unique and has created an inventory of proprietary, incompatible technologies that may not be supported by vendors, require duplicative infrastructures, and do not comply with VA's "to be" architecture model.

Because of these limitations, VBA cannot deliver services directly to its customers as effectively, efficiently or as reliably as possible. Furthermore this infrastructure prevents VBA from leveraging current service delivery platforms including web based technologies and service oriented architectures. VA has initiated the VBA Application Migration Program to address the service delivery gap, reduce risk to the government, and comply with VA "to be" state in the enterprise architecture. VAMP will assist the veteran by implementing web-based technology that will include self-services features and allow veterans to obtain information on their own reducing the reliance on call centers. VAMP will reduce risk to the government and duplication in the infrastructure by modernizing the current VBA infrastructure and leveraging an enterprise approach to selecting technical solutions. The Enterprise Architecture (EA) Strategy of VAMP will be that all VBA applications will become web-based through re-writing and re-hosting. Each application will adhere a set of predefined preferred products and industry standards. The adoption of these standards in conjunction with the move to the VBA Target Web Framework will have a positive impact on the delivery of services to the customer by providing for greater data accuracy

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.

The purpose of this investment is to retire legacy systems, to provide a modern infrastructure that supports VBA self-service delivery model and to consolidate applications where possible.

Forces that drive Application Migration:

(A) Our mission

The mission of the Veterans Benefits Administration, in partnership with the Veterans Health Administration and the National Cemetery Administration, is to provide benefits and services to the veterans and their families in a responsive, timely and compassionate manner in recognition of their service to the Nation. In the VBA, serving veterans is accomplished through five business lines: (1) Compensation and Pension; (2) Education; (3) Vocational Rehab and Employment; (4) Insurance and; (5) Loan Guaranty. Each of these business lines is supported by a set of distinct applications that were deployed as the need arose.

Most of these applications are based on various technologies; they do not share common services, cannot take advantage of popular web-services, and most are not web-based. Because of these limitations, VBA cannot deliver most of the services to its customers cheaply, efficiently and across the Internet. This service delivery gap is addressed by this initiative.

(B) Technical expertise

The subject matter experts in VBA legacy application languages such as COBOL and platforms such as the IBM Mainframe are retiring and are getting more expensive to replace. The expense and technical risk of continuing to operate these systems has grown to an unacceptable level.

(C) Support new business requirements

The current systems cannot support the future business requirements of VBA, most notably the introduction of self-service features for the veteran population.

(D) Enterprise Architecture Strategy

All the 60 applications that are under the VBA will be web-based by re-writing and re-hosting them based on the five application architecture standards below. (211)

(E) Every application will:

- (1) be Browser-based;
- (2) be written in J2EE/Java;
- (3) be hosted on a UNIX operating systems;
- (4) have data in the Corporate (Oracle) Database;
- (5) have interfaces to web-services and databases be XML-based.

The adoption of these standards has a positive impact on Veteran Service Representatives (VSR) at our regional offices. Improvements include more accuracy of veteran data, shifting workload from VSRs to the customer, simplified workstation configuration.

1.2) Contact Information:

| | |
|--|---|
| 1.2.a) Person completing this document: | |
| Title: | John Quigley |
| Organization: | Technical Project Manager, Business Project Management Office (BPMO) |
| Telephone Number: | 202-461-9152 |
| Email Address: | john.quigley@va.gov |
| 1.2.b) Project Manager: | |
| Title: | John Quigley |
| Organization: | Technical Project Manager, Business Project Management Office (BPMO) |
| Telephone Number: | 202-273-8309 |
| Email Address: | John.Quigley@vba.va.gov |
| 1.2.c) Staff Contact Person: | |
| Title: | Michael Miti-Kavuma |
| Organization: | IT Specialist, Enterprise Architecture , VBA, Office of Information and Technology (OI&T) |

| | |
|--------------------------|--------------------------------|
| Telephone Number: | 202-273-6930 |
| Email Address: | michael.miti-kavuma@vba.va.gov |
| | |

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

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.)

This initiative represents a re-platforming of the entire suite of VBA applications. Therefore all VBA data will be "touched" by this project. In this regard, the project will maintain personally identifiable information in the form of benefit data for the clients we serve, specifically the U.S. Veteran population. At this time, we do not anticipate any personally identifiable employee or contractor information being maintained by the project.

Part II. Privacy Impact Assessment

3. PROJECT DESCRIPTION:

Enter the information requested to describe the project.

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.

The Veterans Benefits Administration is responsible for providing Veteran benefits under Title 38 of the United States Code. To perform this function successfully, the Agency maintains data regarding the veterans applying for benefits, information supporting the application for benefits (such as medical information) and the disposition of benefit applications. In the event of a successful claim for benefits, additional data, such as payment information is also maintained. This project is a re-platforming effort that will touch all VBA application data and, therefore, the project will require access to the veteran information already maintained by the Agency.

3.b) What specific legal authorities authorize this project, and the associated collection, use, and/or retention of personal information?

Title 38 of the United States Code.

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.

More than 20,000,000

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.

(1) Design/Planning

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. |
| 10/2008 |
| ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.) |
| Although the supporting infrastructure is expected to be in place prior to 10/2008, this is the anticipated date for the first series of migrated applications going into production. |
| |

4. SYSTEM OF RECORDS:

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 & Managing Privacy Act Systems Of Records", for additional information regarding Systems of Records.

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?

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

Yes

4.b) Are the project and/or system data maintained under one or more approved System(s) of Records?

IF "No" then SKIP to question 4.c.

Yes

4.b.1) For each applicable System of Records, list:

(1) The System of Records identifier (number),

55VA26, 58VA21/22/28, 36VA00 , 46VA00, 53VA00

(2) The name of the System of Records, and

55VA26: System name: Veterans and Armed Forces Personnel United States Government Life Insurance Records-VA.
58VA21/22/28: System name: Compensation, Pension, Education and Rehabilitation Records-VA.
36VA00: System name: Veterans and Armed Forces Personnel United States Government Life Insurance Records-VA.
53VA00: System name: Veterans Mortgage Life Insurance-VA.
46VA00: System name: Veterans, Beneficiaries and Attorneys United States Government Insurance Award Records-VA.

(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL).

All the Systems of Records identified above can be accessed from the attached URL:
<http://vawww.va.gov/privacy/SystemsOfRecords>

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.

All existing VBA systems of records were created to administer veteran benefits as authorized under Title 38, United States Code.

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 Application Migration Program-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.

The VBA benefit systems process entitlements for five mission areas: Compensation and Pension, Education, Vocational Rehabilitation and Employment, Loan Guaranty and Insurance. The primary services of the benefit systems entail the receipt, processing, tracking and disposition of veterans' application for benefits and requests for assistance; and the general administration of legislated benefit programs. Information is collected to provide all entitled benefits in the most complete and effective manner. The information collected includes: Name, Address, Social Security Number, Family/Dependents, marital status, medical status, birth information, death information, service data; Reserve or Guard Participation, retired pay or severance pay, hazardous agent exposure, branch of service, duty date, released date, type of discharge, separation reason, medical records, military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations to include police reports; incarceration at federal, state or local facility, fugitive felon status, and/or investigative reports for some accidents. The records may also contain additional veteran information such: Guardian information; court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accounts. The benefit systems also contain veteran educational records such as: education program approval information, approved courses, effective dates, types of training, facility code, objective code and training type. Income verification is also used for veteran pension based decisions and entitlements.

No

Other Personal Information of the Veteran or Primary Subject

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

| | |
|-----|------------------------------|
| Yes | Dependent Information |
|-----|------------------------------|

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

The VBA benefit systems process entitlements for five mission areas: Compensation and Pension, Education, Vocational Rehabilitation and Employment, Loan Guaranty and Insurance. The primary services of the benefit systems entail the receipt, processing, tracking and disposition of veterans' application for benefits and requests for assistance; and the general administration of legislated benefit programs. Information is collected to provide all entitled benefits in the most complete and effective manner. Systems can contain dependent data of veteran such as personal information including name and address, age, school status, relationship to the veteran and medical status. Additional benefit may be payable for dependents as well.

| | |
|-----|----------------------------|
| Yes | Service Information |
|-----|----------------------------|

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

The VBA benefit systems process entitlements for five mission areas: Compensation and Pension, Education, Vocational Rehabilitation and Employment, Loan Guaranty and Insurance. The primary services of the benefit systems entail the receipt, processing, tracking and disposition of veterans' application for benefits and requests for assistance; and the general administration of legislated benefit programs. Information is collected to provide all entitled benefits in the most complete and effective manner. The benefit systems contains veteran service data such as: Reserve and Guard Participation, retired pay or severance pay, hazardous agent exposure, Branch of service, duty date, released date, type of discharge, separation reason. All service data is collected to determine eligibility to specific benefits.

| | |
|-----|----------------------------|
| Yes | Medical Information |
|-----|----------------------------|

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

The VBA benefit systems process entitlements for five mission areas: Compensation and Pension, Education, Vocational Rehabilitation and Employment, Loan Guaranty and Insurance. The primary services of the benefit systems entail the receipt, processing, tracking and disposition of veterans' application for benefits and requests for assistance; and the general administration of legislated benefit programs. Information is collected to provide all entitled benefits in the most complete and effective manner. The benefit systems contains medical information such as: hazardous agent exposure, branch of service, duty date, released date, type of discharge, separation reason, medical records, military clinical records, government health records, vocational rehabilitation and employment records. All medical data is collected to determine eligibility to specific benefits.

| | |
|-----|------------------------------------|
| Yes | Criminal Record Information |
|-----|------------------------------------|

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

The VBA benefit systems process entitlements for five mission areas: Compensation and Pension, Education, Vocational Rehabilitation and Employment, Loan Guaranty and Insurance. The primary services of the benefit systems entail the receipt, processing, tracking and disposition of veterans' application for benefits and requests for assistance; and the general administration of legislated benefit programs. Information is collected to provide all entitled benefits in the most complete and effective manner. The benefits systems contain criminal data such as: line of duty investigations to include police reports; incarceration at federal, state or local facility, fugitive felon status, and/or investigative reports for some accidents. Data may be used to determine basic entitlement and continued eligibility that could be reduced as a result of incarceration.

| | |
|-----|-----------------------------|
| Yes | Guardian Information |
|-----|-----------------------------|

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

The VBA benefit systems process entitlements for five mission areas: Compensation and Pension, Education, Vocational Rehabilitation and Employment, Loan Guaranty and Insurance. The primary services of the benefit systems entail the receipt, processing, tracking and disposition of veterans' application for benefits and requests for assistance; and the general administration of legislated benefit programs. Information is collected to provide all entitled benefits in the most complete and effective manner. The benefits systems contain guardian data such as: court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accounting and other dependent information. Medical information would also be used to determine various guardian decisions; e.g., court ordered due to veteran unable to care for dependent.

| | |
|-----|------------------------------|
| Yes | Education Information |
|-----|------------------------------|

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

The VBA benefit systems process entitlements for five mission areas: Compensation and Pension, Education, Vocational Rehabilitation and Employment, Loan Guaranty and Insurance. The primary services of the benefit systems entail the receipt, processing, tracking and disposition of veterans' application for benefits and requests for assistance; and the general administration of legislated benefit programs. Information is collected to provide all entitled benefits in the most complete and effective manner. The benefit systems also contain veteran educational records such as: education program approval information, approved courses, effective dates, types of training, facility code, objective code and training type.

| | |
|-----|-----------------------------------|
| Yes | Rehabilitation Information |
|-----|-----------------------------------|

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

The VBA benefit systems process entitlements for five mission areas: Compensation and Pension, Education, Vocational Rehabilitation and Employment, Loan Guaranty and Insurance. The primary services of the benefit systems entail the receipt, processing, tracking and disposition of veterans' application for benefits and requests for assistance; and the general administration of legislated benefit programs. Information is collected to provide all entitled benefits in the most complete and effective manner. The benefit systems also contain veteran service and employment records that are required to support entitlement to vocational rehabilitation benefits.

| | |
|-----|--|
| Yes | Other Personal Information (specify): |
|-----|--|

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.

The benefits systems are also used for statistical and legislative inquiries and contain data required to support electronic file transfer of payments. The information is used to determine eligibility for benefits, process ratings, and to provide payments via Department of the Treasury.

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 | Veteran Source |
|-----|-----------------------|

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) and Veteran Dependent Data (personal information including name and address, age, school status, relationship to the veteran, medical status) 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 | Public Source(s) |
|-----|-------------------------|

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. Information is used to process education benefits.

| | |
|-----|-------------------------------|
| Yes | VA Files and Databases |
|-----|-------------------------------|

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, facility code, objective code, training type), and Rehabilitation Program Approval Information (institution certifications, licenses, approval information) is used to determine eligibility and process entitlement.

| | |
|-----|---------------------------------------|
| Yes | Other Federal Agency Source(s) |
|-----|---------------------------------------|

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.

| | |
|-----|-------------------------------|
| Yes | State Agency Source(s) |
|-----|-------------------------------|

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.

1. To determine eligibility for veteran benefits, either for compensation and pension, education and/or vocational rehabilitation and employment. For example, inquiry to locate and verify status of dependents or to verify a state court decision requiring a veteran to provide care payments in case of separation of marriage.
2. To request veteran information from the state Bureau of Prisons and Police Records: Incarceration at federal state or local facility, fugitive felon status, investigative reports for some accident. Benefits are suspended for incarcerated veterans.

| | |
|----|-------------------------------|
| No | Local Agency Source(s) |
|----|-------------------------------|

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 | Other Source(s) |
|-----|------------------------|

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.

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 | Web Forms: | 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/von-app/main.asp>. The available forms located at this site are: V A Form 22-1990, Application for Education Benefits. 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/>

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

| | | |
|-----|---------------------|--|
| Yes | Paper Forms: | 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.

The available forms located at this site are: VA Form 21-526 – Veteran's Application for Compensation and/or Pension; VA Form 28-1900 – Disabled Application for Vocational Rehabilitation; V A Form 22-1990, Application for Education Benefits. 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/>

VBA forms can be downloaded from this site, filled in and printed to be delivered in paper form. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury.

| | | |
|-----|----------------------------------|--|
| Yes | Electronic File Transfer: | 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.)

The VBA receives secure data transfers from multiple Federal agencies including the Department of Defense, Internal Revenue Service, Social Security Administration, Department of Homeland Security and the Department of Treasury. The VBA also receives secure data transfers from education providers. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury.

| | | |
|-----|----------------------------------|--|
| Yes | Computer Transfer Device: | 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.

Various media are used to exchange information with the agencies and institutes identified above including electronic file transfers, batch updates; CD-ROMS and Tape cartridges. Secure Data interchange with the Social Security Administration; Internal Revenue Service, Department of Treasury and the Department of Homeland Security.

| | | |
|-----|---------------------------|---|
| Yes | Telephone Contact: | 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. Clients are referred to and transferred to the Regional Office of Jurisdiction, where they can provide a service representative with required information. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury.

| | | |
|----|---------------------------------|--|
| No | Other Collection Method: | 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 Act information is provided on the website (<http://www.va.gov/privacy/index.htm>) and Privacy Act information is provided to claimants when information is requested. In addition, most VA forms requesting information are accompanied by Privacy Act information. These notices inform the claimant as to what information is mandatory or voluntary.

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 | Not applicable |
| Yes | Privacy notice is provided on each page of the application. |

| | |
|-----|--|
| Yes | A link to the VA Website Privacy Policy is provided. |
| Yes | Proximity and Timing: the notice is provided at the time and point of data collection. |
| Yes | Purpose: notice describes the principal purpose(s) for which the information will be used. |
| Yes | Authority: notice specifies the legal authority that allows the information to be collected. |
| Yes | Conditions: notice specifies if providing information is voluntary, and effects, if any, of not providing it. |
| Yes | Disclosures: notice specifies routine use(s) that may be made of the information. |

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

The project itself will not collect information from VBA clients and therefore will not directly provide privacy information to clients. The project is responsible for maintaining data integrity during the project lifecycle. The project will rely on already implemented procedures, practices and systems to continue to notify VA clientele of Privacy Act provisions.

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 | Web Forms: |
|-----|-------------------|

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.

Link to VA site on Privacy, Freedom of Information, and Security. The privacy of our customers has always been of utmost importance to the Department of Veterans Affairs. The VA has a long history of protecting your privacy and our concern for your privacy is no different in the electronic age. Our Internet privacy policy is: 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.

The Privacy Act of 1974 applies to all Federal agencies. For information on the Federal government's Web Site Privacy Policy, see the following documents:

VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act

VA Handbook 6300.5, Procedures for Establishing & Managing Privacy Act Systems of Records.

| | |
|-----|---------------------|
| Yes | Paper Forms: |
|-----|---------------------|

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.

Written notice on all VA forms. 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.

| | |
|-----|----------------------------------|
| Yes | Electronic File Transfer: |
|-----|----------------------------------|

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?

The subjects are told in writing:
- Privacy Act and Paperwork Reduction Act Notice
- 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.
- The PROCEDURES FOR PROCESSING REQUESTS FOR RECORDS SUBJECT TO THE PRIVACY ACT outlined in the VA Handbook 6300.4.

| | |
|-----|----------------------------------|
| Yes | Computer Transfer Device: |
|-----|----------------------------------|

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?

The subjects are told in writing:
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) 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 | Telephone: |
|-----|------------|

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.

Information collected is used to direct the veteran to the nearest VBA regional office to process and/or submit claims, obtain additional veteran eligibility information for veteran, dependent, and/or widow. If unable to do so by existing web services, guidance is provided on how to obtain forms and instructions for mail

| | |
|----|---------------|
| No | Other 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.

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.

| | |
|--|------------|
| | Web Forms: |
|--|------------|

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.

| | |
|--|---------------------|
| | Paper Forms: |
|--|---------------------|

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.

| | |
|--|----------------------------------|
| | Electronic File Transfer: |
|--|----------------------------------|

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.

| | |
|--|----------------------------------|
| | Computer Transfer Device: |
|--|----------------------------------|

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.

| | |
|--|---------------------------------|
| | Telephone Contact Media: |
|--|---------------------------------|

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.

| | |
|--|--------------------|
| | Other Media |
|--|--------------------|

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:

Information is collected primarily on defined forms and entered to specific fields of database records. The required veteran's data are stored within the database(s) which support the individual claim or claims the veteran has been granted.

5.6.b) How is data checked for completeness?

Data are checked for completeness by system audits, manual verifications and annual questionnaires through automated veteran letters. These letters ask specific questions for verification based on the existing entitlement or benefit the veteran is receiving. Also, data are updated with each veteran correspondence.

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

Data are updated as a result of returned mail, or returned direct deposits, or through contact with the veteran, beneficiary, or power of attorney. Additionally, verifications and system audits are performed.

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

All data are matched against supporting claims documentation submitted by the veteran, widow, or dependent. Certain data such as SSN is verified with the Social Security Administration. Prior to any award or entitlement authorization(s) by the VBA, the veteran record is manually reviewed and data validated to ensure correct entitlement has been approved.

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

PIA SECTIONS 6 - 13

Project Name

VBA Application Migration Program-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

System Users

Yes

System Owner, Project Manager

| | |
|-----|-----------------------------|
| Yes | System Administrator |
|-----|-----------------------------|

| | |
|-----|-------------------|
| Yes | Contractor |
|-----|-------------------|

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.

Contractors will be responsible for migrating the system databases as well as the applications accessing those databases. The contractors will require full access to VBA data to perform their task orders successfully. Contracts have not yet been let to perform these tasks. Contractors will be required to have security clearances and sign non-disclosure statements prior to access to any VBA data.

| | |
|-----|---|
| Yes | Internal Sharing: Veteran Organization |
|-----|---|

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.

(1) WebHINQ enables VHA to retrieve data from the new corporate database as well as BDN (until it is completely retired) and BIRLS.

WebHINQ will retrieve 4 new pieces of data when the record is stored in the new corporate database. When available, the following will be retrieved for each SC disability:

- The affected extremity
 - The original effective date of the disability rating and the current (most recent) date the rating was changed
- In addition, the Effective Date of Combined SC Evaluation is provided.

(2) CAPRI enables data flow between VBA and VHA.

For the most part, data flow between VHA and VBA is one way - to VBA. In very few instances, VHA will access VBA information.

| | |
|-----|-----------------------------------|
| Yes | Other Veteran Organization |
|-----|-----------------------------------|

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.

Co-located Veterans Service Organizations (VSOs) –Co-located Veterans Service Organizations at VBA regional offices have been given on-line read only access to BDN, BDN Shell, Covers, Share, State Benefits Reference Systems, VACOLS, Virtual VA, Advisory, WARMS and MAP-D. The co-located VSOs have direct access to veteran data securely through LAN. This access is authorized by VA regulations. The organization requests access and the standard VA logon and password security requirements that are applicable to VA employees are followed.

Remote Veterans Service Organizations (VSOs) –Remote Veterans Service Organizations have been given on-line read only access to SHARE and MAP-D. The remote VSOs access veteran data securely through VA's Virtual Private Network. On-line access is real time and may be accessed by the County/State/National Service Organization at any time. This access is authorized by VA regulations. The County/State/National Service Organization requests on-line access for its representatives. The organization requests access and the standard VA logon and password security requirements that are applicable to VA employees are followed.

| | |
|-----|--|
| Yes | Other Federal Government Agency |
|-----|--|

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.

The VA shares payment information with the Department of Treasury to pay veteran benefit payments.

| | |
|----|--------------------------------|
| No | State Government Agency |
|----|--------------------------------|

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.

| | |
|----|--------------------------------|
| No | Local Government Agency |
|----|--------------------------------|

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 | Other Project/ System |
|-----|------------------------------|

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.

| | |
|----|----------------------|
| No | 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.

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

All employees that are authorized to access and process veterans claims are provided specific password that allow them to obtain or access data within the VBA Corporate system. Approximately 12,000 end-users access the IT systems supporting this data. In addition, Veterans Service Organizations and attorney's that have power-of-attorney over the veteran have restricted read-only access.

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

Users are granted individual levels of authority privileges to view or process veterans claim information. The access levels are provided through strict controls and passwords assigned to individual end-users. There are logs of all passwords provided and the access levels granted. CSUM is the application responsible for performing this task. Reports are created which identify all access attempts both successful and unsuccessful to any information for a veteran with any level of sensitivity restriction. Creation of individual user IDs requires a written request from a supervisor with the work being

| |
|--|
| performed by Information Security Officers. |
| <i>6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents.</i> |
| This system has documented Memorandums of Understanding/Agreement with all of its business partners, including veteran organizations, federal agencies, state agencies, and contractors 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, and the Social Security Administration. A detailed listing of all business partners is available from the project manager. VBA has strict control measures in place to prevent the inadvertent or deliberate release of information to non-authorized personnel. |
| <i>6.1.d) Will users have access to all data on the project systems or will user access be restricted? Explain.</i> |
| The end user access is restricted by the level of authority they require to perform their jobs. The systems include authorization at the application and function level. Users may have inquiry, update (sometimes sub-divided), or verifier authority to different screens. |
| <i>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)</i> |
| he 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. |
| <i>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)</i> |
| No |
| <i>Note: If you have selected No above, then SKIP to question 6.2, "Access to Records and Requests for Corrections".</i> |
| <i>6.1.g) Identify the measures taken to protect the privacy rights of the individuals whose data will be shared.</i> |
| |
| <i>6.1.h) Identify who is responsible, once personal information leaves your project's IT system(s), for ensuring that the information is protected.</i> |
| |
| <i>6.1.i) Describe how personal information that is shared is transmitted or disclosed.</i> |
| |
| <i>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.</i> |
| |
| <i>6.1.k) How is the shared information secured by the recipient?</i> |
| |
| <i>6.1.l) What type of training is required for users from agencies outside VA prior to receiving access to the information?</i> |
| |
| <i>ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)</i> |
| |
| |

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. |
| Yes | 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. |
| No | The application will use other method (explain below). |
| No | 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?

A formal request, be it verbal or in writing has to be submitted to the VBA.

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

A formal request, be it verbal or in writing has to be submitted to the VBA.

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

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

Information such as (1) doctor's report and (2) police report are out of the jurisdiction of the Department of Veterans Affairs. The documents, although accessible to the client, can only be amended by the doctor or police respectively.

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 |
| 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

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>

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.

Data is retained on all VBA systems indefinitely.

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

Data is not eliminated but stored on removable media.

7.c) Where are procedures documented?

Procedures are documented in the Disaster Recover and Continuity of Operations (COOP) plans for the respective data centers where the data is housed.

7.d) How are data retention procedures enforced?

Enforcement procedures are documented in the Disaster Recover and Continuity of Operations (COOP) plans for the respective data centers where the data is housed.

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

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. |
| No | 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:

While the applications are in their source environments, they will continue to employ the existing security controls as documented in their respective security plans and operation and maintenance Exhibit 300s. These include FISMA provisions such as a self-assessment of IT security management, operational, personnel, and technical controls conducted on an annual basis, modeled after NIST Special Publication 800-26, Self-Assessment Guide for Information Technology Systems. These procedures will be adapted to the new target environment as the applications are migrated.

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? If so, describe these controls.

All information stored in VBA databases is secured in agreement with VA strategy. 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, and annual cyber security training, and have signed rules of behavior. All security controls are implemented through a cohesive security structure and is 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 has been 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 the 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.

An annual assessment of security controls is currently conducted and will continue to be conducted to ensure that IT security requirements are being met. 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.

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)

First PIA

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.

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.)

The project team will review the data retention periods identified in Section Seven in an effort to identify best practices and to meet Government guidelines for data retention.

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 assessment⁹. 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)

John Quigley 09/15/2007

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