

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> HINES ITC> LAN

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

Description of System / Application / Program: The Hines ITC is a General Support System that supports user access to multiple applications. The LAN serves as the default repository for incidental data used and processed by various VBA Major Applications. The applications that are accessed are described in Tab 8, Additional Comments. This data is used in granting compensation, pension, education, vocational rehabilitation and employment, insurance, and loan guaranty benefits to veterans. Information stored also includes data used for various administrative functions. Data flows between the desktop, servers, and related telecommunication devices both locally (LAN) and remotely (VA- wide area network (WAN)). The majority of the data resides on the Bull mainframe computer at the Hines ITC and the VBA Corporate Database housed at the Austin Information Technology Center (AITC). Users have access to the VA Intranet and Internet. The system provides RO employees local access to file and print sharing services on the LAN. It also provides client access to various applications, including email.

Facility Name: Hines 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:	n/a		
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)	09/2008		

Date Approval To Operate Expires: 09/04/2011

What specific legal authorities authorize this program or system: Title 38, United States Code, section 501(a) and Chapters 11, 13, 15, 18, 23,30, 31, 32, 34, 35, 36, 39, 51, 53, 55.

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. 9 years

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): 02/27/2009

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?

- 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): 36VA00, 38VA21, 46VA00, 53VA00, 55VA26, 58VA21/22/28
2. Name of the System of Records: 36VA00: SOR Name: Veterans and Armed Forces Personnel Ur Government Life Insurance Records-VA; 38VA21: SOR Name: \ Beneficiaries Identification Records Location Subsystem-VA; 4 Veterans, Beneficiaries and Attorneys United States Governm Records-VA; 53VA00: SOR Name: Veterans Mortgage Life Insu SOR Name: Loan Guaranty Home, Condominium and Manufac Applicants Records, Specially Adapted Housing Applicant Recc Applicant Records-VA; 58VA21/58VA22/58VA28: SOR Name: (Pension, Education, and Rehabilitation 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? Yes

Is PII collected by verbal methods? Yes

Is PII collected by automated methods? Yes

Is a Privacy notice provided? Yes

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 message conveyed to them?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Multiple collection vectors available	Privacy Act statements and notifications are provided by written correspondence to the veteran, widow or dependent claimant. All VBA online Applicants are required to complete form 21-4242 -	Verbally, in writing, and automatically, depending on how the information is collected.
Family Relation (spouse, children, parents, grandparents, etc)	Multiple collection vectors available	Authorization and Consent to Release Information to the Department of Veterans Affairs (VA). Privacy Act	
Service Information	Multiple collection vectors available	statements and notifications are provided on all data collection web portals. Data	
Medical Information	Multiple collection vectors available	from the BDN databases are transferred to the US Treasury System to generate the veterans payments. Federal Agencies	
Criminal Record Information	Multiple collection vectors available	provide the required Privacy Act authorizations to handle such data.	
Guardian Information	Multiple collection vectors available		
Education Information	Multiple collection vectors available		
Benefit Information	Multiple collection vectors available		
Other (Explain)	Multiple collection vectors available		

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?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Multitple sources, but primarily the Veteran.	Mandatory
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Multitple sources, but primarily the Veteran.	Mandatory
Service Information	Yes	DoD	Mandatory
Medical Information	Yes	Veteran, VHA, DoD, private doctors.	Mandatory
Criminal Record Information	Yes	Federal, State, Local law enforcement	Mandatory
Guardian Information	Yes	Multitple sources, but primarily the Veteran.	Mandatory
Education Information	Yes	Multitple sources, but primarily the Veteran.	Mandatory
Benefit Information	Yes	Multitple sources, but primarily the Veteran.	Mandatory
Other Personal Information of the Veteran or Primary Subject Other (Explain) Other (Explain)	Yes	Multitple sources, but primarily the Veteran.	Mandatory

How is a privacy notice provided?

Verbally, in writing, and automatically, depending on how the information is collected.

Additional Comments

All data collection is r
in the sense that ben
cannot be provided to
unless the appropriat
information is submit
VBA. The veteran's de
release information is
voluntary, yet the typ
information that mus
provided is mandator
content.

(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?
Internal Sharing: VA Organization	VBA, VHA, NCA	Yes	Provide monetary payments to veterans in recognition of the effects of disabilities, diseases, or injuries incurred or aggravated during active military service. EDU administers education and training programs for veterans and eligible beneficiaries. VR&E assists eligible, service-connected, disabled veterans in preparing for employment, and assistance for testing, training, and education for eligible beneficiaries. VA Hospital access is for verifying veteran eligibility for hospital care and services; access is limited to INQUIRY-only capabilities. NCA performs inquiries to establish veteran status for authorization for internment in VA cemetery.	Both PII & PHI

Other Veteran Organization	VSO	Yes	Co-located Veterans Service Organizations (VSOs) –Co-located Veterans Service Organizations at VBA regional offices have been given on-line read only access. Remote Veterans Service Organizations have been given on-line read only access to SHARE and MAPD. The remote VSOs access veteran data securely through VA’s Virtual Private Network. This access is authorized by VA regulations.	Both PII & PHI
----------------------------	-----	-----	---	----------------

Other Federal Government Agency	Treasury, DoD, HUD, SSA, FHA, IRS	No	Shared data includes any veteran data relating to benefits provided by Federal, State, and Local organizations. The system has documented Memorandums of Understanding Agreements with all of its VA business partners, federal agencies, state agencies and local agencies in regard to confidential business information, Privacy Act and certain information that is subject to confidentiality protections.	Both PII & PHI
---------------------------------	-----------------------------------	----	---	----------------

State Government Agency	Various agencies providing veterans benefits.	No		Both PII & PHI
-------------------------	---	----	--	----------------

Local Government Agency				
-------------------------	--	--	--	--

Research Entity				
-----------------	--	--	--	--

Other Project / System	Educational Institutions	No		PII
------------------------	--------------------------	----	--	-----

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: * All systems and applications that provide data to Hines ITC LAN can be found in Tab 8, Additional Comments.

Does the system gather information from an individual? Yes

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

if yes, please check all that apply: Drug/Alcohol Counseling Mental Health HIV Research Sickle Cell Other (Please Explain)

Describe process for authorizing access to this data.
Answer:

What is the procedure you reference for the release of information?

Applicants are also required to complete form 21-4242 - authorization and Consent to Release Information to the Department of Veterans Affairs (VA). All VBA benefit forms are located at <http://www.vba.va.gov/pubs/forms1.htm>. The VBA toll free number for benefits is 1-800-827-1000. 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

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. VBA has emplaced strict control measures to prevent the inadvertent or deliberate release of information to non-authorized personnel.



(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 collected primarily on defined forms and entered to specific fields of database records. The required veteran's data is stored within the databases, which support the individual claim or claims the veteran has been granted. The LAN accesses these databases to retrieve the data.

How is data checked for completeness?

Answer: Data are checked by system audits, manual verifications and annual questionnaires through automated veteran letters from the BDN system. These letters ask specific questions for verification based on the existing entitlement or benefit that the veteran is receiving. For example, data such as monthly rates of compensation and pension are updated on an annual basis, other data is updated as a result of returned mail, or returned direct deposits, or through contact with claimants after a significant event affecting their entitlement or benefit.

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

Answer: The veterans data are validated by computer matches and verifications, by system audits, also matched with Social Security Administration (SSN verification); other data are updated as a result of returned mail (incorrect address), returned direct deposits, or through contact with claimants after events that may impact their existing entitlement.

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

Answer: All data are matched against supporting claim documentation submitted by the veteran, widow or dependent. Prior to any award or entitlement authorization(s) by the VBA, the veteran record is manually reviewed and data are validated to ensure correct entitlement has been authorized. The data are also verified by computer database comparisons and system audits.

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

Answer:

(FY 09) PIA: Retention & Disposal

What is the data retention period?

Answer: The data retention period for VBA data is contained in RCS VBA-1, Part I, Item Number 08-065.000 and subparagraphs, which state "Destroy files data in accordance with system design." All active and terminated veterans records are retained indefinitely; therefore, there are no procedures for eliminating data.

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

Answer: Data on active records is changeable. Prior copies of active records and their changed values are also retained. Additional backup copies of all data is stored in an off-site location indefinitely.

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

Answer: The veterans records are not eliminated but are stored either on tape or disk indefinitely. The VA has detailed retention requirements, however, there is little reference to retention requirements for electronic records. The current working practice is to retain the electronic patient/veteran record for 75 years after the last episode of patient care or any benefit activity for that veteran. At the present time, this project retains all images.

Where are these procedures documented?

Answer: The procedures are part of the daily operations of the BDN payment system. 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.

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:

(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:

Answer:

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 include ke

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 |
| <input checked="" type="checkbox"/> Data Disclosure | <input checked="" type="checkbox"/> Theft of Data |

-
- Data Disclosure
 - Data Integrity Loss
 - Denial of Service Attacks
 - Earthquakes
 - Eavesdropping/Interception
 - Fire (False Alarm, Major, and Minor)
 - Flooding/Water Damage

-
- 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:

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.

Hines ITC LAN Application Summary

Automated Folder Processing System (AFPS)

Automates various file maintenance projects (XCR, NOD, CH30, CER retirement projects, processing system folder relocation (REL) and sequence checking) for inactive folders located at the Regional Offices (ROs).

Automated Medical Information Exchange II (AMIE II)

AMIE II allows VA Medical Center staff full read access to the Information Exchange II BDN system for veteran eligibility inquiries while VA RO staffs have electronic access to medical supporting data and streamlined logon capability with VHA Veterans Health Information Systems & Technology Architecture (VistA) systems.

Committee on Waivers and Compromises (COWC)

Provides a tracking system for requests for waivers of debt through the regional office waiver process.

Common Security User Manager (CSUM)

A Microsoft Windows-based client/server application that VBA Security Officers and Information Resources Management (IRM) personnel use for granting security access to applications and sensitive file processing.

Compensation and Pension (C&P) Record Interchange (CAPRI)

The CAPRI software acts as a bridge between VBA and VHA information systems. It assists VBA Rating Specialists building the rating decision documentation through online access to medical data. In addition to using established mechanisms to ensure only authorized access to medical data, CAPRI adds a level of security by allowing VBA users read but not alter electronic medical records by integrating highly detailed Compensation and Pension Rating examination results into the veterans' medical records.

Control of Veterans Records (COVERS)

A Microsoft Windows-based client/server application using bar code technology to support RO and RMC folder activity including requests, mail, search, and external transfer. The initial release applies to claims and Notice of Disagreement (NOD) folders only.

Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)

Corporate WINRS – a comprehensive Vocational Rehabilitation and Employment (VR&E) case management system maintains complete case histories, generates forms and letters, controls authorizations and payments on behalf of participants, and assists in scheduling and tracking appointments. Corporate WINRS replaced the old WINRS application and includes additional functionality. This new application has been migrated to the VBA Corporate environment and the shared corporate database and VBA's three-tier architecture.

Fiduciary Beneficiary System (FBS)

Provides an on-line method for input and retrieval of system maintenance of incompetent veteran cases.

Hearing Officer Letters and Reports System (HOLAR)

Maintains Hearing Officer schedules and data and permits automatic letter and report generation. Incorporates case reporting functionality, ad hoc reporting capabilities, and quality review for work measurement statistics.

Personal Computer Generated Letters (PCGL)

Provides letter generation capabilities to Veterans Service Centers (C&P, EDU), LGY, and ORM (Office of Resource Management) using PCs and accessing BDN data.

Personnel Information Exchange System (PIES)

A client/server application designed to improve the quality and timeliness of requesting veteran information from out-

Management) using PCs and accessing BDN data.

Personnel Information Exchange System (PIES)

A client/server application designed to improve the quality and timeliness of requesting veteran information from other agencies. Information gained from these requests is used to process claims for compensation, pension, education and loans. These improvements are achieved by automating and standardizing the data requests, improved routine request tracking, standard output generation processes, and process metrics involved with claims development.

Rating Board Automation 2000 (RBA 2000)

RBA2000 is the replacement system for the RBA application in use nationwide to support the preparation of disability decisions. RBA2000 is integrated with the Veterans Services Network (VETSNET) specifications for award process data storage formats and will provide improved support for the creation of text documents needed to document rating decisions. Future capabilities will include direct transfer of award data from RBA2000 to the BDN. RBA2000 will continue the collection of claims data to support both information and budgetary requirements.

SHARE

A Microsoft Windows-based client/server application that allows regional office employees to inquire against legacy information such as BIRLS, C&P, Payment History, and other information from other agencies (e.g. Social Security Administration [SSA]). This application is the starting point of MAP-D.

State Benefits Reference System

A system of references for all the veterans' benefits programs in each state. In addition to describing benefits and criteria, the references provide instructions for VSRs to follow in issuing certifications to veterans regarding information on VA records. Information is also provided on VA facilities, as well as certain state and local resources.

Training and Performance Support System (TPSS)

A family of Computer Based Training (CBT) programs that combine interactive CBT and electronic support with self-cooperative learning events. The training focus is subject matter associated with a job. A job will be typically covered by a module containing one or more lessons. Modules have been fielded for the Compensation and Pension Service. Variations of the concept have also been fielded in the Insurance and Loan Guaranty services. Modules are tested for training effectiveness and tests are validated.

Veterans Appeals Control and Locator System (VACOLS)

Allows RO personnel to view, update, and track the status of appeals cases submitted to the Board of Veterans' Appeals (BVA). It also permits initiation of pre-programmed queries, such as "Advance Call-Ups for Specified Months," "Outstanding Call-Ups," "Remands by RO," "Cases Transferred to RO," and "Advance Cases Pending Call-Ups." The system allows all adjudicators at each RO to generate and print reports locally.

Veterans On-line Applications (VONAPP)

Internet application that allows veterans to complete and submit VA forms: 21-526, Veterans Application for Compensation and/or Pension; 28-1900, Disabled Veterans Application for Vocational Rehabilitation; and 22-1990, Application for Education Benefits. The ROs access the server through an admin module to download and print the submitted forms for review/action.

Web Automated Reference Materials System (WARMS)

A Web-based application created for use by the public Reference Materials System and VBA personnel when not at a workstation. The content mirrors the ARMS application.

g system folder

or veteran eligibility
n capability within the

s.

ources Management

ating Specialists in
g established
owing VBA users to
n Rating examination

!MC folder activities,
e of Disagreement

agement system –
s on behalf of the
ld WINRS application
environment and uses

ses.

corporates centralized
cs.

ice of Resource

nation from outside

nation from outside
ion, education, burial,
mproved routing,
velopment.

ation of disability rating
award processing and
document rating
BA2000 will continue

against legacy
social Security

g benefits and eligibility
arding information in
i.

upport with small group
typically covered in a
ion Service.
ules are tested for

if Veterans' Appeals
l Months," "Outstanding
The system allows

tion for Compensation
Application for
submitted forms for

nel when not on

(FY 09) PIA: Final Signatures

Facility Name: Hines 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: 02/27/2009

OMB Unique Project Identifier 029-00-02-00-01-1120-00

Project Name REGION 5> VBA> HINES ITC> LAN