

Welcome to the PIA for FY 2011!

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.

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://vawww.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 VA Directive 6508 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 Directive 6508.
- 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 Directive 6508 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 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 and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

Macros Must Be Enabled on This Form

Microsoft Office 2003: To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable All Macros; 2) Click OK

Final Signatures

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the MA Business Center and the customer has indicated that the information is all that is necessary to submit a request.

(FY 2011) PIA: System Identificatio

Program or System Name:

OMB Unique System/Application/Program Identifi

Description of System/ Application/ Program:

Facility Name:

Title:

Privacy Officer:

Information Security Officer:

System Owner/ Chief Information Officer:

Information Owner:

Other Titles:

Person Completing Document:

Other Titles:

Services: (MM/YYYY)

Date Approval To Operate Expires:

program or system:

What is the expected number of individuals that
Program is at:

The approximate date (MM/YYYY) the system
will be operational (if in the Design or
Development stage), or the approximate number

Is there an authorized change control process
which documents any changes to existing

If No, please explain:

Has a PIA been completed within the last three
years?

Date of Report (MM/YYYY):

continue to the next TAB and complete the

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?

2. System identification/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?

If there is no Personally Identifiable Information

Or

Region 5 > VBA > St Paul Region > VARO Wilmington > LAN

ifier (AKA:UPID #) 029-00-02-00-01-1120-0

The Regional Office (RO) Local Area Network (LAN) serves as default responsitory for incidental data used vocational rehabilitation and employment, insurance, and loan guaranty benefits to veterans. Information stored also stored also includes data used for various administrative functions. The systems provides RO employees local access to file Information stored also includes data used for various administrative functions. The system provides RO including email.

applications, including email.

Wilmington Regional Office

Name:	Phone:
Janet Hardt	215-842-2000 x2649
Genea Morris	215-842-2000 x4814
Kevin Causley	202-461-9170
Thomas M. Lastowka	215-842-2000 x3001
Mary D. Barley	202-461-9175
Janet Hardt	215-842-2000 x2649

08/13/2008

08/21/2011

Title 38 of the United States Code

Approx. 1,000 - 5,000

Operations/Maintenance

Aug-11

Yes

Yes

06/08/2011

the system sinc

/program collecting PII data from Federal employees, contractors, or others performing wc

2. System Identification Information on the basis of name, unique identifier, symbol, or otl

rogram retrieve information on the basis of name, unique identifier, symbol, or otl

rogram collect, store or disseminat

rogram collect, store or dissem

Email:

janet.hardt@va.gov
genea.morris@va.gov
kevin.causley@va.gov
thomas.lastowka@va.gov
mary.barley@va.gov
janet.hardt@va.gov

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.

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

1. All System of Record Identifier(s) (number):
2. Name of the System of Records:

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

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

Does the System of Records Notice require modification or updating?

Is PII collected by paper methods?

Is PII collected by verbal methods?

Is PII collected by automated methods?

Is a Privacy notice provided?

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

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

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

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

Yes

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

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 Award 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)

<http://www.va.gov/oit/cio/foia/Privacy/SystemsOfRecords>

Yes

No

(Please Select Yes/No)

Yes

Yes

No

Yes

Yes

Yes

Yes

Yes

(FY 2011) 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?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	Benefits	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Benefits	All	All
Service Information	ALL	Benefits	All	All
Medical Information	ALL	Benefits	All	All
Criminal Record Information	ALL	Benefits	All	All
Guardian Information	ALL	Benefits	All	All
Education Information	ALL	Benefits	All	All
Benefit Information	ALL	Benefits	All	All
Other (Explain)	ALL	Benefits	All	All

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	Veteran	Voluntary	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	No	Veteran	Voluntary	

Medical Information	Yes	Veteran	Voluntary
Criminal Record Information	Yes	Veteran	Voluntary
Guardian Information	Yes	Veteran	Voluntary
Education Information	Yes	Veteran	Voluntary
Benefit Information	Yes	Veteran	Voluntary
Other (Explain)			
Other (Explain)			
Other (Explain)			

(FY 2011) 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	Veteran's Health Administration/ National Cemetery Administration	Yes	<p>WebHINQ enables VHA to retrieve data from the corporate database and BIRLS. WebHINQ retrieves 4 pieces of data when the record is stored in the corporate database . When available, the following will be retrieved for each SC disability: The affected extremity The original effective date of the disability rating and the current (most recent) date the rating was changed. In addition, the Effective Date of combined SC Evaluation is provided. CAPRI enables data flow between VBA and VHA.</p>	Both PII & PHI
Other Veteran Organization	Veteran Service Organizations	Yes	<p>Co-located Veterans Service Organizations (VSOs)-Co located Veterans Service Organizations at VBA regional regional offices have been given on-line read only access to BDN, BDN Shell, Covers, Share, State Benefits</p>	Both PII & PHI

Reference Systems, VACOLS, Virtual VA, Advisory, WARMS and MAP'D. The co-located VSOs have direct access to veteran data securely through LAN. This access is authorized by VA regulations. The organization requests access and the standard VA logon and password security requirements that are applicable to VA employees are followed. Remote Veteran Service Organizations have been on-line read only access to SHARE, and MAP'D. The remote VSOs access veteran data securely through VA's Virtual Private Network. On-line access is real time and may be accessed by County/State/National Service Organizations at any time. This access is authorized by VA regulations. The County/State/National Service Organization requests on-line access for its representatives. The organization requests access and the standard VA logon and password security requirements that are applicable to VA employees are followed.

Other Federal Government Agency

No

State Government Agency

No

5. Data Sharing & Access

Local Government Agency		No		
Research Entity		No		
Other Project / System	VBA Corporate database and the Benefits Delivery Network database	Yes	Data in the VBA Corporate database and the Benefits Delivery Network database are accessed primarily to support the applications running on the LAN.	Both PII & PHI
Other Project / System		No		
Other Project / System		No		

(FY 2011) PIA: Access to Records

Does the system gather information from another system?

Please enter the name of the system:

Per responses in Tab 4, does the system gather information from an individual?

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?

(FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?

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:

Users are granted individual levels levels of authority privileges to view or process veterans claim\ information. The access levels are provided through strict controls and passwords assigned to individual end-users. CSUM is the

application responsible for performing this task. Reports are for a veteran with any level of sensitivity restriction. Creation of individual user Ids requires a written request from a Requesting Official with approval from the Director and/or Information Security Officer, depending upon the level of access requested.

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

VA Directive 6500, M20-4
Part II, VBA IRM Handbook
5.00.02HB2 and M20-4, Part II,
VBA IRM Handbook
5.00.02HB4

VA Directive 6500, M20-4,
Part II, VBA IRM Handbook
5.00.02HB2 and M20-4, Part II,
VBA IRM Handbook
5.00.02HB4.

VA Directive 6500, M20-4,
Part II, VBA IRM Handbook
5.00.02HB2 and M20-4,
Part II, VBA IRM Handbook
5.00.02HB4

No

Yes

Yes

No



(FY 2011) PIA: Program Level Questions

Does this PIA form 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: All data that is collected is done through the use of forms. The forms are limited to specific fields required by the data base. The data is collected from the forms and then input into the appropriate field. The system does not allow for erroneous data elements.

How is data checked for completeness?

Answer: There are various checks and balance throughout the data collection and input process. All users are assigned specific permissions with the systems. One user has the authority to establish information and another user has the authority to authorize the information. During the authorization process the user verifies the completeness for data.

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

Answer: The data is constantly kept current through the utilization of veteran outreach. The Regional Office staff has a yearly program where data that needs updating is verified by the veteran.

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

Answer: The minor applications that run on this system all have built in alerts that are flagged if anyone tries to access any veterans data outside of their individual authorization permissions. These alert messages are compiled into daily reports that are provided to the information Security Office and are reviewed to verify what incidents took place. Depending on the degree of error, corrective action is followed through. All access can be tracked to individual end-users to identify any unauthorized attempts to access veterans' records. Users also sign a Rules of Behavior prior to system access and annually thereafter. VA also utilizes encryption technology to ensure the authenticity of transmitted data.

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

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Data retention policies and procedures are being updated. The updates will be completed by the department and Federal Government guidance.

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

Answer: For benefits purposes.

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

Answer: In general, support systems retain information until that work in progress is completed and data is committed to master systems and records. The master systems retain data in a permanent basis (beyond the actual death of the veteran). If incidental data is maintained in a user's personal folder on the network, the data is deleted when the employment is terminated.

Where are these procedures documented?

Answer: VA Handbook 6300.5 and Records Control Schedule (RCS) VBA-1, Part 1, Section 8, available online at <http://www.warms.vba.va.gov/admin23/part1/sec08.co> and the Systems of Record 58VA21/22 and 38VA23

How are data retention procedures enforced?

Answer: Management oversight and review enforces data retention policies.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

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

Answer: Yes

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

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

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

Answer: No

(FY 2011) 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? Yes

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

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

Answer:

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: An annual assessment of security controls is currently conducted to ensure that IT security requirements are being met.

This strategy implements federal Regulations, VA IT security policy and guidelines and industry best practices.

Security is implemented with VA's guidelines, policies and mandates.

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"/> Data Disclosure | <input checked="" type="checkbox"/> Hardware Failure |
| <input checked="" type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Data Integrity Loss | <input checked="" type="checkbox"/> Identity Theft |
| <input checked="" type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Denial of Service Attacks | <input checked="" type="checkbox"/> Malicious Code |
| <input checked="" type="checkbox"/> Bomb Threats | <input checked="" type="checkbox"/> Earthquakes | <input checked="" type="checkbox"/> Power Loss |
| <input checked="" type="checkbox"/> Burglary/Break In/Robbery | <input checked="" type="checkbox"/> Eavesdropping/Interception | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Cold/Frost/Snow | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) | <input checked="" type="checkbox"/> Storms/Hurricanes |
| <input checked="" type="checkbox"/> Communications Loss | <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input checked="" type="checkbox"/> Substance Abuse |

~~Communications Risk~~

- Computer Intrusion
- Computer Misuse
- Data Destruction

Answer: (Other Risks)

- Fire (False Alarm, Major, and Minor)
- Flooding/Water Damage
- Fraud/Embezzlement

~~Substance Abuse~~

- Theft of Assets
- Theft of Data
- Vandalism/Rioting

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

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

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: 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 information stored on VBA/Region Five LANs are secured per VA security standards

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

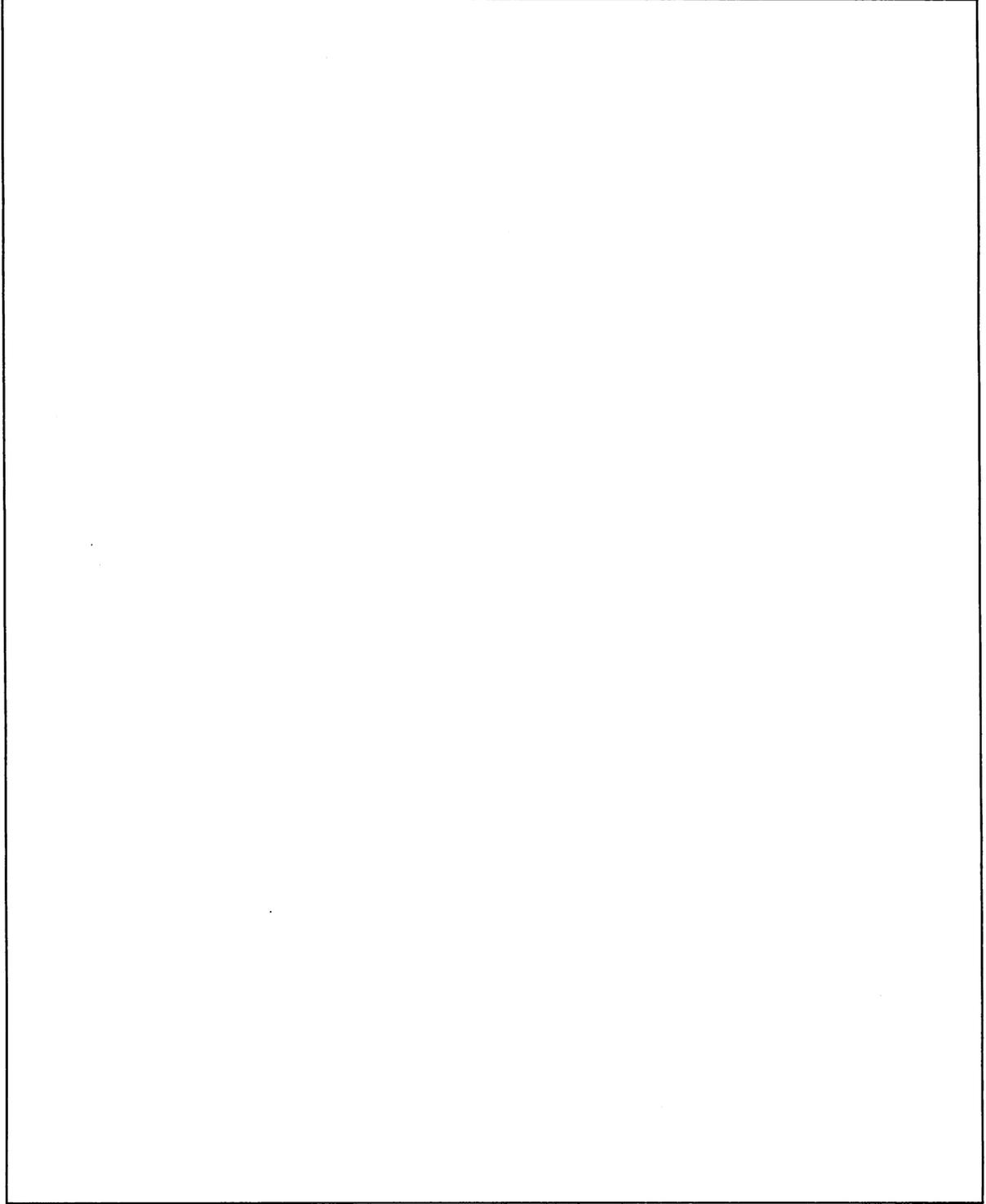
The controls are being considered for the project based on the selections from the previous assessments?

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 2011) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.



(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	x Automated Medical Information Exchange II (AIME II)
Appraisal System	x Benefits Delivery Network (BDN)	x Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	x Automated Standardized Performace Elements Nationwide (ASPEN)
x Awards	x Common Security User Manager (CSUM)	x Centralized Accounts Receivable System (CARS)
x Awards	x Compensation and Pension (C&P)	x Committee on Waivers and Compromises (COWC)
Baker System	x Control of Veterans Records (COVERS)	x Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	x Control of Veterans Records (COVERS)	x Compensation & Pension Training Website
x BDN Payment History	x Control of Veterans Records (COVERS)	x Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
x BIRLS	Courseware Delivery System (CDS)	x Distribution of Operational Resources (DOOR)
x C&P Payment System	Dental Records Manager	x Educational Assistance for Members of the Selected Reserve Program CH 1606
x C&P Training Website	Education Training Website	x Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	x Enterprise Wireless Messaging System (Blackberry)
x Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
Data Warehouse	x Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	x Inquiry Routing Information System (IRIS)
FOCAS	x Fiduciary Beneficiary System (FBS)	x Modern Awards Process Development (MAP-D)
Inforce	x Fiduciary STAR Case Review	x Personnel and Accounting Integrated Data and Fee Basis (PAID)
x INS - BIRLS	x Financial and Accounting System (FAS)	x Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	x Personnel Information Exchange System (PIES)
Insurance Self Service	x Inventory Management System (IMS)	x Personnel Information Exchange System (PIES)
x LGY Home Loans	x LGY Centralized Fax System	x Post Vietnam Era educational Program (VEAP) CH 32
x LGY Processing	x Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	x Loan Guaranty Training Website	Reinstatement Entitelment Program for Survivors (REAPS)
x Montgomery GI Bill	Master Veterans Record (MVR)	x Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Asisstant	x Service Member Records Tracking System
Omnicell	National Silent Monitoring (NSM)	x Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	x Systematic Technical Accuracy Review (STAR)
RAI/MDS	x Rating Board Automation 2000 (RBA2000)	x Training and Performance Support System (TPSS)
x Right Now Web	x Rating Board Automation 2000 (RBA2000)	x VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	x Rating Board Automation 2000 (RBA2000)	x VA Reserve Educational Assistance Program
Script Pro	x Records Locator System	x Veterans Appeals Control and Locator System (VACOLS)
x SHARE	Review of Quality (ROQ)	x Veterans Assistance Discharge System (VADS)
x SHARE	Search Participant Profile (SPP)	x Veterans Exam Request Info System (VERIS)
x SHARE	Spinal Bifida Program Ch 18	x Veterans Service Representative (VSR) Advisor
Sidexis	x State Benefits Reference System	x Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	x State of Case/Supplemental (SOC/SSOC)	x Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

- | | | |
|---|--|---|
| VBA Data Warehouse | Telecare Record Manager | <input type="checkbox"/> Web Automated Folder Processing System (WAFPS) |
| <input checked="" type="checkbox"/> VBA Training Academy | <input checked="" type="checkbox"/> VBA Enterprise Messaging System | <input checked="" type="checkbox"/> Web Automated Reference Material System (WARMS) |
| Veterans Canteen Web
VIC | <input checked="" type="checkbox"/> Veterans On-Line Applications (VONAPP) | <input checked="" type="checkbox"/> Web Automated Verification of Enrollment |
| <input checked="" type="checkbox"/> VR&E Training Website | <input checked="" type="checkbox"/> Veterans Service Network (VETSNET) | <input checked="" type="checkbox"/> Web-Enabled Approval Management System (WEAMS) |
| <input checked="" type="checkbox"/> Web LGY | Web Electronic Lender Identification | <input checked="" type="checkbox"/> Web Service Medical Records (WebSMR) |
| | | <input checked="" type="checkbox"/> Work Study Management System (WSMS) |

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this min or application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
x CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	Health Level Seven	Master Patient Index VistA
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
x PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	Progress Notes	Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Verified Components - DSSI
VBECs	VistALink Security	Text Integration Utilities	Vendor - Document Storage Sys
VDEF	Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistALink		Voluntary Timekeeping	Voluntary Timekeeping National

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

(FY 2011) PIA: Minor Applications

Which of these are sub-components of your system?

1184 Web	ENDSOFT	RAFT
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS

(FY 2011) PIA: Final Signatures

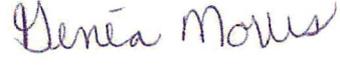
Facility Name: Region 5 > VBA > St Paul Region > VARO Wilmington > LAN

Title:	Name:	Phone:	Email:
--------	-------	--------	--------

		215-842-2000	
Privacy Officer:	Janet Hardt	x2649	janet.hardt@va.gov

 Digital Signature Block

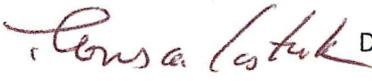
		215-842-2000	
Information Security Officer:	Genea Morris	x4814	genea.morris@va.gov

 Digital Signature Block

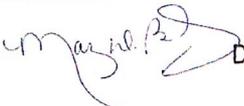
System Owner/ Chief Information Officer:	Kevin Causley	202-461-9170	kevin.causley@va.gov
--	---------------	--------------	----------------------

 Digital Signature Block
Digitally signed by Kevin Causley
DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=Internal Staff, 0.9.2342.19200300.100.1.1=kevin.causley@va.gov, cn=Kevin Causley
Date: 2011.06.22 08:16:10 -04'00'

Information Owner:	Thomas M. Lastowka	215-381-3100	thomas.lastowka@va.gov
--------------------	--------------------	--------------	------------------------

 Digital Signature Block

Other Titles:	Mary D. Barley	202-461-9175	mary.barley@va.gov
---------------	----------------	--------------	--------------------

 Digital Signature Block
Digitally signed by Mary Barley
DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=Internal Staff, 0.9.2342.19200300.100.1.1=mary.barley@va.gov, cn=Mary Barley
Date: 2011.06.22 08:16:53 -04'00'

Date of Report: 6/8/11

OMB Unique Project Identifier 0

Region 5 > VBA > St Paul Region >

Project Name VARO Wilmington > LAN