

Welcome to the PIA for FY09!

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.

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.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirectly identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

(FY 09) PIA: System Identification

Program or System Name: REGION 5> VBA> BDN Payment History> CFD

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

Description of System / Application / Program: The BDN Payment History application enables VBA employees to track benefit outlays to eligible veterans, their families, and their beneficiaries in an efficient, timely, and compassionate manner through the Treasury Inquiry (TINQ) functionality. The BDN Payment History application provides information from benefit outlays from Compensation and Pension (C&P), Education, and Vocational Rehabilitation and Employment (VR&E) business lines. The BDN Payment History application is an exact replica of the legacy BDN system TINQ functionality that has been migrated and re-hosted to operate in the new Web Logic Java Web-enabled processing environment, which utilizes the corporate three-tier database.

Facility Name: Austin Information Technology Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Michael Regis	202-461-9702	michael.regis@va.gov
Information Security Officer:	Gregory H. Johnson	202-461-9174	gregory.johnson6@va.gov
Acting Assistant Secretary of Information & Technology	Stephen W. Warren	202-461-6910	stephen.warren@va.gov
Person Completing Document:	Stephen M. King	202-461-9454	stephen.king3@va.gov
System Owner:	Kevin C. Causley	202-461-9170	kevin.causley@va.gov
Alternate Information Security Officer	Mary D. Barley	202-461-9175	mary.barley@va.gov
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	08/2008		
Date Approval To Operate Expires:	08/28/2011		

What specific legal authorities authorize this program or system: Title 38, United States Code

What is the expected number of individuals that will have their PII stored in this system: ~20,000,000

Identify what stage the System / Application / Program is at: Operations/Maintenance

The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.

1 year

Is there an authorized change control process which documents any changes to existing applications or systems?

Yes

If No, please explain:

Date of Report (MM/YYYY): 02/2009

If answers 'Yes' to one or more of the following, please check the appropriate box, continue to the next tab, and complete the remaining questions on this form. If none have been checked then skip to Signatures tab, obtain the appropriate signatures, and submit this document.

- Has a PIA NOT been completed within the last three years?
- Have any changes been made to the system since the last PIA?
- Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- Does this system/application/program collect, store or disseminate PII/PHI data?
- Does this system/application/program collect, store or disseminate the SSN?

(FY 09) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

For each applicable System(s) of Records, list:

1. All System of Record Identifier(s) (number):

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

2. Name of the System of Records:

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

3. Location where the specific applicable System of Records Notice may be
accessed (include the URL):

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

Have you read, and will the application, system, or program comply with, all data
management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

No

Is PII collected by verbal methods?

No

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

No

Proximity and Timing: Is the privacy notice provided at the time of data collection?

Yes

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

Yes

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

Yes

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

Yes

(FY 09) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this messaged conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	VA File Database	Veterans are not notified of their Privacy Act protection via BDN Payment History; they are notified when the PII is collected by other BDN Payment History feeder systems, such as BDN, VADIR, or BIRLS.	Automated	Automated
Family Relation (spouse, children, parents, grandparents, etc)				
Service Information				
Medical Information				
Criminal Record Information				
Guardian Information				
Education Information				
Benefit Information	VA File Database	Veterans are not notified of their Privacy Act protection via BDN Payment History; they are notified when the PII is collected by other BDN Payment History feeder systems, such as BDN, VADIR, or BIRLS.	Automated	Automated

Other (Explain): Payment or debt collection information in dollars and categorized by type of payment.	VA File Database	Veterans are not notified of their Privacy Act protection via BDN Payment History; they are notified when the PII is collected by other BDN Payment History feeder systems, such as BDN, VADIR, or BIRLS.	Automated	Automated
--	------------------	---	-----------	-----------

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (BDN)	Voluntary	Data collection is voluntary at the feeder systems.
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	No			
Medical Information	No			
Criminal Record Information	No			
Guardian Information	No			
Education Information	No			
Benefit Information	Yes	VA Files / Databases (BDN)	Voluntary	Data collection is voluntary at the feeder systems.

Other (Explain): Payment or debt collection information in dollars and categorized by type of payment.

Yes

VA Files / Databases (BDN)

Voluntary

Data collection is voluntary at the feeder systems.

Other (Explain)

Other (Explain)

(FY 09) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VBA	Yes	Payment History receives PII data from BDN	PII	
Other Veteran Organization					
Other Federal Government Agency					
State Government Agency					
Local Government Agency					
Research Entity					
Other Project / System					
Other Project / System					
Other Project / System					

(FY09) PIA: Access to Records

Does the system gather information from another system? Yes

Please enter the name of the system: Benefits Delivery Network

Does the system gather information from an individual? No

If information is gathered from an individual, is the information provided:

- Through a Written Request
- Submitted in Person
- Online via Electronic Form

Is there a contingency plan in place to process information when the system is down?

Yes

(FY09) PIA: Secondary Use

Will PII data be included with any secondary use request?

No

- Drug/Alcohol Counseling Mental Health HIV
 Research Sickle Cell Other (Please Explain)

if yes, please check all that apply:

Describe process for authorizing access to this data.

Answer:

(FY 09) PIA: Program Level Questions

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

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Information is generated from system provide information and entered to specific fields of database records. The Payment history information is stored within the database(s) for auditing and tracking purposes in support of activities related to processing individual claim or claims the veteran has been granted.

How is data checked for completeness?

Answer: Data are checked for completeness by system audits and manual verifications.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Data are updated from an interface with the BDN mainframe. There is no requirement to validate the payment information with the veteran. Verifications and system audits are performed.

How is new data verified for relevance, authenticity and accuracy?

Answer: Manually by examining content for accuracy and relevance to other veteran data.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer: n/a

(FY 09) PIA: Retention & Disposal

What is the data retention period?

Answer: Individual claims file folders and the compensation, pension, rehabilitation and education claims records contained therein are retained at the servicing regional office for the life of the veteran. At the death of the veteran, these records are sent to the Federal Records Center (FRC), maintained by the FRC for 75 years and thereafter destroyed at the direction of the Archivist of the United States.

Explain why the information is needed for the indicated retention period?

Answer: The veterans records are not eliminated but are stored either on tape or disk indefinitely. If veterans records are inactive, the master record remains in the Beneficiary Identification Record Locator System (BIRLS). If the veterans records are active (benefit claims have been awarded) these records remain within the BDN databases.

What are the procedures for eliminating data at the end of the retention period?

Answer: Data is not eliminated but stored on removable media.

Where are these procedures documented?

Answer: The data retention period for BDN Payment History data is contained in RCS VBA-1. All active and terminated veterans records are retained indefinitely; therefore, there are no procedures for eliminating data.

How are data retention procedures enforced?

Answer: Daily journal logs are generated and tape backups are performed daily which are stored off site. In addition a duplicate set of the back up tapes are stored for the BDN Disaster Recovery platform installed at the Philadelphia ITC.

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.)

Answer: The data retention schedule for BDN was approved by NARA; BDN Payment History operates within the scope of this approval as a subfunction of BDN operations.

(FY 09) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 09) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.

Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..

Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

No

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?

No

If 'No' to any of the 3 questions above, please describe why:

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

Is adequate physical security in place to protect against unauthorized access?

Yes

If 'No' please describe why:

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

Answer: A standardized Department methodology based on the direction in National Institute of Standards and Technology (NIST) guidance is used to continuously monitor, test and evaluate security for this major application. The approximately 60 common security controls provided by the Office of Information and Technology (OIT), or other respective VA Program Office, are tested every year. Application-specific security testing evaluates approximately one-third of the remaining 90 controls on an annual basis, with the entire respective application NIST Special Publication (SP) 800-53 security control baseline—at the Federal Information Processing Standard (FIPS) 199 level of moderate--being tested over each three-year period. The testing supports certification and re-accreditation requirements, as well as Federal Information Security Management Act (FISMA) requirements to annually test the operational, management, and technical controls of each Department system. The specific controls identified for testing are selected by OIT Operations, with advice from the VA Office of Cyber Security (OCS), and inclu

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- | | |
|---|--|
| <input checked="" type="checkbox"/> Air Conditioning Failure | <input checked="" type="checkbox"/> Hardware Failure |
| <input checked="" type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Malicious Code |
| <input checked="" type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Computer Misuse |
| <input checked="" type="checkbox"/> Bomb Threats | <input checked="" type="checkbox"/> Power Loss |
| <input checked="" type="checkbox"/> Cold/Frost/Snow | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Communications Loss | <input checked="" type="checkbox"/> Storms/Hurricanes |
| <input checked="" type="checkbox"/> Computer Intrusion | <input checked="" type="checkbox"/> Substance Abuse |
| <input checked="" type="checkbox"/> Data Destruction | <input checked="" type="checkbox"/> Theft of Assets |

- Data Destruction
- Data Disclosure
- Data Integrity Loss
- Denial of Service Attacks
- Earthquakes
- Eavesdropping/Interception
- Fire (False Alarm, Major, and Minor)
- Flooding/Water Damage
- Theft of Assets
- Theft of Data
- Vandalism/Rioting
- Errors (Configuration and Data Entry)
- Burglary/Break In/Robbery
- Identity Theft
- Fraud/Embezzlement

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- Risk Management
- Access Control
- Awareness and Training
- Contingency Planning
- Physical and Environmental Protection
- Personnel Security
- Certification and Accreditation Security Assessments
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Media Protection

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

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

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?

(Choose One)

The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.

The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

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

(Choose One)

The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.

The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

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

(Choose One)

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

The controls are being considered for the project based on the selections from the previous assessments?

The VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility' common security controls. These issues are identified and described in the system security plans for the individual information systems.

Please add additional controls:

FY 09: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on. Please indicate the question you are responding to and then add your comments.

(FY 09) PIA: Final Signatures

Facility Name: Austin Information Technology Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Michael Regis	202-461-9702	michael.regis@va.gov
Information Security Officer:	Gregory H. Johnson	202-461-9174	gregory.johnson6@va.gov
Chief Information Officer:			
Person Completing Document:	Stephen M. King	202-461-9454	stephen.king3@va.gov
System / Application / Program Manager:	Kevin C. Causley	202-461-9170	kevin.causley@va.gov

Date of Report: 02/01/2009
OMB Unique Project Identifier: 029-00-02-00-01-1120-00
Project Name: REGION 5> VBA> BDN Payment
History> CFD