Appendix R - Region 5 VBA INS Philadelphia ITC Web Applications PIA
Privacy Impact Assessment/Benefits Support Services (C&A 2008)

PIA SECTIONS 1 - 4

INTRODUCTION:

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

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

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

Primary Privacy Impact Assessment objectives include:

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

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

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

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

Additional important objectives include:

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

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

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

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

o Promote awareness and understanding of privacy issues.

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

Completion of this PIA Form:

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

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

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

CLICK ON THE LINK BELOW TO VIEW PIA PROJECT REVIEW SUMMARY:
https://vaww.camsit....%20Summary

Part I. Project Identification and Determination of PIA Requirement

1. PROJECT IDENTIFICATION:

1.1) Project Basic Information:

1.1.a) Project or Application Name:

Benefits Support Services

1.1.b) OMB Unique Project Identifier:

029-00-01-16-01-1268-00

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 Benefits Support Services investment sustains a full range of VBA applications and associated interfaces to include the following applications to be Certified and Accredited: BIRLS/VADS, Compensation and Pension (C&P) Corporate Applications (PIES, COVERS, VAI and VIS), C&P Web Applications (AMIS, STAR, VERIS, Web SMR), Common Security Services (CSS), CWINRS, Education Web Applications (LACAS, ECERT, RightNow Fax, WAVE), FBS, IBBA, Insurance General Ledger, Insurance LAN (VICTARS, SKIPPES), Insurance IPS, Insurance Web Applications (ISS), VONAPP, LS&C, VR&E Web Applications (ROQ), VIP (ACE,CPB, TAS, Web GIL, Web ELI, E-Appraisal, CPTS), TPSS, and WEAMS.

These applications are in place to meet legislative mandates, court decisions, world events and industry standard service to the veterans and beneficiaries. These applications and systems provide continuing and up-to date payment and services information vital to the veteran. Without continuing maintenance of these systems veterans would not receive timely delivery of mandated payment benefits. This initiative crosses all Benefits program areas including: Compensation, Pension, Education, Housing, Insurance and Vocational Rehabilitation. The initiative identifies all VBA program areas that determine, provide, and manage veterans' benefits for maintenance of existing applications (not include VETSNET and Virtual VA).

Benefits Support Services investment contributes to meeting the following VA strategic goals; Restore the capability of disabled veterans to the greatest extent possible and improve the quality of their lives and their families; Ensure a smooth transition for veterans from active military services to civilian life; and Honor and serve veterans in life and memorialize them in death for their sacrifices on behalf of the Nation.

In order to meet these crucial business requirements, VBA has created this investment to ensure that the systems in operations and maintained are meeting expected performance goals and are following the established maintenance plans. This investment will address operations and maintenance tasks like, resolving processing flaws, making mandatory changes to address privacy and security issues, and maintenance required by technical obsolescence or changes in business processes. This investment will enable VBA to consolidate O&M activities into a centrally managed environment which will allow for better accountability, enable enterprise priority setting and greater access to industry standards and best practices for these mission critical systems.

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:

	C&P Application Maintenance (LAN, Corporate, Web, IBBA, CSS, FBS)	
	1.2.a) Person completing this document:	Gregory H. Johnson
	Title:	Director, IT Security Service, OI&T Field Operations Region Five
	Organization:	OI&T Field Operations, Region Five

Telephone Number:	(202) 461-9174
Email Address:	fred.tolley@va.gov
1.2.b) Project Manager:	Fred Tolley
Title:	Business Program Management Office (BPMO)
Organization:	Office of Enterprise Development (OED)
Telephone Number:	202-461-9143
Email Address:	bernie.pessagno@va.gov
1.2.c) Staff Contact Person:	Brian Stephens
Title:	Chief, C&P Business Process Development
Organization:	C&P Service
Telephone Number:	727-319-5807
Email Address:	Brian.stephens1@va.gov
LGY Application Maintenance	(LS&C, VIP)
1.2.a) Person completing this document:	Gregory H. Johnson
Title:	Director, IT Security Service, OI&T Field Operations Region Five
Organization:	OI&T Field Operations, Region Five
Telephone Number:	(202) 461-9174
Email Address:	gregory.johnson@va.gov
1.2.b) Project Manager:	George Riddick
Title:	Technical Project Manager
Organization:	Business Program Management Office (BPMO)
Telephone Number:	(202) 461-9146
Email Address:	george.riddick@va.gov

1.2.c) Staff Contact Person:	Frank Purgason
Title:	Chief, IT and Program Analysis
Organization:	Loan Guaranty Service
Telephone Number:	(202) 461-9556
Email Address:	frank.purgason@va.gov

VR&E Application Maintenance (CWINRS, Web Applications)	
1.2.a) Person completing this document:	Gregory H. Johnson
Title:	Director, IT Security Service, OI&T Field Operations Region Five
Organization:	OI&T Field Operations, Region Five
Telephone Number:	(202) 461-9174
Email Address:	gregory.johnson@va.gov
1.2.b) Project Manager:	Jon Abbey
Title:	Technical Project Manager
Organization:	Business Program Management Office (BPMO)
Telephone Number:	(202) 461-9149
Email Address:	jon.abbey@va.gov
1.2.c) Staff Contact Person:	Fred Rash
Title:	Management Analyst
Organization:	Education Service
Telephone Number:	202-461-9631
Email Address:	Frederick.rash@va.gov

BIRLS/VADS Application Maintenance	
1.2.a) Person completing this document:	Gregory H. Johnson
Title:	Director, IT Security Service, OI&T Field Operations Region Five
Organization:	OI&T Field Operations, Region Five
Telephone Number:	(202) 461-9174
Email Address:	gregory.johnson@va.gov
1.2.b) Project Manager:	John Quigley
Title:	Technical Project Manager
Organization:	Business Program Management Office (BPMO)
Telephone Number:	(202) 461-9152
Email Address:	john.quigley@va.gov
1.2.c) Staff Contact Person:	Carla Andresen
Title:	Chief, Technical Rules Development Staff
Organization:	C&P Service
Telephone Number:	202-461-9692
Email Address:	carla.andresen@va.gov

Education Application Maintenance (WEAMS, LAN/TIMS, WEB, TPSS)	
1.2.a) Person completing this document:	Gregory H. Johnson
Title:	Director, IT Security Service, OI&T Field Operations Region Five
Organization:	OI&T Field Operations, Region Five
Telephone Number:	(202) 461-9174
Email Address:	gregory.johnson@va.gov

1.2.b) Project Manager:	Rebecca Wells
Title:	Technical Project Manager
Organization:	Business Program Management Office (BPMO)
Telephone Number:	(202) 461-9135
Email Address:	jon.abbey@va.gov
1.2.c) Staff Contact Person:	Rhonda Jones
Title:	Management Analyst
Organization:	Education Service
Telephone Number:	202-461-9631
Email Address:	Frederick.rash@va.gov

Insurance Application Maintenance (General Ledger, Victars, Skippes, IPS, ISS)	
1.2.a) Person completing this document:	Gregory H. Johnson
Title:	Director, IT Security Service, OI&T Field Operations Region Five
Organization:	OI&T Field Operations, Region Five
Telephone Number:	(202) 461-9174
Email Address:	gregory.johnson@va.gov
1.2.b) Project Manager:	Thomas I. Buffington
Title:	Chief, Policy, Procedures and IT Staff
Organization:	Insurance Service
Telephone Number:	(215) 381-3034
Email Address:	thomas.buffington@va.gov
1.2.c) Staff Contact Person:	Thomas Lastowka
Title:	Director, Insurance Service

Organization:	Insurance Service
Telephone Number:	(215) 381-3100
Email Address:	thomas.lastowka@va.gov

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

-		**SECTION INCOMPLETE**
	Yes	**SECTION COMPLETED**
	GHJ	I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Dec 03, 2007	**Section Update Date**

Section 1 Review:

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

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

2. DETERMINATION OF PIA REQUIREMENTS:

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

2.a) Will the project collect and/or maintain personally identifiable information 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

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

Yes

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

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.)

-		**SECTION INCOMPLETE**
	Yes	**SECTION COMPLETED**
	GHJ	I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.

	Dec 03, 2007	**Section Update Date**

Section 2 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

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 applications supported by this OMB 300 collect personal information that is necessary to determine various veterans benefits and entitlements, for example: The Education Service component uses this information to provide financial assistance for education, training, certification, etc. generally in the form of monthly benefit payments, to veterans, active duty service persons, reservists, and certain eligible dependents of disabled or deceased veterans in recognition of their military service to this nation. Beneficiary Identification and Records Locator Subsystem (BIRLS) and Veterans Assistance Discharge System (VADS) databases maintain veteran's personal information necessary for determining eligibility for benefits and processing of associated claims. The Insurance program uses this information to provide life insurance

benefits to veterans and service members that are not available from the commercial insurance industry due to lost or impaired insurability resulting from military service. Information is collected to determine who are entitled to the provided benefits. The information collected in the loan applications supported by this investment is used to determine entitlements, issue loan guarantees, and assist veterans in retaining their homes. The Compensation program uses this information 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 Pension program uses this information 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. Information is also collected to provide for services and assistance necessary to enable veterans with service-connected disabilities to achieve maximum independence in daily living and, to the maximum extent feasible, to become employable and to obtain and maintain suitable employment.

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

38 USC 3700 et seq and 38 USC 2100 et seq; 38, USC, section 210(c) and Chapters 11, 13, 15, 31, 34, 35, and 36; 38, USC, Chapter 3, Section 21(c)(1); 38 USC 1901 et seq. 38 USC. 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.

10,000,000 - 19,999,999

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.

(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.

LGY applications operational 06/1964.
LGY Web applications went into production 01/2000.
BIRLS/VADS has been operational 01/1969.
VADS has been operational 01/1998.
EDU systems have been operational 01/2001
The C&P systems (non-BDN) are operational at various dates fro 1997 - 2004
Common Security Service (CSS) was operational 8/1997
Insurance systems have been operational various dates between 1959 - 2000.
VR&E system has been operation for 5 years.

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

-		**SECTION INCOMPLETE**
	Yes	**SECTION COMPLETED**
	GHJ	I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and hit submit and then select "Yes" and hit submit.
	Dec 03, 2007	**Section Update Date**

Section 3 Review:

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

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

4. SYSTEM OF RECORDS:

The Privacy Act of 1974 (Section 552a of Title 5 of the United States Code) and VA policy provide privacy protections for employee or customer information that VA or its suppliers maintain in a System of Records (SOR). A SOR is a file or application from which personal information is retrieved by an identifier (e.g. name, unique number or symbol). Data maintained in a SOR must be managed in accordance with the requirements of the Privacy Act and the specific

provisions of the applicable SOR Notice. Each SOR Notice is to be published in the Federal Register. See VA Handbook 6300.5 "Procedures for Establishing & Managing Privacy Act Systems Of Records", for additional information regarding Systems of Records.

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

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

Yes

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

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

Yes

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

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

55VA26, 58VA21/22/28, 38VA21, 36VA00, 46VA00, 53VA00

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

Loan Guaranty Home, Condominium and Manufactured Home Loan Applicant Records, Specially Adapted Housing Applicant Records, and Vendee Loan Applicant Records--VA, Compensation, Pension, Education and Rehabilitation Records-VA, Veterans and Beneficiaries Identification Records Location Subsystem—VA. 36VA00 Veterans and Armed Forces Personnel United States Government Life Insurance Records-VA. 46VA00 Veterans, Beneficiaries and Attorneys United States Government Insurance Award Records- VA. 53VA00 Veterans Mortgage Life Insurance-VA, Veterans and Beneficiaries Identification and Records Location (BIRLS) and Compensation, Pension, Education, and Rehabilitation (covers BDN and Corporate databases)

(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/Privacy/SystemsOfRecords/VApart2.asp#55VA26

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 specifically for this project.

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

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

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

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.

Not Applicable

Explanation:

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

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update date**

PROCEED TO SECTION 5 OF THE PRIVACY IMPACT ASSESSMENT FORM BY CLICKING THE LINK BELOW
https://vaww.camsit....ection%205

Section 4 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

PIA SECTION 5

Project Name

Benefits Support Services

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.

Depending on the benefits being requested or provided different personal data will be requested, For example: Veteran Personal data (Name, Address, Social Security Number, Family/Dependents, Marital Status, Medical Status, Birth Information, Death Information) and Veteran Dependent Data (personal information including name and address, age, school status, relationship to the veteran, medical status) is used to (1) communicate with the Veteran about his/her benefits, to notify of change in account status and advise about new options and (2) to determine eligibility and process entitlements and advise about new options. Insured's name, address, bank data (optional), telephone number (optional), insurance file number. This is to contact the veteran policyholder on a scheduled basis in order to pay annual dividends, advise of new or changed benefits, advise of changes to policy status, or request repayment of loan or lien. Name, SSN, Address, Service information, financial information - Determination of entitlement, credit underwriting review, assisting veterans to retain their homes and to perform outreach.

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

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

Information such as Account History (case/account number, identity of beneficiary, eligibility determination information, benefit information), Education Program Approval Information (approved courses, effective dates, types of training, facility code, objective code, training type), and Rehabilitation Program Approval Information (institution certifications, licenses, approval information) Vocational & education goals and any other information that impacts their achievement.

Yes	**Dependent Information**

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

Loan Guaranty uses personal information to determine if appropriate credit and income standards were used in underwriting the loan. Education-Veteran Dependent Data (personal information including name and address, age, school status, relationship to the veteran, medical status) is used to (1) communicate with the Veteran about his/her benefits, to notify of change in account status and advise about new options and (2) to determine eligibility and process entitlement. BIRLS/VADS – uses this information to identify and contact veterans' family members or beneficiaries with respect to benefits.

Yes	**Service Information**

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

Department of Defense provides (1) Service Data: reserve and guard participation, retired pay or severance pay, hazardous agent exposure, branch of service, active duty date, released date, type of discharge, separation reason; and (2) Medical Records: Military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations. This information is used to determine eligibility and process entitlement. BIRLS/VADS- uses this information to determine veterans eligibility for VA benefits; uses information such as name, SSN, address, date of birth, service record number, dates of service and any disability ratings.

Yes	**Medical Information**

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

Diagnostic codes, percent of disability - Determine eligibility for specially adapted housing, determine appropriate modifications under specially adapted housing program

Note: Service connected disability is used to determine if veteran is exempt from funding fees – other than existence of disability determination, no other medical information is used for this purpose.

Yes	**Criminal Record Information**

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

Incarceration at a state or local facility, fugitive felon status, investigative reports for some accident. These records are used to suspend benefits during imprisonment at local and Federal facilities

Yes	**Guardian Information**

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

Guardian name, address, telephone number is used to communicate with guardians regarding the veteran or his/her dependent and court proceedings, field examinations, appointments and annual accountings. Guardianship Information may also include court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accountings. It may also include Veteran Dependent Data: Personal information including name and address, age, school status, relationship to the veteran, medical status.

Yes	**Education Information**

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

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

Yes	**Rehabilitation Information**

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

Diagnostic codes, percent of disability - Determine eligibility for specially adapted housing, determine appropriate modifications under specially adapted housing program.

No	**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.

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

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update Date**

Section 5.1 Review:

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

**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

5.2 Data Sources

Identify the source(s) of the collected information.

a) Select all applicable data source categories provided below.

b) For each category selected:

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

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

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

Yes	**Veteran Source**

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

Veteran Personal data (Name, Address, Social Security Number, Family/Dependents, Marital Status, Medical Status, Birth Information, Death Information) and Veteran Dependent Data (personal information including name and address, age, school status, relationship to the veteran, medical status) is used to (1) communicate

with the Veteran about his/her benefits, to notify of change in account status and advise about new options and (2) to determine eligibility and process entitlement

Yes	**Public Source(s)**

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

Commercial Credit reports are obtained for the purpose of credit underwriting – Equifax Transunion & TRW are the normal providers. Educational institutions (schools) and other training facilities provide information on veterans enrollment and attendance. Information is used to process education benefits.

Yes	**VA Files and Databases**

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

Information such as Account History (case/account number, identity of beneficiary, eligibility determination information, benefit information), Education Program Approval Information (approved courses, effective dates, types of training, facility code, objective code, training type), and Rehabilitation Program Approval Information (institution certifications, licenses, approval information) is used to determine eligibility and process entitlement. The following list of sources provide, receive, or share data/information with BIRLS: BDN - Benefits Delivery Network connects to BIRLS; BDN is employed by VBA to process entitlements for Compensation and Pension, Education, and Vocational Rehabilitation and Employment. CARS – Centralized Accounts Receivable System requires an interface with BIRLS to update the bankruptcy indicator. C&P - Compensation and Pension requires BIRLS for creation of the pending issue file which is used for the C&P master record. Corporate Database - BIRLS interfaces with VBA's corporate database to provide service information and identifying information. COVERS Control of Veterans Records System - BIRLS tracks folders between Regional Offices or places of folder retirement. It has an interface with the (COVERS), which tracks folders within a Regional Office. Data Warehouse - BIRLS interfaces with VBA's data warehouse to provide service information, identifying information, and other data that may be used at a meta-data level. INS - BIRLS also interfaces with the Insurance system in Philadelphia, enabling VA personnel at regional offices to identify Insurance information. Mobilization requires an online interface with BIRLS. MVR Master Veterans Record - BIRLS provides an online interface to the Austin Automation Center's (AAC) Master Veteran Record (MVR) application, allowing all of the users of MVR to access the identification and service information located in the

BIRLS database. OIG – Office of Inspector General uses BIRLS as one of their primary sources for investigating fraud. PAID - Personnel and Accounting Integrated Data and Fee Basis interface with BIRLS to identify veterans that are VA employees for security purposes. PIES - Personnel Information Exchange System requires an online interface with BIRLS. RBA2000 – Rating Board Automation requires an online interface with BIRLS. SHARE – SHARE is a client-server application that performs inquires/updates against BIRLS. SMRTS - Service Medical Records Tracking System processing generates automatic updates to BIRLS. When a service medical record (SMR) folder is established in BIRLS, BIRLS determines if a claims folder already exists. If a claims folder exists, BIRLS will set the SMR folder in transit and RMC will send the record to the location of the claims folder. VADS - Veterans Assistance Discharge System and BIRLS interface allows service information for veterans to be added to BIRLS as soon as they are discharged from the service. VBA Training Academy - BIRLS provides a training database to enable the training of new adjudicators. VBA Common Security and BIRLS provide critical sensitive information to help maintain the security of VBA applications and records. VETSNET - Veterans Service Network requires an online interface with BIRLS. VHA - Veterans Health Administration obtains information from BIRLS to determine eligibility for treatment at VA hospitals. VHA uses HINQ (Hospital INQuiry) transactions to access pertinent information from BIRLS. WINRS - WACO Indianapolis Newark Roanoke Seattle case management system requires an online interface with BIRLS. The following list of sources provide, receive, or share data/information with VADS: BIRLS – Veterans Assistance Discharge System and BIRLS interface allows service information for veterans to be added to BIRLS as soon as they are discharged from the service. Education (Chapter 30) provides list of veterans to be contacted regarding educational benefits. VACO - VA Central Office receives list of veterans added into VADS. Other VA data source is the Benefits Delivery Network (BDN), to determine eligibility, and to allow for paying insurance premiums by deductions from benefits. We also receive through this channel a copy of a Notice of Death (NOD) entered at VA facilities. Insurance Center personnel may request paper records from the VA Regional Office having jurisdiction of a veteran's compensation folder, or may request previously retired folders, in order to determine eligibility for new insurance and/or waiver of premiums.

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.

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. To locate, contact, and pay veterans and beneficiaries. Other Federal Agency Sources are: Social Security Administration (SSA), Defense Finance and Accounting Service (DFAS), Defense Manpower Data Center (DMDC), U.S. Coast Guard, and Department of Treasury. National Service Life Insurance, Veterans Mortgage Life Insurance, Veterans Government Life Insurance, and Social Security Administration (verifies if Veteran is deceased), Department of Defense provides (1) Service Data: reserve and guard participation, retired pay or severance pay, hazardous agent exposure, branch of service, active duty date, released date, type of discharge, separation reason; and (2) Medical Records: Military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations. Federal Bureau of Prisons provides records of: Incarceration at federal state or local facilities, fugitive felon status, investigative reports for some accidents. Benefits are suspended for incarcerated felons. Other Federal agencies that provide

information that is used to determine eligibility and to process entitlements are the Department of Labor, Department of Treasury, Federal Parent Locator Service, General Accounting Office, Office of Inspector General, Office of Personnel Management, and Bureau of Census, Federal Housing Administration, Internal Revenue Service, Department of Housing and Urban Development.
The following list of sources provide, receive, or share data/information with BIRLS:
DMDC – Defense Manpower Data Center sends new enlistee information to BIRLS thereby ensuring that VBA has a record for military personnel as soon as they enlist into the service. It also interfaces with DMDC to record and display retired military pay for all retired veterans.
DOD (Quantico) – Department of Defense Marine Corps in Quantico, VA requests service medical records information through BIRLS.
DOE – Department of Education exchanges information with BIRLS regarding veteran enrollment in various schools throughout the nation and allows educational institutions to verify that a student is a veteran for whom educational benefits may be paid.
Department of Treasury is notified by check intercept processing regarding checks that need to be stopped.
Federal Archives receives all retired folders from BIRLS.
National Academy of Sciences Institute of Medicine requests batch extracts from BIRLS.
Medical Follow-up Agency request information from BIRLS.
Office of Child Support requests batch extracts from BIRLS.
Office of Policy and Planning requests information from BIRLS.
Selective Service requests batch extracts from BIRLS.
Loan Guaranty applications indirectly use data obtained from DoD. E.g. Defense Manpower Data Center (DMDC) feeds Veterans Information System (VIS) which is queried by ACE for entitlement determination purposes (read only).

Yes	**State Agency Source(s)**

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

Data input provided from State National Guard and Reserve Units is to determine eligibility for veterans benefits. State Bureau of Prisons provide Police Records: Incarceration at state or local facility, fugitive felon status, investigative reports for some accident. Benefits are suspended for veterans incarcerated for a felony.

No	**Local Agency Source(s)**

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

Yes	**Other Source(s)**

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

American Red Cross and Blind American Veterans provides information that is used to determine eligibility and to process entitlements. Blind American Veterans also exchange information in their capacity as fiduciaries for the veteran or the veteran's dependents. Guardianship Information may include court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accountings. It may also include Veteran Dependent Data: Personal information including name and address, age, school status, relationship to the veteran, medical status. Other sources used are InfoUSA and Westlaw. These are available subscription services that provide locator (address) information from local telephone and similar records. The VA Insurance Service also supervises the Office of Servicemembers' Group Life Insurance (OSGLI) at Prudential, and has access to information they have collected through a hold harmless agreement in our contract. Access is restricted to that information required to perform the user's duties – CAIVRS (Credit Alert Interactive Voice Response System).

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

-		**SECTION INCOMPLETE**
	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update Date**

Section 5.2 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

5.3 Collection Methods

Identify and describe how personal information is collected:

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

Yes	**Web Forms:**	Information collected on Web Forms and sent electronically over the Internet to project systems.

Identify the URL(s) of each Web site(s) from which information will be submitted, and the URL(s) of the associated privacy statement. (Note: This question

only applies to Web forms that are submitted online. Forms that are accessed online, printed and then mailed or faxed are considered "Paper Forms.")

The VBA website is http://www.vba.va.gov; with the specific online form located at http://vabenefits.vba.va.gov/vonapp/main.asp. The available forms located at this site are: V A Form 28-1900, Application for Vocational Rehabilitation Benefits. Applicants are required to complete form 21-4142, Authorization and Consent to Release Information to the Department of Veterans Affairs (V A). All VBA benefit forms are located at http://www.va.gov/vaforms/ For VA insurance, the website is at www.insurance.va.gov/ This site from which forms are accessed references the VA Privacy and Security site http://www.va.gov/p-rivacy/ , as well as the VA Disclaimer site (http://www.va.gov/disclaim.htm) and the VA FOIA site (http://vaww.va.gov/OIT/CIO/FOIA/default.asp).

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.

VA Form 28-1900, Application for Vocational Rehabilitation Benefits; Form 21-4142, Authorization and Consent to Release Information to the Department of Veterans Affairs (VA).VA Form 26-1880, 16-1883, VA Form 22-1990, Application for Education Benefits; All VBA benefit forms can be downloaded from http://www.vba.va.gov/pubs/forms1.htm. The VBA toll free number for benefits is 1-800-827-1000. The VBA website is http://www.vba.va.gov. For VA insurance the paper forms are the following:
29-0165, VA Matic Change
29-0309, Direct Deposit Enrollment
29-0352-1, Application for VA Matic Authorization
29-1546, Application for Cash Surrender Value/Application for Policy Loan
29-1549, Application for Change of Permanent Plan
29-336, Designation of Beneficiary
29-352, Application for Reinstatement
29-357, Claim for Disability Insurance Benefits
29-4364, Application for Service-Disabled Veterans Insurance
29-8636, Application for Veterans Mortgage Life Insurance
29-888, Insurance Deduction Authorization
Insurance Center personnel may request paper records from the VA Regional Office having jurisdiction of a veteran's compensation folder, or may request previously retired folders, in order to determine eligibility for new insurance and/or waiver of premiums.
21-0510 Eligibility Verification Reports
21-0511S 21-0511S-1 21-0511V 21-0511V-1 21-0512S 21-0512S-1 21-0512V 21-0512V-1 21-0513 21-0538 Status of Dependents Questionnaire,
21-2545 Report of Medical Examination for Disability Evaluation
21-4138 Statement in Support of Claim.
21-4169 Supplement to VA Forms
21-526, 21-534, and 21-535 (For Philippine Claims)
21-4171 Supporting Statement Regarding Marriage,
21-8951-2 Notice of Waiver of VA Compensation or Pension to Receive Military Pay and Allowances
21-0571 Application for Exclusion of Children's Income,
21-8924 Application of Surviving Spouse or Child for REPS Benefits (Restored Entitlement Program for Survivors),
21-8941REPS Annual Eligibility Report,
21-674 21-674B 21-674C Request for Approval of School Attendance
VA Form 21-674 VA Form 21-674b, and VA Form 21-674c. School Attendance Report
21-8416B Report of Medical, Legal, and Other Expenses Incident to Recovery for Injury or Death,
21-534 Application 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),
21-4709 Certificate As To Assets,

21-4185 Report of Income from Property or Business,
21-8938 Student Beneficiary Report -- REPS
21-8960, 21-8960-1 Certification of School Attendance or Termination,
21-4176 Report of Accidental Injury In Support of Claim for Compensation or Pension/Statement of Witness to Accident.
21-22, 21-22A Appointment of Veterans Service Organization As Claimant's Representative
(21-22), Appointment of Individual as Claimant's Representative (
21-22A). 21-2008 Application for United States Flag for Burial Purposes
21-530A State Application for Interment Allowance Under 38 U.S.C, 21-4703Fiduciary Agreement,
21-4706, 21-4706B, 21-4706C, 21-4718, 21-4718A Court Appointed Fiduciary's 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,
21-526 Veteran's Application for Compensation and/or Pension
21-0307 Spina Bifida Award Attachment Important Information,
21-0161A Income Verification,
21-0304 Application for Spina Bifida Benefits
21-0537 Marital Status Questionnaire, 21-535Application for Dependency and Indemnity Compensation by Parent(s) (Including Accrued Benefits and Death Compensation When Applicable),
21-527 Income -Net Worth and Employment Statement,
21-4192 Request for Employment Information in Connection with Claim for Disability Benefits,
21-686C Declaration of Status of Dependents,
21-0779 Request for Nursing Home Information in Connection with Claim for Aid and Attendance,
21-530 Application for Burial Benefits.
21-8049 Request for Details of Expenses,
20-0344 Annual Certification of Veteran Status and Veteran-Relatives,
21-4165 Pension 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)), 21-509 Statement of Dependency of Parent(s),
21-1775 Statement of Disappearance

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.)

Some data is not collected directly from individuals but is electronically transfered from another government entity: such as; the allotments from retired pay (DFAS, U.S. Coast Guard) and deductions from benefits (Hines VAITC), the data is collected specifically to start, stop or change payments for VA Insurance. Data interchange with Social Security Administration (SSA) – to request and receive addresses, date of death. The Insurance Center receives this data via VA's Hines data center. Data interchange with Department of Defense (DFAS) – to process allotments from military retired pay to pay premiums. Data interchange with VAITC, Hines, Illinois – to process deductions from benefits (DFB) to pay premiums; to receive address changes for veterans who elect this method to pay; to receive Notice of Death (NOD). Data interchange with Department of Treasury – to process disbursements and returned items. This data is received in Philadelphia over a dedicated line from Treasury that employs their approved encryption. Data interchange with the Federal Reserve Bank – to process pre-suthorized debits through automated clearinghouse procedures. This is currently done by "Fedline", to be replaced by 2007 with "Fedadvantage", both of which employ their approved encryption.
Data interchange with Defense Manpower Data Center - to identify military personnel who have been medically retired with a service disability of 50% (DoD disability) or higher so they can be contacted. This data is received in Philadelphia via OSGLI (Prudential).

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.

Educational institutions submit electronic information (via the VA-ONCE program) to the VA on veterans enrollment, attendance, credits, term, and courses using Form 22-1999 and Form 22-1999b. The veterans can also submit electronic information (via the WAVE program) certifying their school attendance. This information is used to process educational benefits. Information may be transferred electronically by using Secure+ Connect:Direct File Transfer Protocol (FTP) and Network Data Mover (NMD) from BIRLS to VBA Corporate System, VBA Data Warehouse/Operational Data Store and inquires from the Benefits Delivery Network and/or VA Insurance System.

Yes	**Telephone Contact:**	Information is collected via telephone.

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

The VBA toll free number for 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 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 to the veteran and/or claimant. Since 1988, insured veterans, beneficiaries, and other interested parties have been able to communicate and do business via toll free telephone service. The Insurance toll-free number (1-800-669-8477) is advertised on outgoing correspondence as well as the Insurance website and other venues. Callers enter a selection tree designed with the assistance of focus groups so to not be too long or confusing. Calls from policyholders about maintenance to their policies (e.g.address changes, loan requests) are referred to the Veterans Information Phone Section. Another unit, the Claims Queue, is responsible for the calls regarding Deaths, Beneficiary Designations, and applications for new Insurance. The Insurance call center answers 3,000 calls per workday on 80 lines. Mondays and Tuesdays are busiest days, especially after a holiday weekend. The beginning of the month is busier than the end of the month. We utilize real-time monitoring of call activity with our ACD's management information system and make immediate staffing adjustments when needed. Recognizing the special nature of our callers, our specialists learn techniques to assist angry, grieving, and elderly callers. Quality is assessed by call monitoring, with specialists judged on a 5-point scale, the highest rating indicating "over and above" courteous, accurate and thorough service was provided. We review 10 calls per month on each specialist. The monitoring is done "live" but silent. We survey callers (80/month) to make sure we are meeting their needs and implement countermeasures for problems uncovered. We utilize a “signature service” approach, meaning that the Insurance Specialist answering the call will, in most cases, be responsible for completing any work items required as the result of a call. About 85% of our calls are answered in their entirety at the time they are received, without hand-offs or further follow-up action. Call center employees receive 6-7 months of classroom training in various Insurance topics. Therefore, VBA Insurance call center staff is trained to provide quality service, not only in telephone communications but in all aspects of technical work. They are also trained to recognize when a call must be referred to another agency

(e.g., pension, request for service records), and how best to direct the customer.

Yes	**Other Collection Method:**	Information is collected through a method other that those listed above.

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

Veterans and program participants occasionally complete hard copy forms, and fax copies to VA. These do not meet the definition of web media since they are not completed on line. InfoUSA and Westlaw systems are used for on-line research by Insurance Center employees actively looking for individuals with whom we have a contract or to whom we owe money.

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

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update Date**

Section 5.3 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

5.4 Notice

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

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

Yes

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

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

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 VBA forms 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." Privacy policy is provided on the website

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

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

Ongoing

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

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

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

A privacy policy notice linkage is found on all VBA sites that request personal information, however, a privacy notice is not found on all the follow-on screens where further personal information is being collected. This requirement post-dates many of these screens. A project to add a link to the VBA privacy statement to all appropriate screens has been initiated. Also, VA Form 29-4364 is a two-page form. Privacy notice is provided on the second page.

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

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

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

Yes	**Web Forms:**

Explain:

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

Applicants for benefits are informed in writing: 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. Provided by electronic notice. Insurance forms, and the Insurance website, include this statement (here taken from VA Form 29-4364): “Important Notice About Information Collection. We need this information to determine, establish, or verify your eligibility for VA Insurance benefits (38 U.S.C. 722). Title 38, United States Code, allows us to ask for this information. We estimate that you will need an average of 40 minutes to review the instructions, find the information, and complete this form. VA cannot collect or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed. Valid OMB control numbers can be located on the OMB Internet page at www.whitehouse.gov/library/omb/OMBINVC.html#VA. If desired, you can call 1-800-827-1000 to get information on where to send comments or suggestions about this form.” “Privacy Act Notice. The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 5, Code of Federal Regulations 1.526 for routine uses identified in the VA system of records, 36VA00, Veterans and Armed Forces Personnel U.S. Government Life Insurance Records- VA, published in the Federal Register. Your obligation to respond is voluntary, but your failure to provide us the information could impede processing. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a Federal Statute of law in effect prior to January 1, 1975, and still in effect. The responses you submit are considered confidential (38 U.S.C. 5701).”

Yes	**Paper Forms:**

Explain:

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

There is a 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.

On Insurance forms and the Insurance website, include this statement (here taken from VA Form 29-4364): “Important Notice About Information Collection. We need this information to determine, establish, or verify your eligibility for VA Insurance benefits (38 U.S.C. 722). Title 38, United States Code, allows us to ask for this information. We estimate that you will need an average of 40 minutes to review the instructions, find the information, and complete this form. VA cannot collect or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed. Valid OMB control numbers can be located on the OMB Internet page at www.whitehouse.gov/library/omb/OMBINVC.html#VA. If desired, you can call 1-800-827-1000 to get information on where to send comments or suggestions about this form.” “Privacy Act Notice. The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 5, Code of Federal Regulations 1.526 for routine uses identified in the VA system of records, 36VA00, Veterans and Armed Forces Personnel U.S. Government Life Insurance Records- VA, published in the Federal Register. Your obligation to respond is voluntary, but your failure to provide us the information could impede processing. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a Federal Statute of law in effect pprior to January 1, 1975, and still in effect. The responses you submit are considered confidential (38 U.S.C. 5701).”

Applicants for educational benefits will be told in writing. Privacy Act Notice: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 5, Code of Federal Regulations 1.526 for routine uses (i.e., allowing VA to send educational forms or letters with a veteran’s identifying information to the veteran’s school or training establishment to (1) assist the veteran in the completion of claims forms or (2) for VA to obtain further information as may be necessary from the school for VA to properly process the veteran’s education claim or to monitor his or her progress during training) as identified in the VA system of records, 58VA21/22, Compensation, Pension, Education and Rehabilitation Records - VA, and published in the Federal Register. Your obligation to respond is required to obtain or retain education benefits. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a Federal Statute of law in effect prior to January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine the maximum benefits under the law. Payment of education benefits cannot be made unless the information is furnished as required by existing law (38 U.S.C. 3471). The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies. Forms state: “Important Notice About Information Collection: We need this information to determine your eligibility to education benefits (38 U.S.C. 3471). Title 38, United States Code, allows us to ask for this information. We estimate that you will need an average of 54 minutes to review the instructions, find the information, and complete this form. VA cannot conduct or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed. Valid OMB control numbers can be located on the OMB Internet Page at www.whitehouse.gov/library/omb/OMBINVC.html#VA . If desired, you can call 1-888-GI-BILL1 (1-888-442-4551) to get information on where to send comments or suggestions about this form”

Yes	**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?

Interchange with Department of Treasury and the Federal Reserve Bank are governed by their regulations. A MOA exists with SSA and DoD. Notice is not provided - Data was already collected by another government entity responsible for a privacy notice.

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?

Usually a notice is not provided as the data transfered from another federal agency which has provided the privacy notice to information sources. For VA loans transfers are with program participants only. Veterans are advised of their privacy rights at the time of their application for a loan, and at loan closing that personal data will be provided to VA.

Yes	**Telephone:**

Explain:

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

Provided by verbal notice. Guidance concerning notice and acceptable methods of authentication are included in the “VIPS Procedures

and Guidelines" training materials for the phone specialists.

Yes	**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.

Veterans sometimes fax completed forms. Privacy notice is printed on the forms.

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

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update Date**

Section 5.4 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.

-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

5.5 Consent For Secondary Use of PII:

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

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

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

Yes

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

Outreach by VA/VBA lines of business.

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.

Yes	**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.

Consent will be signaled by the user continuing to log in after the notice is displayed.

Yes	**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.

Consent is signaled by completion and submission of the form(s)

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 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.

Consent is signaled by completion and submission of the data / form(s)

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 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.

Consent is obtained via signed release obtained by the lender at time of application and/or loan closing

Yes	**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.

Consent is obtained verbally if necessary

Yes	**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.

Consent is signaled by the person submitting completed forms via fax

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

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update Date**

Section 5.5 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

5.6 Data Quality

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

Information is collected primarily on defined forms and entered to specific fields of database records. We ask for minimal identifying information. Because of GPRA we review forms on a schedule and remove any request for data we no longer need to collect. Electronic data transfers are subject to design criteria, industry format standards and automated checks to ensure that only appropriate data is contained in the transfer.

5.6.b) How is data checked for completeness?

Original submission of data is verified for completeness by the Regional Office Veterans Claims Examiners. There are also internal program controls, edits, and checks to ensure that the data submitted is complete. Automated edits and audits determine that a) a data element is present, and b) that the value is consistent with the data requested, and c) consistent with the record being created/updated. Veterans who participate in VBA education programs must certify their enrollment monthly. The School certifying official must also certify the same enrollment information. Data is also verified through computer matching programs with other agencies.

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

Veterans who participate in VBA education programs must certify their enrollment monthly. The School certifying official must also certify the same enrollment information. Data is also verified through computer matching programs with other agencies. Regulations (to be placed in effect FY 2006) require loan program participants to provide loan performance data on existing active VA home loans monthly or more often. Certain data such as dividend rates are updated on an annual schedule. Other data is updated as a result of returned mail, or returned direct deposits, or through contact with policyholders after a significant event affecting their account.

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

Veterans must provide supporting documentation that verifies their claims such as marriage, birth, and death certificates, DD-214's and other documentation. These documents are reviewed by the Regional Office Veterans Claims Examiners to certify authenticity and accuracy. Automated edits and audits determine that a) a data element is present, and b) that the value is consistent with the data requested, and c) consistent with the record being created/updated. Applications for insurance benefits are verified using other data within the VA. For instance, applicants for Service-Disabled Veterans Insurance must have received rating for a new service-connected disability in the last two years, and applicants for Veterans Mortgage Life Insurance must previously have received a grant for specially adapted housing. Applications from current customers, such as to receive a loan, are verified against existing insurance records. Certain data such as SSN is verified with Social Security Administration. This and other data about current customers is verified through contact after a significant event affecting their account, or as a result of returned mail/ returned direct deposits that cause us to search out a better address. All data are matched against supporting claims documentation submitted by the veteran, widow, or dependent. Certain data such as SSN is verified with the Social Security Administration. Prior to any award or entitlement authorization(s) by the VBA, the veteran record is manually reviewed and data validated to ensure correct entitlement has been approved.

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

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.

**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update Date**

PROCEED TO SECTIONS 6 - 13 OF THE PRIVACY IMPACT ASSESSMENT FORM BY CLICKING THE LINK BELOW
https://vaww.camsit....6%20-%2013

Section 5.6 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

PIA SECTIONS 6 - 13

Project Name

Benefits Support Services-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.

VRE-Contractor is the systems Administrator and has access to all data. There provide maintenance of the system and data management. The contract number they operate under is: 101-Y57163. PSI - Contractor provides system maintenance support which requires access to data for troubleshooting and verification of system performance. Contract # 101Y-Y67161.

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.

VRE-Compensation and Pensions Service – Information related to the service related disabilities. Education Service – Information related to Education and Training. Veterans Health Administration – Information related to VA hospitalization. VA Insurance Service – Information related to insurance for severely disabled veterans. Loan Guaranty – Information related to specially adapted housing. 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. INS - Information is shared with the BDN and BIRLS systems to update insurance-specific fields in those systems. Also, interface with BDN is to allow policyholders to pay premiums by deduction from benefits. BIRLS/VADS information is used by various departments within Veterans Health Administration to process veteran benefits claims (e.g., health related benefits/claims). Information would be veterans name, SSN, date of birth, dates of service, and address).

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.

BIRLS shares (sends/receives) information to/from the following agencies: DMDC – Defense Manpower Data Center sends new enlistee information to BIRLS thereby ensuring that VBA has a record for military personnel as soon as they enlist into the service. It also interfaces with DMDC to record and display retired military pay for all retired veterans.
DOD (Quantico) – Department of Defense Marine Corps in Quantico, VA requests service medical records information through BIRLS.
DOE – Department of Education exchanges information with BIRLS regarding veteran enrollment in various schools throughout the nation and allows educational institutions to verify that a student is a veteran for whom educational benefits may be paid.
Department of Treasury is notified by check intercept processing regarding checks that need to be stopped.
NARA – National Archives and Records Administration receives all retired folders from BIRLS.
National Academy of Sciences Institute of Medicine requests batch extracts from BIRLS.

Medical Follow-up Agency request information from BIRLS.
Office of Child Support requests batch extracts from BIRLS.
Office of Policy and Planning requests information from BIRLS.
Selective Service requests batch extracts from BIRLS.
SSA - Social Security Administration access the BIRLS database to obtain appropriate information regarding veterans.
VADS shares (sends/receives) information to/from the following agencies:
DMDC - Defense Manpower Data Center sends new enlistee information.
Prudential Insurance – VADS provides a list of veterans that Prudential contacts regarding continuation of insurance benefits.
LASON - VADS provides a list of veterans that LASON contacts regarding educational benefits
Selective Service –Selective Service receives list of veterans added into VADS.

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.

INS - Housing and Urban Development - loan origination and default data including VA Loan Identification number. Veteran name/address/ssn are NOT included.
BIRLS shares (sends/receives) information to/from the following agencies: DMDC – Defense Manpower Data Center sends new enlistee information to BIRLS thereby ensuring that VBA has a record for military personnel as soon as they enlist into the service. It also interfaces with DMDC to record and display retired military pay for all retired veterans.
DOD (Quantico) – Department of Defense Marine Corps in Quantico, VA requests service medical records information through BIRLS.
DOE – Department of Education exchanges information with BIRLS regarding veteran enrollment in various schools throughout the nation and allows educational institutions to verify that a student is a veteran for whom educational benefits may be paid.
Department of Treasury is notified by check intercept processing regarding checks that need to be stopped.
NARA – National Archives and Records Administration receives all retired folders from BIRLS.
National Academy of Sciences Institute of Medicine requests batch extracts from BIRLS.
Medical Follow-up Agency request information from BIRLS.
Office of Child Support requests batch extracts from BIRLS.
Office of Policy and Planning requests information from BIRLS.
Selective Service requests batch extracts from BIRLS.
SSA - Social Security Administration access the BIRLS database to obtain appropriate information regarding veterans.
VADS shares (sends/receives) information to/from the following agencies:
DMDC - Defense Manpower Data Center sends new enlistee information.
Prudential Insurance – VADS provides a list of veterans that Prudential contacts regarding continuation of insurance benefits.
LASON - VADS provides a list of veterans that LASON contacts regarding educational benefits
Selective Service –Selective Service receives list of veterans added into VADS.

No	**State Government Agency**

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

No	**Local Government Agency**

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

Yes	**Other Project / System**

If information is shared with other projects or systems:

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

Each interfacing system is responsible for the protection of Privacy Act and Freedom of information Act information residing on that system.
BIRLS Internal Interfaces:

BDN - Benefits Delivery Network connects to BIRLS; BDN is employed by VBA to process entitlements for Compensation and Pension, Education, and Vocational Rehabilitation and Employment.
· CARS – Centralized Accounts Receivable System requires an interface with BIRLS to update the bankruptcy indicator.
· C&P - Compensation and Pension requires BIRLS for creation of the pending issue file which is used for the C&P master record.
· Corporate Database - BIRLS interfaces with VBA's corporate database to provide service information and identifying information.
· COVERS Control of Veterans Records System - BIRLS tracks folders between Regional Offices or places of folder retirement. It has an interface with the (COVERS), which tracks folders within a Regional Office.
· Data Warehouse - BIRLS interfaces with VBA's data warehouse to provide service information, identifying information, and other data that may be used at a meta-data level.
· INS - BIRLS also interfaces with the Insurance system in Philadelphia, enabling VA personnel at regional offices to identify Insurance information.
· Mobilization requires an online interface with BIRLS.

· MVR Master Veterans Record - BIRLS provides an online interface to the Austin Automation Center's (AAC) Master Veteran Record (MVR) application, allowing all of the users of MVR to access the identification and service information located in the BIRLS database.
· OIG – Office of Inspector General uses BIRLS as one of their primary sources for investigating fraud.
· PAID - Personnel and Accounting Integrated Data and Fee Basis interface with BIRLS to identify veterans that are VA employees for security purposes.
· PIES - Personnel Information Exchange System requires an online interface with BIRLS.
· RBA2000 – Rating Board Automation requires an online interface with BIRLS.
· SHARE – SHARE is a client-server application that performs inquires/updates against BIRLS.
· SMRTS - Service Medical Records Tracking System processing generates automatic updates to BIRLS. When a service medical record (SMR) folder is established in BIRLS, BIRLS determines if a claims folder already exists. If a claims folder exists, BIRLS will set the SMR folder in transit and RMC will send the record to the location of the claims folder.
· VADS - Veterans Assistance Discharge System and BIRLS interface allows service information for veterans to be added to BIRLS as soon as they are discharged from the service.
· VBA Training Academy - BIRLS provides a training database to enable the training of new adjudicators.
· VBA Common Security – BIRLS provides critical sensitive information to help maintain the security of VBA applications and records.
· VETSNET – Veterans Service Network requires an online interface with BIRLS.
· VHA - Veterans Health Administration obtains information from BIRLS to determine eligibility for treatment at VA hospitals. VHA uses HINQ (Hospital INQuiry) transactions to access pertinent information from BIRLS.
· WINRS - WACO Indianapolis Newark Roanoke Seattle case management system requires an online interface with BIRLS.

VADS Internal Interfaces:
· BIRLS – Veterans Assistance Discharge System and BIRLS interface allows service information for veterans to be added to BIRLS as soon as they are discharged from the service.
· Education (Chapter 30) provides list of veterans to be contacted regarding educational benefits.
· VACO - VA Central Office receives list of veterans added into VADS.

· BDN - Benefits Delivery Network connects to BIRLS; BDN is employed by VBA to process entitlements for Compensation and Pension, Education, and Vocational Rehabilitation and Employment.
· CARS – Centralized Accounts Receivable System requires an interface with BIRLS to update the bankruptcy indicator.
· C&P - Compensation and Pension requires BIRLS for creation of the pending issue file which is used for the C&P master record.
· Corporate Database - BIRLS interfaces with VBA's corporate database to provide service information and identifying information.
· COVERS Control of Veterans Records System - BIRLS tracks folders between Regional Offices or places of folder retirement. It has an interface with the (COVERS), which tracks folders within a Regional Office.
· Data Warehouse - BIRLS interfaces with VBA's data warehouse to provide service information, identifying information, and other data that may be used at a meta-data level.
· INS - BIRLS also interfaces with the Insurance system in Philadelphia, enabling VA personnel at regional offices to identify Insurance information.
· Mobilization requires an online interface with BIRLS.
· MVR Master Veterans Record - BIRLS provides an online interface to the Austin Automation Center's (AAC) Master Veteran Record (MVR) application, allowing all of the users of MVR to access the identification and service information located in the BIRLS database.
· OIG – Office of Inspector General uses BIRLS as one of their primary sources for investigating fraud.
· PAID - Personnel and Accounting Integrated Data and Fee Basis interface with BIRLS to identify veterans that are VA employees for security purposes.
· PIES - Personnel Information Exchange System requires an online interface with BIRLS.
· RBA2000 – Rating Board Automation requires an online interface with BIRLS.
· SHARE – SHARE is a client-server application that performs inquires/updates against BIRLS.
· SMRTS - Service Medical Records Tracking System processing generates automatic updates to BIRLS. When a service medical record (SMR) folder is established in BIRLS, BIRLS determines if a claims folder already exists. If a claims folder exists, BIRLS will set the SMR folder in transit and RMC will send the record to the location of the claims folder.
· VADS - Veterans Assistance Discharge System and BIRLS interface allows service information for veterans to be added to BIRLS as soon as they are discharged from the service.
· VBA Training Academy - BIRLS provides a training database to enable the training of new adjudicators.
· VBA Common Security – BIRLS provides critical sensitive information to help maintain the security of VBA applications and records.
· VETSNET - Veterans Service Network requires an online interface with BIRLS.
· VHA - Veterans Health Administration obtains information from BIRLS to determine eligibility for treatment at VA hospitals. VHA uses HINQ (Hospital INQuiry) transactions to access pertinent information from BIRLS.
· WINRS - WACO Indianapolis Newark Roanoke Seattle case management system requires an online interface with BIRLS.

VADS Internal Interfaces:
· BIRLS – Veterans Assistance Discharge System and BIRLS interface allows service information for veterans to be added to BIRLS as soon as they are discharged from the service.
· Education (Chapter 30) provides list of veterans to be contacted regarding educational benefits.
· VACO - VA Central Office receives list of veterans added into VADS.

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:

System Users: Employees with a need to know: e.g. employees are granted access to data that is necessary for the performance of their duties System Owner and Project Manager: Access is used for quality control, program management and oversight System Administrator and Contractors: Access is used to research and trouble shoot application problems. Other Federal Agency/Other System: Loan level information is provided to GNMA via secure FTP for GPADS – that application is used by Federal residential credit / home loan agencies for lender management and oversight and economic analyses – Note: This information does not contain names or SSNS, but may be consider private in that it does include the VA loan identification number and default status information. Other User(s): Program participants have restricted access to some applications for use in requesting appraisals, reporting loan information, etc. Access is restricted to cases being processed by the participant. ED-VA employees who process the benefits have access. School certifying officials at education institutions are designated" Other Users." They use the VA-ONCE system to submit veterans' claims for education benefits and to submit information on their enrollment, attendance, credits, terms, and courses. Education institutions initially provide the veterans' personal information to the VA, and this information is, in turn, made available to them in administering school enrollment and certification. No external system has access to personal information processed by the systems under this PIA (reference paragraph 1.A.3). The systems reference in paragraph 1.A.3 interfaces with each other and the Benefits Delivery Network (BDN) to process education benefit claims. We have the authority to exchange data with Other Veteran Organizations, Other Federal Agencies, and State and Local Agencies as outlined in the System of Records 58VA21/22/28. LGY- System Users: Employees with a need to know: e.g. employees are granted access to data that is necessary for the performance of their duties. System Owner and Project Manager: Access is used for quality control, program management and oversight. System Administrator and Contractors: Access is used to research and trouble shoot application problems. Other Federal Agency/Other System: Loan level information is provided to GNMA via secure FTP for GPADS – that application is used by Federal residential credit / home loan agencies for lender management and oversight and economic analyses – Note: This information does not contain names or SSNS, but may be consider private in that it does include the VA loan identification number and default status information. Other User(s): Program participants have restricted access to some applications for use in requesting appraisals, reporting loan information, etc. Access is restricted to cases being processed by the participant.

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

Access is authorized by VA officials based on the need of the person/agency applying for access and their responsibilities, privileges, 'need to know', and security profiles. VA Form 9957 is submitted to the ISO for access to BIRLS/VADS. Access security is implemented in compliance with VA's Office of Cyber and Information Security (OCIS) guidelines, policies, and mandates. VBA systems have documented Memorandums of Understanding/Agreement with all of its business partners, including veteran organizations, federal agencies, state agencies, and local agencies in regard to confidential business information, Privacy

Act, and certain information that is subject to confidentiality protections. Access by VA employees is restricted by a security control module to that data they need to do their job. There are also internal controls which limit which record a user and review or update.

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

VBA systems have documented Memorandums of Understanding/Agreement with all of its business partners, including veteran organizations, federal agencies, state agencies, and local agencies in regard to confidential business information, Privacy Act, and certain information that is subject to confidentiality protections. This includes all the entities mentioned previously within this document and includes the Department of Defense, the Social Security Administration, Educational Institutions, Federal Housing Administration, Internal Revenue Service and the Department of Housing and Urban Development. A detailed listing of all business partners is available from the project manager. VBA has emplaced strict control measures to prevent the inadvertent or deliberate release of information to non-authorized personnel. Access criteria, procedures controls, and responsibilities are implemented in compliance with VA's Office of Cyber and Information Security (OCIS) guidelines, policies, and mandates. The information processed on the EDU Maintenance and Operations applications is sensitive data because it contains personal information associated with veterans of all the armed services and their family members. This information includes names, social security numbers, and dates of birth, marriage, and death as well as information describing the financial status of veterans. VBA has emplaced strict control measures to prevent the inadvertent or deliberate release of information to non-authorized personnel. Criteria, procedures, controls, and responsibilities regarding access are documented in the Security Plan. Ensuring that protection of data to only authorized persons has been identified as a low risk. It is a defined system requirement.

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

User access is restricted. Access is granted on the principles of least privilege and separation of duties. A sensitive file is used to control further access to selected veteran records, which contain “sensitive” information not generally disclosed to all the VBA users. Internally, station directors may authorize access to the system for any employee that requires access to the network, providing the employee meet the appropriate personnel security requirements as outlined in the VBA IT Handbook No. 5.00.02 HB2. Non-VBA employees, such as Veterans Service Organization (VSO) representatives and student interns, are not considered employees of the United States for the purpose of laws administered by the Office of Personnel Management. Since these individuals do not meet the requirement for employee security review, their access to veterans benefits data is limited to inquiry commands only. These individuals must go through a certification process in order to gain access to the system. Application security is controlled through the use of Common Security Services (CSS) through the establishment of a special login account and the creation of a separate security account for each application accessible through CSS. In addition, access to certain records, specifically those that contain data of a sensitive nature, is restricted through the assignment, to those records, of varying levels of sensitivity.

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

Internal controls are in place that disallows unauthorized browsing. A security violation is generated if an employee attempts unauthorized browsing and the event is investigated by the Security Officers. Incident handling capability has been incorporated into the system, including intrusion detection monitoring, and audit log reviews. The Department has centralized all component incident response capabilities into a single VA-CIRC. Associated guidelines and procedures require that all VA computer security incidents be reported to the VA-CIRC through the facility or office ISO within one business day of the first observation of the incident. VA-CIRC policy requires that, upon identification of an incident/suspected incident, a preliminary report is

generated. For incidents that affect critical systems and/or may have adverse global effects on the VA network, the VA-CIRC will dispatch a fly-away team of technical and forensic experts to assist facility personnel in impact containment. A complete incident report, including a full description of the final incident resolution, is submitted to the VA-CIRC no more than five business days after the incident is resolved by the reporting entity. The VA-CIRC is also responsible for supplying incident reports to OCIS, the primary organizational contact for the affected organization, and to other VA organizations as appropriate; providing a quarterly report summarizing all incidents to the FedCIRC as provided for in a letter of agreement between VA and the FedCIRC; and, responding directly to FedCIRC inquiries. If an individual incident appears to constitute criminal activity, the facility ISO coordinates the incident with local area law enforcement authorities; and, the VA-CIRC notifies the VA OIG. The OIG provides the necessary federal law enforcement coordination (i.e. Federal Bureau of Investigation, Bureau of Alcohol, Tobacco, and Firearms) although the VA-CIRC does respond directly to federal law enforcement inquiries concerning specific incidents upon request. Annual training is taken by all VBA employees and contractors on rules of behavior with regards to the proper use of access to data, including privacy and security requirements and rules.

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.

Memo of understanding or agreement, Interagency Agreements, etc., are used to define responsibilities for protection of data provided. Data included in transfers is restricted to the minimum necessary for a specific task, e.g., to locate a veteran address, to pay a claim, to process a pre-authorized debit.

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

The federal agency receiving data from VBA is under the same Privacy Act and security requirements as VBA. Once they receive data it is their responsibility to ensure that it is properly used and handled. VA continues to work with federal agencies it shares personal information with to see that appropriate standards are in place and operational. VBA makes every effort ensure that i any personal information transmitted to other agencies is done in the most secure manner. FMS information transmitted to Treasury is 3DES-encrypted. For data transfer, VA uses Connect:Direct over a T-1 line. A description of the communications interconnection requirements for Treasury can be found in the Standards Document for External Network Connections, General Edition; this contains available communications protocols, data transfer capabilities, specific communications hardware, and encryption requirements to establish a secure connection to FMSnet. As of October 2006, data interchange with the Federal Reserve Bank is accomplished by connecting to their Fedadvantage system through the VA NOC. This requires use of a VPN device specially purchased from the FRB. Records are transmitted to DOD (DFAS) via file transfer protocol. Records are mailed to Coast Guard. In both cases, the records do not include addresses or bank data, but can include other personal information such as insurance file number.

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

Encrypted files, via CD, tape, secure file transfer protocol. Information transmitted to Treasury is 3DES-

encrypted. For data transfer, VA uses Connect:Direct over a T-1 line. A description of the communications interconnection requirements for Treasury can be found in the Standards Document for External Network Connections, General Edition; this contains available communications protocols, data transfer capabilities, specific communications hardware, and encryption requirements to establish a secure connection to FMSnet. As of October 2006, data interchange with the Federal Reserve Bank is accomplished by connecting to their Fedadvantage system through the VA NOC. This requires use of a VPN device specially purchased from the FRB. Records are transmitted to DOD (DFAS) via file transfer protocol. Records are mailed to Coast Guard. In both cases, the records do not include addresses or bank data, but can include other personal information such as insurance file number. If or when 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.

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

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

Any federal agency receiving data from VBA is under the same Privacy Act and security requirements as VBA. Therefore any personal data they obtain must be kept in secure areas on secured networks. In addition, VBA requires the recipients of any data must sign rules of behavior to assist in prevention of unauthorized disclosure of privacy information.

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

Any federal agency receiving personal data from VBA are under the same Privacy Act and security training requirements as VBA.

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

-		**SECTION INCOMPLETE**

★	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 22, 2007	**Section Update Date**

Section 6.1 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

6.2 Access to Records and Requests for Corrections

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

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

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

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

VBA systems and BIRLS/VADS are not accessible to the public. Individuals may request information concerning their benefits/claims from the VBA Regional Office in their area. Individuals may also request their information under the Freedom of Information Act (FOIA). Education benefit application has implemented a multi level information access control system. This control system is based upon information sensitivity, access requirements based on individual or group roles and responsibilities. Individual PII access requires admin or supervisory roles above the individual. PII for the admin or supervisory levels must be obtained by another peer admin or supervisory level. Insurance benefits Self-Service application makes certain Insurance data available via the Internet. Veterans may access their basic policy information about premiums, dividends, and loan value, view their beneficiary (B&O) designation or request a mailed copy of their policy, policyholders' annual statement, premium bills and other information. They may also request a policy loan. Access to Self-Service requires a PIN, which the policyholder requests online and is mailed to the address of record. The B&O and loan functions also require a user-specified password. PIN and password cannot be viewed by Insurance Center personnel; the process must be re-initiated at the website by the user. Policyholders may also request information by mail, e-mail, and telephone at the toll-free number. However, employees are not allowed to access their records. 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?

Individuals currently report errors to the VBA Regional Office in their area. VBA Regional Office claim representative enter corrections on behalf of the individual. Any person who wishes to determine whether a record is being maintained in BIRLS/VADS under his or her name or other personal identifier, or who has a routine inquiry concerning the accuracy of the status of his or her established benefits may contact the nearest VA Regional Office. Requests concerning the specific content of a record must be in writing or in person to the VA Regional Office and/or Insurance Center at Philadelphia, Pennsylvania or St. Paul, Minnesota.

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

Every VA beneficiary has appeal rights. Appeal rights are addressed on VA Form 1-4107

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

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

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 22, 2007	**Section Update Date**

Section 6.2 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

7 Retention and Disposal

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

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

VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures.
System of Records Notices may be accessed via:
http://vaww.vhaco.va...ecords.htm
or
http://vaww.va.gov/f...y_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/v...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 ...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.

VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures. Electronic loan records are retained until they are no longer of interest to the program. Active insurance records are retained. Data on active records is changeable. Prior copies of active records and their changing values are not retained. Inactive records are purged from some applications, but the record as it appeared at its final active day is retained. A list of transactions affecting the system has been maintained since 1995 and there are no plans to remove records. The records retention program requires storage of inactive records at a servicing Federal Archives and Records Center for 50 years. Life insurance programs for veterans have been in force since 1919. It is not uncommon for VA to receive inquiries about old insurance policies. For instance, we receive frequent inquiries about military and VA insurance paperwork found in the effects of deceased veterans. Occasionally, these date back several years, and in a few well-publicized cases to deaths that occurred in WW II. To the extent these records can be retrieved and/or reconstructed, we can discharge our

duty to those veterans and their families. Loan Guaranty is evaluating this practice in relation to privacy requirements: e.g. does the privacy information need to be retained, or can program needs be met by retention of information that is not subject to privacy considerations? The data retention period for BIRLS data is contained in RCS VBA-1, Part I, Item Number 08-065.000 and subparagraphs, which states “Destroy files data in accordance with system design.” In 1968, BIRLS was designed to retain service member records indefinitely; therefore, there are no procedures for eliminating data. Record information pertaining to service members will continue to be maintained into perpetuity. Records are archived in accordance with retention policies and procedures. Education benefit records are retained at servicing Regional Office (RO) for the life of the veteran. At the death of the veteran, education benefit records are sent to the Federal Records Center (FRC) and maintained by FRC for 75 years

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

VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures. Shredding or burning for hard copy, erasure, and destruction of storage media for electronic records. Insurance data on tapes are controlled by the CA-TMS product. At the expiration of their retention period, tapes are returned to the pool and are written-over with subsequent processing cycles. Tapes returned from off-site storage are also returned to the pool and written-over. Electronic records are retained indefinitely. When hardware is excessed, fixed drives are sanitized of that copy of the data in accordance with VA and VBA procedures. After 75 years retention at the FRC, the education benefit records are destroyed. The data retention period for BIRLS data is contained in RCS VBA-1, Part I, Item Number 08-065.000 and subparagraphs, which states “Destroy files data in accordance with system design.”

7.c) Where are procedures documented?

VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures. System of Records 58VA21/22/28. Records Control Schedule (RCS) VBA-1, Part I, Section 8, available online at http://www.warms.vba.va.gov/admin23/rcs/part1/sec08.doc For insurance records: Philadelphia ITC Operating Memorandum 284-07-00, Subj: Protection of VA Indispensable Records and Philadelphia ITC Operating Memorandum 284-16-05, SUBJ: Direct Access Storage Device (DASD) Management.

7.d) How are data retention procedures enforced?

The Director of each RO enforces retention procedures at his/her station. The application prevents the deletion of data from the IDMS database where BIRLS data is stored. By using the CA-TMS product, and manual procedures in OMs 284-07-00 and 284-16-05. Proper off-site tape retentions are periodically verified via the Disaster Recovery Exercise when the depository sends all of the stored tapes to the alternate site.

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.)

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

Section 7 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

8 SECURITY

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

8.1 General Security Measures

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

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

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

At the project level, a standardized Department methodology is used to continually monitor and evaluate security for this major application. In accordance with the provisions of FISMA, a self-assessment of IT security management, operational, personnel, and technical controls is conducted on an annual basis, modeled after NIST Special Publication 800-26, Self-Assessment Guide for Information Technology Systems. The survey encompasses information concerning over 200 controls in 17 discrete categories, and is completed by team(s) of information security officers, business process owners, and technical leads.
The results of the survey are used in the annual IT Security Review, which is conducted immediately following the close of the survey period. During this review, the VA CIO, in conjunction with program managers and VA component CIOs, and with advice from the VA Office of Inspector General (OIG), evaluates the Department's overall IT security posture. The results of the review include identification of significant security performance gaps, and prioritization of key weakness areas for immediate remediation action, thereby effectively targeting those areas that will most improve the Department's security posture in the near-term. Security logs are reviewed on a daily basis. The Internal Control Staff is second signature to all manually-initiated disbursements. It receives reports and samples system disbursements.

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

Yes

8.2 Project-Specific Security Measures

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

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

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

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

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

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

All information stored in VBA databases is secured in agreement with VA strategy. This strategy implements Federal Regulations, VA IT security policy and guidelines, NIST Guidelines and industry best practices. Security is implemented in compliance with VA's Office of Cyber and Information Security (OCIS) guidelines, policies, and mandates. With guidance from OCIS, the VBA administers and monitors security controls on multiple operating levels including the managerial, operational and technical levels. This System uses strong passwords. Access is granted on the principles of least privilege and separation of duties. Users have completed ethics training, annual 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 are network (WAN) boundaries. Moreover, the VA employs a comprehensive incidence response unit to respond to unwanted incursions and institutes enterprise level anti-virus system to protect mission critical applications on the desktop. Finally, the VA security program is an iterative program with repeatable processes that, in an ongoing basis, will mitigate vulnerabilities, minimize security exposures and maintain security and operating risk at acceptable levels. A security plan has been developed that documents the procedures required ensuring the integrity, confidentiality, and availability to VA information. Specifically, personnel security, physical protection, production input/output controls, contingency planning, system hardware and software maintenance controls, security awareness and training, and incident response capabilities are discussed in detail. The details contained within these sections include specific activities and procedures, which ultimately ensure that the integrity, confidentiality, and availability to VA information contained within the system is protected as required by Federal policy. All files, records, reports, and other papers and documents pertaining to any claim under any of the laws administered by the Department of Veterans Affairs and the names and addresses of present or former members of the Armed Forces, and their dependents, in the possession of the Department shall be confidential and privileged. This specifically includes all individually identifiable health information of a veteran, which is stored electronically and in hard copy form. 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.

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

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update Date**

Section 8 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

9. CHANGE RECORD

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

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

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.

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETE**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update Date**

Section 9 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL

-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

10. CHILDREN'S ONLINE PRIVACY PROTECTION ACT

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

No

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

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

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

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETED**

		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update Date**

Section 10 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

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.

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

Full C&A every three years. During FISMA continuous monitoring phase (non C&A cycle) Region Five 1/3 of controls are re-tested annually per VA Handbook 6500. Patch management includes use of automated tools,

e.g. VBA Menu XXX, ACRB, Austin AC Computer Associates Unicenter, to effectively manage Operating system patches (UNIX and Windows). Use of User ID and strong passwords are required for access. Guest logons are not allowed. Technical controls are designed to minimize risk through "Least privilege" and internal controls (e.g. can't create and approve same veteran payment). Inactive accounts are automatically disabled after 90 days of non-use. Security software incorporates Power of Attorney (POA) restrictions and Sensitive Record management features (aka celebrity file) further restricting general access to the veteran data. Mandatory use of pre-set screen saver set at 15 minutes on workstations provides physical barrier to unauthorized access. Audit files record user activity. Security reports track activity in the Sensitive/POA files.

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

N	**The potential impact is <u>high</u> if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.**
Y	**The potential impact is <u>moderate</u> if the loss of availability could be expected to have a serious adverse effect on operations, assets, or individuals.**
N	**The potential impact is <u>low</u> if the loss of availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.**

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

N	**The potential impact is <u>high</u> if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.**
Y	**The potential impact is <u>moderate</u> if the loss of integrity could be expected to have a serious adverse effect on operations, assets, or individuals.**
N	**The potential impact is <u>low</u> if the loss of integrity could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.**

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

N	**The potential impact is <u>high</u> if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.**
Y	**The potential impact is <u>moderate</u> if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets, or individuals.**
N	**The potential impact is <u>low</u> if the loss of confidentiality could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.**

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

Moderate

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

NIST SP800-53a (Second Public Draft) and NIST SP800-60 (FIPS-200) for Moderate rated systems.

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

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update Date**

Section 11 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

12. PUBLIC AVAILABILITY

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

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

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

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

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

No

12.b) If yes, specify:

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

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.
**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update Date**

Section 12 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.

-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)

13. ACCEPTANCE OF RESPONSIBILITY AND ACKNOWLEDGEMENT OF ACCOUNTABILITY:

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

[SIGNATURE]

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

Kevin Causley, Acting Director OI&T Field Operations Region 5 12/05/2007

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

-		**SECTION INCOMPLETE**
★	Yes	**SECTION COMPLETED**
		I have completed and reviewed my responses in this section.

**	**NOTE:**	If you are resubmitting your updates, first select "NO Value" from the dropdown and submit and then select "Yes" and submit again.
	Aug 21, 2007	**Section Update Date**

Section 13 Review:

		PRIVACY SERVICE SECTION REVIEW AND APPROVAL
-		The Privacy Service has not reviewed this section.
-		The Privacy Service has reviewed this section. Please make the modifications described below.
★	Yes	The Privacy Service has reviewed and approved the responses in this section.
**	**NOTE:**	If you are resubmitting your REVIEW or if you already have an YES, then first select "NO Value" and submit
		and then select "Yes" and submit again.
	Sep 23, 2007	**Section Review Date**

PRIVACY SERVICE COMMENTS: (Include reviewers Name and Contact)