# APPENDIX J - Region 5 VBA VBAVACO LAN PIA

**Privacy Impact Assessment / Region 5 > VBA > VBAVACO > LAN**

**PRIVACY IMPACT ASSESSMENT 2008**

**INTRODUCTION:**

*Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.*

*To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person. Appendix A, "Applicable Legal and Regulatory Requirements" summarizes the applicable legal and regulatory requirements that are addressed by the PIA process.*

*Update regarding PIV projects: Federal Information Processing Standards Publication (FIPS PUB) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors and subsequent OMB guidance explicitly require PIAs for PIV projects collecting any personal data, not just of the public.*

*Primary Privacy Impact Assessment objectives include:*

*o Ensure and promote the trust and confidence of Veterans and the general public.*

*o Ensure compliance with the eGov Act and other applicable privacy laws, regulations and policies, including the PIV regulations.*

*o Identify the risks and adverse effects of collecting, maintaining and disseminating personal information in electronic information systems.*

*o Evaluate and develop protections and alternative processes for handling information to mitigate potential privacy risks.*

*Additional important objectives include:*

*o Provide a mechanism for ensuring responsibility and accountability for privacy issues.*

*o Provide documented assurance that privacy, security and other vital data stewardship considerations are integrated into information technology systems, starting with the initial outlining of a project's objectives and data usage requirements and continuing through design, operation, maintenance and disposal.*

*o Ensure that decision-makers are provided the information required to make informed system design or procurement decisions, based on an understanding of privacy risk, and of options available for mitigating that risk.*

*o Greatly reduce the risk of needing to interrupt a program or service because privacy and other vital data stewardship considerations were not adequately addressed before the program or service was implemented.*

*o Promote awareness and understanding of privacy issues.*

*o Provide valuable documentation on the flow of personal information, and related privacy considerations and design decisions.*

*Completion of this PIA Form:*

*o Part I (Sections 1 and 2) of this form must be completed for all projects. Part I documents basic project information and establish whether a full PIA is required.*

*o This entire PIA Form (Parts I and II) must be completed/updated every year for all projects with information technology (IT) systems that collect, maintain, and/or disseminate "personally identifiable information" information that may be used to identify a specific person of the public, OR is a PIV project.*

*Important Note: While this form provides detailed instructions for completing a Privacy Impact Assessment for your project, support documents that provide additional guidance are available on the OCIS Portal (VA network access required).*

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

### 1. PROJECT IDENTIFICATION:

#### 1.1) Project Basic Information:

*1.1.a) Project or Application Name:*

**Region 5 > VBA > VBAVACO > LAN**

*1.1.b) OMB Unique Project Identifier:*

029-00-02-00-01-1120-00

*1.1.c) Concise Project Description*

*Provide a concise description of the project. Your response will be automatically limited to approximately 200 words, and should provide a basic understanding of the project, and its most essential elements. (If applicable, use of personal data is to be described in Section 3.)*

The VBAVACO LAN is a general support system providing identification & authentication and access control. Primarily, it provides administrative support to the VBAVACO staff, such as electronic mail, Intranet and Internet connectivity services for approximately 800 plus VBA users, file and printer sharing, as well as access to VA Headquarters administrative applications, applications under development, and the VBA production applications that are used in the regional offices. The Central Office is rarely involved in the direct processing of veterans' benefits. More typically, the applications are used in special, high visibility cases or to provide management oversight, quality assurance, or produce summary information about RO workloads.

*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.*

N/A

#### 1.2) Contact Information:

| | |
|---|---|
| **1.2.a) Person completing this document: Gregory H. Johnson** | |
| **Title: Director, Region Five Security Service** | |
| **Organization: Veterans Benefits Administration** | |
| **Telephone Number: (202) 461-9174** | |
| **Email Address: gregory.johnson6@va.gov** | |
| **1.2.b) Project Manager: Kevin Causley** | |
| **Title: Director, OI&T Field Operations, Region Five** | |
| **Organization: Office of Information & Technology (OI&T)** | |
| **Telephone Number: (202) 461-9170** | |
| **Email Address: Kevin.Causley@va.gov** | |
| **1.2.c) Staff Contact Person: Anne Moroz** | |
| **Title: Chief, Network Security Operations** | |
| **Organization: Veterans Benefits Administration** | |
| **Telephone Number: (202) 461-9255** | |
| **Email Address: Anne.Moroz@va.gov** | |
| | |

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

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 1 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

## 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 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 13 and affirm.***

*2.c) Has a previous PIA been completed within the last three years?*

*No.*

*2.d) Has any changes been made to the system since last PIA?*

*No*

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

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 2 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

## Part II. Privacy Impact Assessment

### 3. PROJECT DESCRIPTION:

*The purpose of NIST SP 800-60 is to address recommending the types of information and information systems to be included in each category of potential security impact. Using NIST SP800-60, 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 VBAVACO LAN is a general support system (GSS) that supports access to VA HQ administrative and VBA production applications that are used in the regional offices. Although the Central Office is rarely involved in the direct processing of veterans' benefits other than viewing data, it is a strong possibility for employees in creating reports or performing analysis for quality control, performance monitoring, Congressional inquiries to store extracted files containing Personal Identifiable Information (PII) and rating decisions data (based on medical diagnosis) on the network. This is done for a variety of reasons in support of the VBA mission to process veteran benefits under U.S.C Title 38 to include but not limited to temporary storage of unstructured data while working a case, for reference purposes, or to assist in case management.

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

Title 38, United States Code, chapter 3, section 210(c) (1), chapters 21, 30 and 37; Title 38, United States Code, section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 34, 35, 36, 39, 51, 53, 55, Sections 901 and 903 PL96-342, PL98-77, PL102-484, 10 USC 106

*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.*

1,000,000 – 9,999,999

*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.*

Operation/Maintenance

*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.*

12 yrs.

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

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and hit submit and then select "Yes" and hit submit. |
| | 4/1/08 | **Section Update Date** |

**Section 3 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

**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.***

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

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

58VA21/22

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

Compensation, Pension, Education, and Rehabilitation Records-VA

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

http://www.va.gov/oit/egov/rms/sor_records.asp

***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?*

No.

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

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

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

No.

*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.)*

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update date** |

**Section 4 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

## 5. DATA COLLECTION:

### 5.1 Data Types and Data Uses

*FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. 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.)** |

The VBA benefit systems accessed through the LAN, 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 accessed through the LAN 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. Most of the information provided above is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.

| Yes | **Other Personal Information of the Veteran or Primary Subject** |
|---|---|

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

Other personal information accessible through the LAN includes: bank account information, employment history, gross income and net worth information, etc. Intended use is to determine, award, and pay eligible individuals VA benefits. Most of the information provided above is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.

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

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

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. Most of the information provided above is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.

| 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. Most of the information provided above is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.

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

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

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. Most of the information provided above is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.

| | |
|---|---|
| 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. Most of the information provided above is kept in a central database not located at

this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.

| 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. Most of the information provided above is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.

| 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. Most of the information provided above is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.

| 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. Most of the information provided above is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.

| 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.*

Social Security Administration information including awards and monetary amounts based on receipt of SSA disability income, supplemental income, and retirement benefits. Intended to determine entitlement to VA compensation and pension benefits. Most of the information provided above is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.

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

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 5.1 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

**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 veteran's enrollment and attendance. Information is used to process education benefits. Other information is collected from public sources (i.e., websites or databases) in order to locate
and contact the veteran and develop information to support the veteran's claim.

| 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.*

To determine eligibility for veterans benefits, all VA IT systems such as BIRLS, VA Insurance System, Corporate Databases, and information from VISTA (Veterans Health Administration system) are used

| 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 verifies if a veteran is deceased. The Social Security Administration also verifies if a veteran is deceased and provides income verification, SSN match. Department of Defense (DFAS) 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 Bureau of Prisons, Department of Health and Human Services, Defense Manpower Data Center, 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.*

N/A.

Yes **Other Source(s)**

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.

*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.*

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

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 5.2 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

**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.*

| | | |
|---|---|---|
| No | **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.")*

| | | |
|---|---|---|
| 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.*

Common Security Services (CSS) User Access Request form (VA Form 20-8824e) is used to approve access to VA applications and data; Notification of an Employee or Employee-Relative Claims File (VA Form 20-0344a)

| | | |
|---|---|---|
| No | **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.)*

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

| | | |
|---|---|---|
| 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. VBA employees may also contact a veteran directly to obtain clarifying information for a claim for benefits.

| | | |
|---|---|---|
| No | **Other Collection Method:** | Information is collected through a method other that 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.)*

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 5.3 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

**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?*

Mandatory

*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 for web applications is provided on the website (http://www.va.gov/privacy/index.htm). The CSS User Access Request Form (VA Form 20-8824e) requires all users who need access to VBA systems from Central Officer provide their SSN for identification purposes. The current form is for internal use (and Veteran Service Organizations) and does not provide a Privacy Use statement. 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.)*

| | |
|---|---|
| | **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:*

*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.*

The following link on the web form site tells subjects what the VA's privacy policy is, how the information is stored and collected, and how it will be kept secure - http://www.va.gov/privacy/

| 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.*

The following Written notice is 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.

| No | **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?*

N/A

| No | **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?*

N/A

| | |
|---|---|
| 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.*

N/A

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

N/A

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | **X** | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 5.4 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

**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.*

| y/n? | **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.*

| y/n? | **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.*

| y/n? | **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.*

| y/n? | **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.*

| y/n? | **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.*

| y/n? | **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.)*

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 5.5 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and |

| | | |
|---|---|---|
| | | submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

## 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 is stored within the databases, which support the individual claim or claims the veteran has been granted. The LAN accesses these databases to retrieve the data.

*5.6.b) How is data checked for completeness?*

Data is 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.)*

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 5.6 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

**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** |

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

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

(1) WebHINQ enables VHA to retrieve data from the corporate database and BIRLS. WebHINQ retrieves 4 pieces of data when the record is stored in the 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.

** Data that is shared – information about a veteran's service connected disability (affected extremity, original effective date of the disability rating and the current (most recent) date the rating was changed, and the effective date of the combined service connected evaluation)

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

** Data that is shared – PII information to include but not limited to veteran's name, address, contact information, and medical records (treatment records, lab information, appointment information)

*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.*

| | |
|---|---|
| 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.

The above service organizations include all accredited service organizations. The following site has a complete list of recognized veterans service organizations - http://www.va.gov/ogc/recognizedvsos.asp.

** Data that is shared - 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 accessed through the LAN 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 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.*

| 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.*

Data in the VBA Corporate database and the Benefits Delivery Network database are accessed primarily to support the applications running on the LAN.

** Data that is shared - 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 accessed through the LAN 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.
All users of the system are responsible for the privacy of this information. Users are trained annually on their privacy responsibilities.

| | |
|---|---|
| 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 VBA employees that are authorized to access and process veterans claims are proved specific password that allow them to obtain or access data within the VBA Corporate system. 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. 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 Requesting Official with approval from the Director and/or Information Security Officer, depending upon the level of access requested. |
| *6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents.* |
| Yes – VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4 |
| *6.1.d) Will users have access to all data on the project systems or will user access be restricted? Explain.* |
| Per VA Directive 6500, user access is restricted to a need to know basis. 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 screen |
| *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)* |
| AU-2 (Auditable Events) - Most of the major applications that run on the LAN have built in alerts that are flagged if anyone tries to access any veteran data outside of their individual authorization permissions. AU-6 (Audit Monitoring) - These alert messages are compiled into daily reports that are provided to the Information Security Officer and are reviewed to verify what incidents took place. Depending on the degree of error, corrective action is followed through. All access can be tracked to individual end-users to identify any unauthorized attempts to access veterans' records. PL-4 (Rules of Behavior) - Users also sign a Rules of Behavior prior to system access and annually thereafter. AT-3 (Security Training) – Users also take an annual security awareness training course that reaffirms to them what constitutes authorized use. |
| *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)* |
| No. Although personal information is accessed by non-VA entities as system users (ie, service organizations), the information is not shared outside the boundaries of the system |
| ***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.* |

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

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

*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.*

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

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

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

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 6.1 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |

| | | |
|---|---|---|
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

## 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.** |
| No | **The application will provide a phone number of a VA representative who will provide instructions.** |
| Yes | **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?*

Individuals may request information concerning their benefits/claims status from the VBA Regional Office in their area either in writing or by calling the 1-800 number. In addition, individuals may also request their information under the Freedom of Information Act or the Privacy Act. Once a formal request is received (no official form, but it must be in writing with the veteran's signature), the VA will process the request and send the requesting information back to the veteran via mail.

*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 VA. Once a formal request is received (no official form, but it must be in writing with the veteran's signature), the VA will process the request and correct the erroneous information and then let the veteran know of their actions in writing.

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

**N/A**

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

**N/A**

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

**N/A**

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

## Section 6.2 Review:

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

## 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 retention policies and procedures are being updated. The updates will be completed by the end of FY2008. The update will evaluate existing data retention practices against current best practices and department and Federal Government guidance. The current retention periods can be found in VA Handbook 6300.5 and Records Control Schedule (RCS) VBA-1, Part 1, Section 8 available online at http://www.warms.vba.va.gov/admin23/part1/sec08.doc |
| *7.b) What are the procedures for eliminating data at the end of the retention period?* |
| In general, support systems retain information until that work in progress is completed and data is committed to master systems and records. The master systems retain data on a permanent basis (beyond the actual death of the veteran). If incidental data is maintained in a user's personal folder on the network, that data is deleted from the system when the employment is terminated. Deleting this information is a form of media wiping, which is acceptable because the server is reused within VA. Once the server reaches end of life, the device is physically destroyed. |
| *7.c) Where are procedures documented?* |
| VA Handbook 6300.5 and Records Control Schedule (RCS) VBA-1, Part 1, Section 8 available online at http://www.warms.vba.va.gov/admin23/part1/sec08.doc and the Systems of Record 58VA21/22 and 38VA23 |
| *7.d) How are data retention procedures enforced?* |
| 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.)* |
| |
| |

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

## Section 7 Review:

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

## 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 LAN. 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. 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 PO&AM 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 (Physical security controls are documented in the VBAVACO LAN System Security Plan)

**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 OI&T, 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 privacy 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 are 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

| *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 guidelines, policies, and mandates. |
| *8.2.c) Explain what security risks were identified in the security risk assessment.* |
| Unauthorized Physical Access to Facility; Forceful Occupation; Riot/Civil Disorder; Fire Related Threat; Wind Related Threat; Seismic Related Threat; Water Related Threat; Total Loss of Electrical Service; Temperature and Humidity Control Service; Bandwidth Usage; Telecom Interruption; System Configuration Error (Accidental); Alteration of Software; Theft; Illegal Use of Resources; Information Browsing; Administrative Errors; Unauthorized Software Installed; Receipt Denies Receiving Information; Sender Denies Sending Information; Participant Denies Performing a Transaction; Bomb Threat; Vandalism; Chemical/Biological Attack; Fraud, Waste, or Abuse; Penetration; Hardware Failure; Failure of a distributed system component. |
| *8.2.d) Explain what security controls are being used to mitigate these risks.* |
| Physical access controls exist via magnetometer, x-ray machine, cameras, and VA police. The guards check the photo ID of every visitor and they must sign in as well. However, entry controls can be bypassed via emergency release. Accept risk, there are several layers of physical security defense in place.<br><br>The physical security in the building is sufficient to eliminate this threat i.e. Guards, x-ray machine, magnetometer, cctv, cipher locks. In addition, VA Law Enforcement, Washington Metro police available for mitigating such activities.<br><br>DVA OLE&S officers on site.<br><br>Local fire department is relatively close; There are sprinklers through out the building; The CR contains a sprinkler and detectors for smoke, noise and temperature and a floor drain to allow water to escape; Fire drills are conducted on a regular basis.<br><br>Accredited according to GCAHO standards.<br><br>Building is not retrofitted for earthquake contingences. Accept risk. Review, test and update continuity of operations plan.<br><br>The Computer Room (CR) has a raised floor and a floor drain in the room to allow liquids to runoff.<br><br>CR has UPS capability to allow for gracefully shutdown.<br><br>High humidity area. Humidity/environmental controls in place.<br><br>Employee education. |

Certain pre-approved employees could work from their homes, or off site offices. Benefit processing workload could be shifted to other Regional Offices. Employees could be temporality relocated to satellite offices.

Accept risk, review service level agreements with local telecommunication providers to ensure priority restoration of telecommunication circuits. Review, test and update continuity of operations plan.

IT staff works as a team to develop procedures for inserting new hardware or software into LAN environment.

Extensive security awareness and training program in place. IT staff works as a team to develop procedures for inserting software into LAN environment. Authorized changes to LAN environment are instituted as directed by Hines.

Supplies and portable equipment are locked.

Employee education. Rules of Behavior or user access agreements are maintained on file.

Employees sign agreements for various accesses to applications and programs that detail rules of behavior, privacy, illegal and unauthorized use. Windows 2000 implementation provides standardized least privilege and access permission management controls.

Annual background checks are conducted on all system administrators. Management controls policy established.

Employee education. Windows 2000, System Update Server (SUS), and configuration controls in place. Common users locked down to VBA-wide standard image that prevents users from installing or downloading.

Generally, discovery of a user receiving a message comes from an outside source allowing time for validation. Upon which, appropriate action is taken with respect to reporting requirements and discipline, if necessary. Non-repudiation being addressed in the Authentication and Authorization Infrastructure Project (AAIP).

Mitigated through CSUM, and Common System Security (CSS).

Emergency electronic broadcast and audible alerting system in place for rapid building-wide notification.

Some spare hardware is available at RO, however, primary router spare is not available and RO Information Technology (IT) staff does not have admin user accounts on the primary router. Arrangements are in place for overnight shipment, if necessary.

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 8 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

**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.* |

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETE** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 9 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

| |
|---|
| *PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)* |
| |

**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.)* |

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 10 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

**11. PIA Assessment**

*11a) 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 on VBA/Region Five LANs are secured per VA security standards.

*11b) What auditing measures and technical safeguards are in place to prevent misuse of data?*

Full C&A every three years. During FISMA continuous monitoring (non C&A cycle) Region Five 1/3 of controls are re-tested annually per VA Handbook 6500. Patch management includes use automated tools, e.g. VBA Menu XXX, ACRB, Austin AC Computer Associates Unicenter, to effectively manage Operating system patches (UNIX and Windows). Use of User ID and strong passwords are required for access. Technical controls minimize risk through "Least privilege" and internal controls (e.g. can't create and approve same veteran payment). Inactive accounts are automatically disabled after 90 days of non-use. Security software incorporates Power of Attorney (POA) restrictions and Sensitive Record management features (aka celebrity file) further restricting general access to the veteran data. Mandatory use of pre-set screen saver set at 15 minutes on workstations provides physical barrier to unauthorized access. Audit files record user activity. Security reports track activity in the Sensitive/POA files. Please see 6.1.e

*11c) Availability assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?*

| | |
|---|---|
| No | **The potential impact is <u>high</u> if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.** |
| Yes | **The potential impact is <u>moderate</u> if the loss of availability could be expected to have a serious adverse effect on operations, assets, or individuals.** |
| No | **The potential impact is <u>low</u> if the loss of availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.** |

*11d) Integrity assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?*

| | |
|---|---|
| No | **The potential impact is <u>high</u> if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.** |
| Yes | **The potential impact is <u>moderate</u> if the loss of integrity could be expected to have a serious adverse effect on operations, assets, or individuals.** |
| No | **The potential impact is <u>low</u> if the loss of integrity could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.** |

*11e) Confidentiality assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization?*

| | |
|---|---|
| No | **The potential impact is <u>high</u> if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.** |
| Yes | **The potential impact is <u>moderate</u> if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets, or individuals.** |
| No | **The potential impact is <u>low</u> if the loss of confidentiality could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.** |

*11f) What was the highest impact from questions 11c, 11d, and 11e?*

*Moderate for all.*

*11g) What controls are being considered for this impact level?*

All security controls required for a Federal Information Processing Standard (FIPS) 199 level of moderate as documented in NIST Special Publication 800-53, are implemented or planned for this LAN. Documented security controls can be found in the VBAVACO LAN System Security

Plan.

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

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 11 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

**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:*

N/A

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

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 12 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*

**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.*

04/01/08

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

Kevin Causley, Acting Director OI&T Field Operations Region 5

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

| | | |
|---|---|---|
| | | **SECTION INCOMPLETE** |
| | X | **SECTION COMPLETED** |
| | **MDB** | I have completed and reviewed my responses in this section. |
| ** | **NOTE:** | If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again. |
| | 4/1/08 | **Section Update Date** |

**Section 13 Review:**

| | | |
|---|---|---|
| | | **PRIVACY SERVICE SECTION REVIEW AND APPROVAL** |
| | | The Privacy Service has not reviewed this section. |
| | | The Privacy Service has reviewed this section. Please make the modifications described below. |
| | | The Privacy Service has reviewed and approved the responses in this section. |
| ** | **NOTE:** | If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit |
| | | and then select "Yes" and submit again. |
| | | **Section Review Date** |

*PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)*