

Privacy Impact Assessment - 2009 (Form) / Program Integrity/Data Management-2009 (Item)

Part I. Project Identification and Determination of PIA Requirement

1. PROJECT IDENTIFICATION:

1.1) Project Basic Information:

1.1.a) Project or Application Name:

Program Integrity/Data Management-2009

1.1.b) OMB Unique Project Identifier:

029-00-03-00-01-1014-00

1.1.c) Project Description

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

The Budget and Performance Integration Initiative in the PMA states, "Managers do not have timely and complete information with which to monitor and improve their results." Strategic Goal One of the 2006-2011 VA Strategic Plan states, "Restore the capability of veterans with disabilities to the greatest extent possible, and improve the quality of their lives and that of their families."

This investment bridges the gap between successfully meeting the objectives in Strategic Goal One while monitoring and improving program results. It is the foundation of VBA's business intelligence and program integrity initiative and provides direct support in meeting the objectives outlined in VA Strategic Goal One. In support of the PMA, this investment allows managers to have timely and accurate information to monitor and improve program results. This investment has improved VBA's decision-making capabilities and its organizational information management by using an enterprise data warehouse (EDW) as the central information repository. The VBA EDW is a business intelligence program that facilitates decision-making throughout all organization levels – business lines, regional offices, and management departments. VBA lacked the means to manage information, from a headquarters perspective, and make timely decisions to improve and positively affect the benefit programs managed by the lines of business. The EDW information reporting capabilities close these gaps and allow VBA to monitor workloads, check the status of cases, as well as prioritize and allocate appropriate resource levels to Regional Offices. Additionally, this business intelligence program enables VBA to provide timely and accurate reports to internal and external veteran stakeholders, including VA organizations, Veteran Service Organizations, Congress, and the Department of Defense. These reports tell one story from a single source rather than disparate messages presented from various VBA organizations. The information emanating from this centralized repository allows VBA to look, Administration-wide, at potential integrity flaws and shortcomings. Previous attempts to manage a data integrity program, from a headquarters level, fell short because of a lack of centralized information and a means to review and take timely action. The VBA EDW fills this performance gap and continues to provide a means of managing and reviewing information to improve the integrity of crucial veteran benefits programs.

1.1.d) Additional Project Information (Optional)

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

1.2) Contact Information:

1.2.a) Person completing this document:	
Title:	Anthony Paulson
Organization:	Data Information Services (PA&I)
Telephone Number:	202-461-9073
Email Address:	anthony.paulson@va.gov
1.2.b) Project Manager:	

Title:	Susan Perez
Organization:	Data Information Services (PA&I)
Telephone Number:	202-461-9061
Email Address:	susan.perez@va.gov
1.2.c) Staff Contact Person:	
Title:	Anthony Paulson
Organization:	Data Information Services (PA&I)
Telephone Number:	202-461-9073
Email Address:	anthony.paulson@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.)

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.

Personal information is maintained to assist VBA offices in the timely adjudication of benefit claims. In addition this information is collected to provide statistical analysis to VBA management as well as respond to legislative inquiries.

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) and Chapters 11, 13, 15, 21, 31, 34, 35, 36, and 37.
3.c) Identify, by selecting the appropriate range from the list below, the approximate number of individuals that (will) have their personal information stored in project systems.
More than 20,000,000
3.d) Identify what stage the project/system is in: (1) Design/Planning, (2) Development/Implementation, (3) Operation/Maintenance, (4) Disposal, or (5) Mixed Stages.
(3) 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.
The system is operational since 1999
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

4. SYSTEM OF RECORDS:
<i>The Privacy Act of 1974 (Section 552a of Title 5 of the United States Code) and VA policy provide privacy protections for employee or customer information that VA or its suppliers maintain in a System of Records (SOR). A SOR is a file or application from which personal information is retrieved by an identifier (e.g. name, unique number or symbol). Data maintained in a SOR must be managed in accordance with the requirements of the Privacy Act and the specific provisions of the applicable SOR Notice. Each SOR Notice is to be published in the Federal Register. See VA Handbook 6300.5 "Procedures for Establishing & Managing Privacy Act Systems Of Records", for additional information regarding Systems of Records.</i>
4.a) Will the project or application retrieve personal information on the basis of name, unique number, symbol, or other identifier assigned to the individual?
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; 55VA26: 38VA23; 45VA23
(2) The name of the System of Records, and
Compensation, Pension, Education and Rehabilitation Records – VA; Loan Guaranty Home, Condominium and Manufactured Home Loan Applicant Records & Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records-VA; Veterans and Beneficiaries Identification and Records Location Subsystem (BIRLS); Veterans Assistance Discharge Systems (VADS)
(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL).
http://vawww.vhaco.va.gov/privacy/systemsofrecords.htm
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.
This investment consists of a historical data snapshot from specific VA systems of records. This project does not create a unique set of data, rather it maintains a repository of existing information.
4.b.4) Does the System of Records Notice require modification?

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

Modification of the System of Records is NOT Required.

4.b.5) Describe the required modifications.

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

Explanation:

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

PIA SECTION 5

Project Name

Program Integrity/Data Management-2009

5. DATA COLLECTION:

5.1 Data Types and Data Uses

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

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

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

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

Yes

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

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

To provide accurate identification, payment of benefits, outreach, and benefits eligibility, data elements may include identifying information (e.g. name, address, social security number,) military service and active duty separation information (e.g. name, service number, date of birth, rank, sex, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, whether veteran was discharged with a disability, served in Vietnam conflict, etc, reenlisted, received a Purple Heart or other military decoration, payment information (e.g. veteran payee name, address, dollar amount of readjustment service pay, amount of disability or pension payments, number of nonpay days, any amount of indebtedness (accounts receivable) arising from Title 38 U.S.C. benefits and which are owed to VA,) medical information (e.g. medical and dental treatment in the Armed Forces including type of service-connected disability, medical facilities or by VA health care personnel or received from private hospitals and health care personnel relating to a claim for VA disability benefits or medical or dental treatment), personal information (e.g. marital status, name and address of dependents, occupation, amount of education of a veteran or a dependent, dependent's relationship to veteran,) education benefit information (e.g. information arising from utilization or training benefits such as a veteran trainee's induction, reentrance, or dismissal from a program or progress and attendance in an education or training program,) applications for compensation, pension, education and rehabilitation benefits and training which may contain identifying information, military service and active duty separation information, education benefit information relating to a veteran or beneficiary, claims file number, name and address of penal institution, date of commitment, type of offense, scheduled release date, veteran's date of birth, beneficiary relationship to veteran and whether veteran or beneficiary is in a work release or half way house program, on parole or has been released from incarceration. For a complete list, see Title 38, U.S.C., section 210© and chapters 11, 13, 15, 31, 34, 35 and 36 and the system of records data categories

under 58VA21/22/28, 38VA23 and 45 VA23.

Loan Guaranty data elements may include similar identifying information, military service and active duty separation information, personal information and applications for certificates of eligibility, applications for FHA veterans' low-down payment loans, applications for a guaranteed or direct loan, applications for a release of liability, applications for substitutions of VA entitlement and applications for specially adapted housing (social security number, marital status, identity of dependents, assets and liabilities at financial institutions, profitability data concerning business of self-employed individuals, payment history on a VA-guaranteed, direct, or vendee loan on an acquired property, medical information when specially adapted housing is sought, and information regarding whether a veteran owes a debt to the United States as indicated under 55VA26.

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

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

To provide accurate identification, payment of benefits, outreach, benefits eligibility data elements may include, personal information (e.g. marital status, name and address of dependents, occupation, amount of education of a veteran or a dependent, dependent's relationship to veteran,)

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

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

To determine specific types of benefit eligibility, data elements may include military service and active duty separation information (e.g. name, service number, date of birth, rank, sex, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, whether veteran was discharged with a disability, served in Vietnam conflict, etc, reenlisted, received a Purple Heart or other military decoration, payment information (e.g. veteran payee name, address, dollar amount of readjustment service pay, amount of disability or pension payments, number of nonpay days, any amount of indebtedness (accounts receivable) arising from Title 38 U.S.C. benefits and which are owed to VA)

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

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

To provide accurate identification, payment of benefits, outreach, and benefits eligibility, data elements may include medical information (e.g.name, medical and dental treatment in the Armed Forces including type of service-connected disability, medical facilities or by VA health care personnel or received from private hospitals and health care personnel relating to a claim for VA disability benefits or medical or dental treatment.)

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

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

To provide accurate identification, payment of benefits, outreach, and benefits eligibility, data elements may include medical information (e.g.name, medical and dental treatment in the Armed Forces including type of service-connected disability, medical facilities or by VA health care personnel or received from private hospitals and health care personnel relating to a claim for VA disability benefits or medical or dental treatment.)

No	Criminal Record Information
----	------------------------------------

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

No	Guardian Information
----	-----------------------------

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

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

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

Specifically identify the personal information collected, and describe the intended use of the information.
 To provide accurate identification, payment of benefits, outreach, and benefits eligibility, data elements may include identifying information (e.g. name, address, social security number,) military service and active duty separation information (e.g. name, service number, date of birth, rank, sex, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, whether veteran was discharged with a disability, served in Vietnam conflict, etc, reenlisted, received a Purple Heart or other military decoration, payment information (e.g. veteran payee name, address, dollar amount of readjustment service pay, amount of disability or pension payments, number of non pay days, any amount of indebtedness (accounts receivable) arising from Title 38 U.S.C. benefits and which are owed to VA, education benefit information (e.g. information arising from utilization or training benefits such as a veteran trainee's induction, reentrance, or dismissal from a program or progress and attendance in an education or training program, personal information (e.g. marital status, name and address of dependents, occupation, amount of education of a veteran or a dependent, dependent's relationship to veteran)

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

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

To provide accurate identification, payment of benefits, outreach, and benefits eligibility, data elements may include identifying information (e.g. name, address, social security number,) military service and active duty separation information (e.g. name, service number, date of birth, rank, sex, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, whether veteran was discharged with a disability, served in Vietnam conflict, etc, reenlisted, received a Purple Heart or other military decoration, payment information (e.g. veteran payee name, address, dollar amount of readjustment service pay, amount of disability or pension payments, number of non-pay days, any amount of indebtedness (accounts receivable) arising from Title 38 U.S.C. benefits and which are owed to VA,) medical information (e.g. medical and dental treatment in the Armed Forces including type of service-connected disability, medical facilities or by VA health care personnel or received from private hospitals and health care personnel relating to a claim for VA disability benefits or medical or dental treatment), personal information (e.g. marital status, name and address of dependents, occupation, amount of education of a veteran or a dependent, dependent's relationship to veteran,) education benefit information (e.g. information arising from utilization or training benefits such as a veteran trainee's induction, reentrance, or dismissal from a program or progress and attendance in an education or training program)

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.

VA employee Human resources information is maintained for use by VBA Human Resources Division, including Employee Name, Social security number, Address, Occupation, Education, Pay grade and Step, Base Pay, Locality Pay, Awards, TSP/FERS allotments, Tax information, Leave balances, Life insurance percentages, and Veteran status.

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.

No	Veteran Source
----	-----------------------

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

No	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.

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.

Beneficiary Information Records Locator System (BIRLS), Compensation & Pension Master Record (CPMR), Vocational Rehabilitation and Employment (VRE) files, Loan Guaranty (LGY) files; Employee Personnel data files make up the central data repository for VBA. There is no other source for this type of information for use by VBA management and senior leadership.

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.

Department of Defense (DOD) Defense Management Data Center (DMDC), DOD Deployment Health Support Directorate (DHSD)

No	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.

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

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

Yes	Other Source(s)
-----	-----------------

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

VA employee personal information is maintained for oversight use by VBA Human Resources Division, for human capital management.

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.")

No	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.

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

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

On a recurring scheduled basis, data from VBA systems of records is transferred electronically, in a secure manner, from various VBA maintained computer servers to the data warehouse server.

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

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

Data is collected from the Department of Defense and is transferred to the Data Warehouse using computer transfer media (compact disks)

No	Telephone Contact:	Information is collected via telephone.
----	---------------------------	---

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

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

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

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

5.4 Notice

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

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

No

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

5.4.b) Is the data collection mandatory or 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?

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

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

No	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.

No	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.

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

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

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

This is a secured transfer of data from one system to another. No Privacy Notice Provided.

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

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

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

This is a secured transfer of data from one system to another. No Privacy Notice Provided.

No	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.

No	Other Method:
----	----------------------

Explain:

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

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

5.5 Consent For Secondary Use of PII:

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

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

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

No

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

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

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

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

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

Describe:

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

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

Describe:

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

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

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

information from the primary information source to provide the following:

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

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

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

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

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

Describe:

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

	Other Media
--	--------------------

Describe:

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

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

5.6 Data Quality

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

Pre-established business agreements are in place which limit the size and content of the data.

5.6.b) How is data checked for completeness?

Data is checked for completeness manually and by system audits.

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

Data are updated routinely on predefined schedules.

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

The organization owning the data determines which elements to use and maintain in the data warehouse (DW). Once the data is stored in the DW, the owning organization can verify the authenticity and accuracy through various reports.

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

Project Name

Program Integrity/Data Management-2009

6. Use and Disclosure

6.1 User Access and Data Sharing

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

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

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

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

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

Yes	System Users
-----	---------------------

Yes	System Owner, Project Manager
-----	--------------------------------------

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

Yes	Contractor
-----	-------------------

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

Grant Thorton LLC is under contract with VBA to maintain the data warehouse. (PO number 101-G67186.) Data access is based on a need-to-know, and is contingent upon successful background investigation. VBA employees monitor and track the contractors' activities.

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

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

VA departmental organizations, such as the General Counsel; Public Affairs; Office of Policy; Office of the Secretary requests by Congress, General Accounting Office, IG, etc. Veterans Health Administration (VHA) Environmental Epidemiology Service-related to veteran health surveillance issues. Often, Congressional chartered or Va recognized Veteran Service Organizations (VSO) will request veteran-specific data relevant to thier organizations' assistance in developing benefits claim packages. VSO's receiving data include such groups as Veterans of Foreign Wars, Vietnam Veterans of America, the American Legion, Gulf War Resource Center, Etc.

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.

Congressional chartered or VA recognized Veteran Service Organizations (VSO) will request veteran-specific data relevant to their organizations' assistance in developing benefits claim packages. VSO's receiving data include such groups as Veterans of Foreign Wars, Vietnam Veterans of America, the American Legion, Gulf War Resource Center, Etc.

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

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

Defense Manpower Data Center (DMDC), Social Security Administration, IG and GAO

Yes	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.

State veterans departments occasionally request veteran-specific data related to benefits and services provided to veterans residing in their state.

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.

No	Other Project/ System
----	------------------------------

If information is shared with other projects or systems:

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

No	Other User(s)
----	----------------------

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

6.1.a.1) Describe here who has access to personal information maintained in project's IT systems:
VBA end users and employees within VBA's Data & Information Services Staff (D&IS) and contractors have varying levels of access to data maintained in VBA's DW/ODS. VBA end users typically request report data on behalf of non VA employees, including members of Congress, General Accounting Office (GAO), Inspector General's Office (IG) and other federal agencies or organizations with a valid need for the information.
6.1.b) How is access to the data determined?
Access is determined based on the user having a valid need (as determined by Data & Information Services Staff supervisors and the business owner) for the information, as well as belonging to a VA recognized organization.
6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents.
VBA has placed strict control measures to prevent the inadvertent or deliberate release of information to non-authorized personnel in several Federal Standards publications, VA policies, Directives, Security Configuration Guidelines and employee procedures.
6.1.d) Will users have access to all data on the project systems or will user access be restricted? Explain.
Access is restricted on a "need to know" basis, and based on the organization's role and function.
6.1.e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by those having access? (Please list processes and training materials that specifically relate to unauthorized browsing)
Internal monitoring and auditing, such as System log violations, which track employees attempting to access the records of sensitive level employees. Also, VBA employees and contractors are required to complete annual cyber security and privacy awareness training which covers unauthorized browsing.
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
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.)

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.
No	The application will use other method (explain below).
Yes	The application is exempt from needing to provide access.

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

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

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

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

VBA's data warehouse stores information from source systems. Entries and changes are made to the actual source systems. Changes made to source systems are reflected in the warehouse, through scheduled and periodic updates of data files. Individuals can not have access to the warehouse for viewing of personal information.

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

7 Retention and Disposal

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

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

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

System of Records Notices may be accessed via:

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

or

http://vaww.va.gov/foia/err/enhanced/privacy_act/privacy_act.html

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

VHA Handbook 1907.1 may be accessed at:

http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=434

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

[Start by looking at the http://www.warms.vba.va.gov/20rcs.html](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 from source systems is constantly updated on a scheduled basis. When new source system files are available, they are transferred to the warehouse. Old files are saved using backup tapes.

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

VA is in the process of developing procedures for eliminating data.

7.c) Where are procedures documented?

VBA's Records Control Schedule, VB-1 (<http://www.warms.vba.va.gov/admin23/rcs/part1/toc.doc>)

7.d) How are data retention procedures enforced?

Enforcement of data retention procedures will be performed through a service level agreement with the server maintenance team in the Austin, Texas data center.

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

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

8 SECURITY

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

8.1 General Security Measures

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

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

Security monitoring, testing and evaluation were conducted during the testing phase (prior to implementation) and continue to be monitored routinely during implementation, through the service level agreement with the Austin Automation Center (AAC) and resident database administrators at VBA.

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

Yes

8.2 Project-Specific Security Measures

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

- A concise description of how data will be protected against unauthorized access, unauthorized modification, and how the availability of the system will be protected.

- A concise description of the administrative controls (Security Plans, Rules of Behavior, Procedures for establishing user accounts, etc.).

• A concise description of the technical controls (Access Controls, Intrusion Detection, etc.) that will be in place to safeguard the information.

• Describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses. For example, are audit logs regularly reviewed to ensure appropriate use of information? Are strict disciplinary programs in place if an individual is found to be inappropriately using the information?

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

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

Security monitoring, testing and evaluation were conducted during the testing phase (prior to implementation) and continue to be monitored routinely during implementation, through the service level agreement with the Austin Automation Center (AAC) and resident database administrators at VBA.

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.

As a result of performing the PIA, continual emphasis and attention will be applied to addressing security and privacy concerns including assuring that collection of data and personal information contains appropriate consent and release

information and that all information stored in VBA databases are secured per VA security standards.

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

12. PUBLIC AVAILABILITY

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

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

1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment⁹. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).

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

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

No

12.b) If yes, specify:

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

13. ACCEPTANCE OF RESPONSIBILITY AND ACKNOWLEDGEMENT OF ACCOUNTABILITY:

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

Yes

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

Susan Perez 07-07-2007

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