

PIA SECTIONS 1 - 4

Part I. Project Identification and Determination of PIA Requirement

1. PROJECT IDENTIFICATION:

1.1) Project Basic Information:

1.1.a) Project or Application Name:

VETSNET-2009

1.1.b) OMB Unique Project Identifier:

029-00-01-13-01-1264-00

1.1.c) Project Description

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

VETSNET Compensation and Pension (C&P) is a suite of applications that facilitates the entire C&P claims process. Within the suite, the end user can establish and develop veterans' claims; the rating decision, award and notification letter are documented, and payment information is transmitted to Treasury, accomplishing the necessary accounting. Throughout these activities, data are shared and passed between the applications to support end-to-end claims processing, customer service and notification.

This investment effectively contribute towards VA's Strategic Goal 1 - Restore the capability of veterans with disabilities to the greatest extent possible and improve the quality of their lives and that of their families, and Goal 3 - Honor and serve veterans in life, and memorialize them in death for their sacrifices on behalf of the Nation.

Currently, VA's mission is being supported by the Benefits Delivery Network (BDN). VETSNET C&P is targeted to replace the C&P functions of the BDN, currently in maintenance phase. BDN has passed its system's lifecycle and minimal tools are available to support it. Additionally, various material weaknesses have been identified related to BDN's lack of compliance with the government-wide Standard General Ledger, lack of automated audit trail, and other shortcomings such as over payment errors.

Oversight for the VETSNET investment is provided by the VETSNET Executive Team. The Executive Team is an interdisciplinary team led by a Senior Executive well-versed in C&P processes. The team is responsible for the day to day execution of the project. Strategic direction is provided by the VETSNET Executive Board (VEB). The VEB meets on a regular basis to monitor and control investment progress. VETSNET is a fundamental component of VA's Enterprise Architecture in providing critical C&P informational support to its customers through an integrated and technologically sound environment.

1.1.d) Additional Project Information (Optional)

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

1.2) Contact Information:

<b>1.2.a) Person completing this document:</b>	
<b>Title:</b>	Dianne Thompson, VA Level III PM
<b>Organization:</b>	Technical Project Manager, VETNEST Program Management Office (VPMO)
<b>Telephone Number:</b>	202-461-9214
<b>Email Address:</b>	dianne.thompson1@va.gov

<b>1.2.b) Project Manager:</b>	
<b>Title:</b>	Dianne Thompson, VA Level III PM
<b>Organization:</b>	Technical Project Manager, VETNEST Program Management Office (VPMO)
<b>Telephone Number:</b>	202-461-9214
<b>Email Address:</b>	Dianne.thompson1@va.gov
<b>1.2.c) Staff Contact Person:</b>	
<b>Title:</b>	Kim Graves
<b>Organization:</b>	Director, VBA Office of the Undersecretary of Benefits
<b>Telephone Number:</b>	202-461-9374
<b>Email Address:</b>	kim.graves@va.gov

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


## 2. DETERMINATION OF PIA REQUIREMENTS:

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

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

Yes

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

No

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

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

VETSNET maintains veteran information needed to process claims.


## Part II. Privacy Impact Assessment

### 3. PROJECT DESCRIPTION:

Enter the information requested to describe the project.

3.a) Provide a concise description of why personal information is maintained for this project, such as determining eligibility for benefits or providing patient care.

The mission of the VETSNET C&P program is to provide monthly payments to veterans in recognition of the effects of

disabilities, diseases, or injuries incurred or aggravated during active military service, and to provide access to other VA benefits. The mission of the Pension program is to provide monthly payments to needy wartime veterans who are permanently and totally disabled as a result of disability not related to military service. Information is collected to provide all entitled benefits in the most complete and effective manner.

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, section 210(c) and Chapters 11, 13, 15 31, 34, 35, and 36; 38 U.S.C. chapter 30, 10 U.S.C. chapter 106, Pub. L. 102-484, Pub. L. 98-77

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.

(1) Design/Planning

3.e) Identify either the approximate date (MM/YYYY) the project/system will be operational (if in the design or development stage), or the approximate number of years that the project/system has been in operation.

09/2009

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

#### 4. SYSTEM OF RECORDS:

The Privacy Act of 1974 (Section 552a of Title 5 of the United States Code) and VA policy provide privacy protections for employee or customer information that VA or its suppliers maintain in a System of Records (SOR). A SOR is a file or application from which personal information is retrieved by an identifier (e.g. name, unique number or symbol). Data maintained in a SOR must be managed in accordance with the requirements of the Privacy Act and the specific provisions of the applicable SOR Notice. Each SOR Notice is to be published in the Federal Register. See VA Handbook 6300.5 "Procedures for Establishing & Managing Privacy Act Systems Of Records", for additional information regarding Systems of Records.

4.a) Will the project or application retrieve personal information on the basis of name, unique number, symbol, or other identifier assigned to the individual?

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

Yes

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

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

Yes

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

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

58VA21/22/28

(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/cio/foia/systems\\_of\\_records.asp](http://www.va.gov/oit/cio/foia/systems_of_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?

Created for another project or system

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

The original System of Record was identified as part of the Beenfits Delivery Netowrk initiative which stores Compensation, Pension, education and vocational rehabilitation data required to generate benefit payment to our nation's

veterans.

4.b.4) Does the System of Records Notice require modification?  
 If "No" then skip to section 5, 'Data Collection'.

Modification of the System of Records is Required

4.b.5) Describe the required modifications.  
 The modifications will reflect the corporate database environment as the SORN once all BDN data is migrated to this new system

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.)

Although the Share application is not primary, it integrates with BDN, BIRLS, and Corporate which are Systems of Records.

**PIA SECTION 5**

**Project Name**

VETSNET-2009

**5. DATA COLLECTION:**

**5.1 Data Types and Data Uses**

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

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

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

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

Yes	<b>Veteran's or Primary Subject's Personal Contact Information (name, address, telephone, etc.)</b>
-----	---

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

Personal contact information: Name, address, Social Security Number, telephone number, family/dependents, marital status, medical status, birth information, death information. Intended use of information is to communicate with individuals regarding entitlement to VA compensation and pension benefits and deliver appropriate level of benefit programs.

Yes	<b>Other Personal Information of the Veteran or Primary Subject</b>
-----	---

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

Other personal information includes: bank account information, employment history, gross income and net worth information, etc. Intended use of information is to determine, award, and pay eligible individuals VA compensation and pension benefits.

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

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

Veteran Dependent Data: Personal information including name and address, age, school status, relationship to the veteran, medical status, SSN.

Intended use of information is to calculate monetary amount of VA pension benefits where entitlement is established.

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

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

Service data information: Active, Reserve and Guard Participation; retired pay or severance pay; hazardous agent exposure; Branch of service; duty date; release date; type of discharge; separation reason.

Intended use of information is to determine eligibility for VA compensation and pension benefits.

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

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

Medical Records: Military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations.

Intended use of information is to determine entitlement to VA compensation and pension benefits.

No	<b>Criminal Record Information</b>
----	------------------------------------

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

No	<b>Guardian Information</b>
----	-----------------------------

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

No	<b>Education Information</b>
----	------------------------------

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

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

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

Yes	<b>Other Personal Information (specify):</b>
-----	--

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

Social Security Administration information, including awards and monetary amounts based on receipt of SSA disability income, supplemental income, and old age / retirement benefits.

Intended use of information is to determine entitlement to VA compensation and pension benefits.

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

## 5.2 Data Sources

Identify the source(s) of the collected information.

a) Select all applicable data source categories provided below.

b) For each category selected:

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

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

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

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

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

Information is collected from Veterans to determine veteran eligibility for compensation and pension benefits.

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

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

Information is collected from the identified sources in order to locate and contact the veteran and develop information to support the veteran's claim.

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

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

The BIRLS, BDN and Corporate databases are used to determine veteran eligibility for compensation and pension benefits.

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

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

To determine eligibility for veterans benefits. Data input provided from the SSA for income verification, SSN match; SSA benefit information or death file notices; DoD (DFAS) data input, e.g. DD Form 214; and information from the Internal Revenue Service for income verification. Verification with Department of Treasury payment history files; returned checks; Defense Manpower Data Center for military reserve status, verification of active duty date; and monthly interfaces from DoD, DFAS, Coast Guard, and DHHS.

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

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

Data input provided from State National Guard and Reserve Units to determine eligibility for veterans benefits.

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

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

No	Other Source(s)
----	-----------------

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

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

### 5.3 Collection Methods

Identify and describe how personal information is collected:

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

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.

21-0510Eligibility Verification Reports 21-0511S 21-0511S-1 21-0511V 21-0511V-1 21-0512S 21-0512S-1 21-0512V 21-0512V-1 21-0513 21-0538Status of Dependents Questionnaire, 21-2545Report of Medical Examination for Disability Evaluation 21-4138Statement in Support of Claim. 21-4169Supplement to VA Forms 21-526, 21-534, and 21-535 (For Philippine Claims) 21-4171Supporting Statement Regarding Marriage, 21-8951-2Notice of Waiver of VA Compensation or Pension to Receive Military Pay and Allowances 21-0571Application for Exclusion of Children's Income, 21-8924Application of Surviving Spouse or Child for REPS Benefits (Restored Entitlement Program for Survivors), 21-8941REPS Annual Eligibility Report, 21-674 21-674B 21-674CRequest for Approval of School Attendance - VA Form 21-674 and VA Form 21-674c. School Attendance Report- VA Form 21-674b, 21-8416BReport of Medical, Legal, and Other Expenses Incident to Recovery for Injury or Death, 21-534Application for Dependency and Indemnity Compensation, Death Pension and Accrued Benefits by a Surviving Spouse or Child (Including Death Compensation if Applicable), 21-4502Application for Automobile or Other Conveyance and Adaptive Equipment (Under 38 U.S.C. 3901-3904), 21-4709Certificate As To Assets, 21-4185Report of Income from Property or Business, 21-8938Student Beneficiary Report -- REPS 21-8960, 21-8960-1Certification of School Attendance or Termination, 21-4176Report of Accidental Injury In Support of Claim for Compensation or Pension/Statement of Witness to Accident. 21-22, 21-22AAppointment of Veterans Service Organization As Claimant's Representative (21-22), Appointment of Individual as Claimant's Representative (21-22A). 21-2008Application for United States Flag for Burial Purposes 21-530AState Application for Interment Allowance Under 38 U.S.C, 21-4703Fiduciary Agreement, 21-4706, 21-4706B, 21-4706C, 21-4718, 21-4718A Court Appointed Fiduciarys Account (letter size), Federal Fiduciary's Account, Account Book, and Court Appointed Fiduciary's Account (legal size), Certificate of Balance on Deposit and Authorization to Disclose Financial Records, 21-526Veteran's Application for Compensation and/or Pension 21-0307Spina Bifida Award Attachment Important Information, 21-0161AIncome Verification, 21-0304Application for Spina Bifida Benefits 21-0537Marital Status Questionnaire, 21-535Application for Dependency and Indemnity Compensation by Parent(s) (Including Accrued Benefits and Death Compensation When Applicable), 21-527Income -Net Worth and Employment Statement, 21-4192Request for Employment Information in

Connection with Claim for Disability Benefits, 21-686CDeclaration of Status of Dependents, 21-0779Request for Nursing Home Information in Connection with Claim for Aid and Attendance, 21-530Application for Burial Benefits. 21-8049Request for Details of Expenses, 20-0344Annual Certification of Veteran Status and Veteran-Relatives, 21-4165Pension Claim Questionnaire for Farm Income, Obligation to Report Factors Affecting Entitlement, (38 CFR 3.204(a)(1), 38 CFR 3.256(a) and 38 CFR 3.277(b)), 21-509Statement of Dependency of Parent(s), 21-1775Statement of Disappearance

No	<b>Electronic File Transfer:</b>	Information stored on one computer/system (not entered via a Web Form) and transferred electronically to project IT systems.
----	----------------------------------	--

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

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

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

The various media used are primarily electronic file transfers and batch updates. The process used is TCP/IP connections with Secure FTP encryption.

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

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

The VBA toll free number for benefits is 1-800-827-1000. The Telecommunications Device for the Deaf (TDD) toll free telephone number is 1-800-829-4833. The veteran is directed 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 via the existing services, guidance is provided on how to obtain forms and instructions for mail-in requests. Additionally, information for hospital inquiries and/or services are provided to the veteran and/or claimant.

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

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

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

Additional forms from "Paper Form Media": 21-914Residency Verification Report-Veterans and Survivors, 21-863Request for Information to make Direct Payment to Child Reaching Majority 21-8940Veteran's Application for Increased Compensation Based on Individual Unemployability. 21-4103Information from

Remarried Widow(er)  
 21-524Statement of Person Claiming to Have Stood in Relation of Parent, 21-4170Statement of Marital Relationship, 21-30Request for Contact Information, 21-8926Certification of School Attendance – REPS, 21-4193Notice of Department of Veterans Affairs of Veteran or Beneficiary Incarcerated in Penal Institution, 21-601Application for Accrued Amounts Due a Deceased Beneficiary, 21-4140, 21-4140-1Employment Questionnaire  
 21-0781, 21-0781aStatement in Support of Claim for Service Connection for Post-Traumatic Stress Disorder (PTSD), Statement in Support of Claim for Service Connection for Post-Traumatic Stress Disorder (PTSD) Secondary to Personal Assault. 21-8416Medical Expense Report

**5.4 Notice**

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

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

Yes

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

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

Voluntary

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

The C&P forms and the VBA website include a statement similar to the following: "Important Notice About Information Collection. We will collect personally identifiable information (name, email address, Social Security number, or other unique identifier) only if specifically and knowingly provided by you. Personally identifying information you provide will be used only in connection with VA programs and services or for such other purposes as are described at the point of collection."

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

Ongoing

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

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

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

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

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

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

No	<b>Web Forms:</b>
----	-------------------

Explain:

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

Link to VA site on Privacy, Freedom of Information, and Security. The privacy of our customers has always been of utmost importance to the Department of Veterans Affairs. The VA has a long history of protecting your privacy and our concern for your privacy is no different in the electronic age. Our Internet privacy policy is: You do not have to give us personal information to visit our site. We will collect personally identifiable information (name, email address, Social Security number, or other unique identifier) only if specifically and knowingly provided by you. Personally identifying information you provide will be used only in connection with VA programs and services or for such other purposes as are described at the point of collection. Information is collected for statistical purposes and VA sometimes performs analyses of user behavior in order to measure customer interest in the various areas of our site. We do not give, sell or transfer any personal information to a third party. We may enable "cookies." A "cookie" is a file placed on your personal computer's hard drive by a Web site that allows it to monitor your use of the site. The Privacy Act of 1974 applies to all Federal agencies. For information on the Federal government's Web Site Privacy Policy, see the following documents: VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act VA Handbook 6300.5, Procedures for Establishing & Managing Privacy Act Systems of Records.

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

Explain:

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

Written notice on all VA forms. PRIVACY ACT INFORMATION: No allowance of compensation or pension may be granted unless this form is completed fully as required by law (38 U.S.C. 5101). The responses you submit are considered confidential (38 U.S.C. 5701). VA may disclose the information that you provide, including Social Security numbers, outside VA if the disclosure is authorized under the Privacy Act, including the routine uses identified in the VA system of records, 58VA21/22 Compensation, Pension, Education, and Rehabilitation Records - VA. The requested information is considered relevant and necessary to determine maximum benefits under the law. Information submitted is subject to verification through computer matching programs with other agencies. VA may make a "routine use" disclosure for: civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA programs and delivery of VA benefits, verification of identity and status, and personnel administration. The requested information is considered relevant and necessary to determine maximum benefits under the law. Information that you furnish may be utilized in computer matching programs with other Federal or state agencies for the purpose of determining your eligibility to receive VA benefits, as well as to collect any amount owed to the United States by virtue of your participation in any benefit program administered by the Department of Veterans Affairs

No	<b>Electronic File Transfer:</b>
----	----------------------------------

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

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

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

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

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

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

*Explain:*

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

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-in requests. Additionally, information for hospital inquiries and/or services are provided.

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

*Explain:*

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

NA

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

### 5.5 Consent For Secondary Use of PII:

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

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

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

No

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

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

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

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

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

Describe:

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

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

Describe:

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

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

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

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

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

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

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

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

Describe:

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

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

Describe:

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

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

## **5.6 Data Quality**

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

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

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

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

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

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

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

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

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

PIA SECTIONS 6 - 13

**Project Name**

VETSNET-2009

**6. Use and Disclosure**

**6.1 User Access and Data Sharing**

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

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

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

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

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

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

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

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

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

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

Contractors are granted access to the system on an as needed basis to resolve production issues. A government person would prepare the access request form and submit it for concurrence approval by management. The access is granted for a special purposes and a limited amount of time.

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

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

C&P services shares disability information with the VHA to enable the VHA to deliver the health services the veteran is eligible to receive. VBA also shares burial eligibility information with NCA.

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

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

A veteran may elect a VSO representative to act on his behalf. This requires a power of attorney be submitted by the veteran naming the VSO.

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

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

The system has documented Memorandums of Understanding Agreements with all of its VA business partners, federal agencies, state agencies and local agencies in regard to confidential business information, Privacy Act and certain information that is subject to confidentiality protections. The federal agencies mentioned are as follows: Department of Defense, Social Security Administration, Federal housing Administration, Internal Revenue Service, and Department of Housing and Urban Development.

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

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

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

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

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

*If information is shared with other projects or systems:*

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

Data in the VETSNET environment is "shared" with the BDN system. Since BDN is the system of record, payment data is managed within the BDN and transmitted to Treasury. Treasury uses the merged data to generate benefit payments

No	<b>Other User(s)</b>
----	----------------------

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

6.1.a.1) Describe here who has access to personal information maintained in project's IT systems:
All employees that are authorized to access and process veterans claims are provided specific passwords that allow them to obtain or access data within the VBA Corporate system. Approximately 12,000 end-users access the IT systems supporting this data. Veterans Service Organizations and attorney's that have power-of-attorney over the veteran have restricted read-only access.
6.1.b) How is access to the data determined?
Users are granted individual levels of authority privileges to view or process veterans claim information. The access levels are provided through strict controls and passwords assigned to individual end-users. There are logs of all passwords provided and the access levels granted. CSUM is the application responsible for performing this task. Reports are created which identify all access attempts both successful and unsuccessful to any information for a veteran with any level of sensitivity restriction. Creation of individual user IDs requires a written request with the approval being granted by Information Security Officers..
6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents.
Yes, VBA has strict control measures in place to prevent the inadvertent or deliberate release of information to non-authorized personnel.
6.1.d) Will users have access to all data on the project systems or will user access be restricted? Explain.
The end user access is restricted by the level of authority they require to perform their jobs. The systems include authorization at the application and function level. Users may have inquiry, update (sometimes sub-divided), or verifier authority to different screens.
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)
The C&P non-BDN systems have built in alerts that are flagged if anyone tries to access any veteran records outside of their individual authorization permissions. These alert messages are compiled into daily reports that are provided to the Information Security Officer (ISO) 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.
6.1.f) Is personal information shared (is access provided to anyone other than the system users, system owner, Project Manager, System Administrator)? (Yes/No)
Yes
Note: If you have selected No above, then SKIP to question 6.2, "Access to Records and Requests for Corrections".
6.1.g) Identify the measures taken to protect the privacy rights of the individuals whose data will be shared.
Controls to prevent misuse include signed Rules of Behavior statements of users, security policies and access procedures, strong passwords, security awareness training and audit trails. All veterans records that are accessed by users are coded by user identifiers.
6.1.h) Identify who is responsible, once personal information leaves your project's IT system(s), for ensuring that the information is protected.
Other systems do not access this data on-line; it is provided by interface files and becomes an appropriate a part of the receiving system controlled by the security functions associated with the receiving system.
6.1.i) Describe how personal information that is shared is transmitted or disclosed.
Transmission of data can be shared via a common database or via data transmission. If data transmission is done, the transmitting utility must be NIST 140.2 compliant.
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.
Yes, the system has documented Memorandums of Understanding Agreements with all of its business partners, veteran organizations, federal agencies, and state agencies in reference to access to veterans privacy data. This system has documented Memorandums of Understanding/Agreement with all of its business partners, including veteran organizations, federal agencies, state agencies, and contractors in regard to confidential business information, Privacy Act, and certain information that is subject to confidentiality protections. This includes all the entities mentioned previously within this document and includes the Department of Defense, and the Social Security Administration. A detailed listing of all business partners is available from the project manager.
6.1.k) How is the shared information secured by the recipient?

The recipients of any C&P data must sign a rules of behavior to assist in prevention of unauthorized disclosure of privacy information.

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

Unknown

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

## 6.2 Access to Records and Requests for Corrections

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

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

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

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. In addition, individuals may also request their information under the Freedom of Information Act. Employees are not allowed to access their own information directly through the system. The Privacy Act governs individuals access to their own information. Strong security measures are input in the Corporate environment that will not allow end users to access their own information. If they attempt, this violation is flagged and reports are generated by the Information Security Officers (ISO) and acted upon either at the local regional office level or at the data center.

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

Security logs are generated on a daily basis. VBA Regional Office ISO's receive reports that are reviewed for inconsistencies and can verify what access has been attempted. The ISO's produce monthly reports that are reviewed by the Hines Senior ISO to ensure no unauthorized access has been allowed into the non BDN systems. If any violations are detected, the appropriate officials are notified to correct the incident.

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

The Office of Field Operations and local Regional Office Director(s) are notified to remove/restrict and/or monitor end user access that is attempting to perform unauthorized access to veterans records.

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

Beneficiaries may request information from their local regional office by U.S. Mail.

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

## 7 Retention and Disposal

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

The "Retention and disposal" section of the applicable System of Records Notice(s) often provides appropriate and sufficiently detailed

documented data retention and disposal practices specific to your project.

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

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

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

or

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

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

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

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

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

**Start by looking at the <http://www.warms.vba.va.gov/20rcs.html>**

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.

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 a master system is to be deactivated, critical information is migrated to the new system and the old system along with associated data is archived according to the application disposition worksheet. Once archived, existing application code and files are deleted from the system. Data elimination procedures are also being updated. These procedures will be identified and implemented by the end of FY2008.

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. In addition, every action, which impacts a record, results in an audit record being created; this audit record is permanently retained.

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

Yes

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

## 8 SECURITY

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

### 8.1 General Security Measures

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

applicable boxes.):

Yes	The project is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured.
Yes	The project has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.
Yes	Security monitoring, testing, and evaluating are conducted on a regular basis to ensure that controls continue to work properly, safeguarding the information.

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

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

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

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

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

Yes

## 8.2 Project-Specific Security Measures

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

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

Note: Administrative and technical safeguards must be specific to the system covered by the PIA, rather than an overall description of how

the VA's network is secured. Does the project/system have its own security controls, independent of the VA network? Is so, describe these controls.

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

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

Annual assessments of security controls are conducted to ensure that IT security requirements are being met.

## 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)

No

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

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

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

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

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

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

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

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

New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic

information system accessed by members of the public;

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

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

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

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

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

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

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

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

## 10. CHILDREN'S ONLINE PRIVACY PROTECTION ACT

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

No

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

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

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

## 11. PIA CONSIDERATIONS

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

The VBA continually applies emphasis and attention to addressing security and privacy concerns including the assurance that collection of data and personal information contains appropriate consent and release information and that all information stored in VBA databases are secured per VA security standards. This is an agency-mandated activity performed across individual system boundaries. The PIA helped emphasize the need to revisit, review and update retention and disposal policies and procedures as was planned for 2008.

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

**12. PUBLIC AVAILABILITY**

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

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

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

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

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

No

*12.b) If yes, specify:*

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

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

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

Yes

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

Dianne Thompson 08/14/2007

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