

### **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](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 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, 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**

**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 VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

### **Privacy Impact Assessment Uploaded into SMART**

Privacy Impact Assessments should be uploaded into C&A section of SMART.

## (FY 2011) PIA: System Identification

Program or System Name: Region 5 > VBA > St. Petersburg Region > VARO Washington > LAN  
OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

The Regional Office (RO) Local Area Network (LAN) serves as the default repository for incidental data used and processed by various VBA Major Applications. 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. The system provides RO employees local access to file and print

Description of System/ Application/ Program: sharing services on the LAN. It also provides client access to various applications, including email.

Facility Name: Washington Regional Office

Title:	Name:	Phone:	Email:
Privacy Officer:	Risa Washington	202-530-9262	<a href="mailto:risa.washington@va.gov">risa.washington@va.gov</a>
Information Security Officer:	Michael A. Young	202-530-9311	<a href="mailto:Michael.Young8@va.gov">Michael.Young8@va.gov</a>
System Owner:	Kevin Causley	202-461-9170	<a href="mailto:Kevin.Causley@va.gov">Kevin.Causley@va.gov</a>
Facility Chief Information Officer:	Leonard Ross	202-530-9315	<a href="mailto:Leonard.Ross@va.gov">Leonard.Ross@va.gov</a>
Person Completing Document:	Risa Washington	202-530-9262	<a href="mailto:risa.washington@va.gov">risa.washington@va.gov</a>
C&A Project Officer	Mary Barley	202-461-9175	<a href="mailto:Mary.Barley@va.gov">Mary.Barley@va.gov</a>

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 06/2010

Date Approval To Operate Expires: 08/2011

What specific legal authorities authorize this program or system: Title 38 of the United States code

What is the expected number of individuals that will have their PII stored in this system: aprox. 5,000

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. 10 years

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

If No, please explain:

Has a PIA been completed within the last three years? Yes

Date of Report (MM/YYYY): 05/2011

**Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.**

- 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?

**If there is no Personally Identifiable Information on your system, please complete TAB 2 & TAB 12. ( See Comment for Definition of PII)**

## (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.

Yes

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

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

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

LGY Home Condominium and Manufactured home loan applicant records- VA, compation, penison, education, Rehabilitation Records-VA, Veterans and Beneficiaries Identfication Records Location Subsystem- VA. 36VA00 Veterans and Armed Forces Personnel Untied States Government Life Insurance Records-VA 53VA00 Vertans Mortgage Life Insurance-VA, Veterans and Beneficiaries Identification and Records Location (BIRLS) and Compensation, Pension, Education, and Rehabilitation (civers BDN and Corporate databases).

2. Name of the System of Records:

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](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

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 2011) PIA: Notice**

Please fill in each column for the data types selected.

<b>Data Type</b>	<b>Collection Method</b>	<b>What will the subjects be told about the information collection?</b>	<b>How is this message conveyed to them?</b>	<b>How is a privacy notice provided?</b>
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Paper	Information used to process their benefits is considered confidential and only release as applicable by law.	Verbal & Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper	Information used to process their benefits is considered confidential and only release as applicable by law.	Verbal & Written	Written
Service Information	Paper	Information used to process their benefits is considered confidential and only release as applicable by law.	Verbal & Written	Written
Medical Information	Paper & Electronic	Information used to process their benefits is considered confidential and only release as applicable by law.	Verbal & Written	Written
Criminal Record Information	ALL	Information used to process their benefits is considered confidential and only release as applicable by law.	Verbal & Written	Written
Guardian Information	Paper	Information used to process their benefits is considered confidential and only release as applicable by law.	Verbal & Written	Written
Education Information	Paper	Information used to process their benefits is considered confidential and only release as applicable by law.	Verbal & Written	Written
Benefit Information	Paper	Information used to process their benefits is considered confidential and only release as applicable by law.	Verbal & Written	Written
Other (Explain)		Information used to process their benefits is considered confidential and only release as applicable by law.	Verbal & Written	Written

<b>Data Type</b>	<b>Is Data Type Stored on your system?</b>	<b>Source</b> (If requested, identify the specific file, entity and/or name of agency)	<b>Is data collection Mandatory or Voluntary?</b>	<b>Additional Comments</b>
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Voluntary	
Service Information	Yes	VA Files / Databases (Identify file)	Voluntary	
Medical Information	Yes	VA Files / Databases (Identify file)	Voluntary	
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Voluntary	
Guardian Information	Yes	VA Files / Databases (Identify file)	Voluntary	
Education Information	Yes	VA Files / Databases (Identify file)	Voluntary	
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	
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?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VHA, NCA	Yes	Benefits	Both PII & PHI	VA Handbook 6500, M20-4 II and III
Other Veteran Organization	VSO	Yes	Benefits	Both PII & PHI	VA Handbook 6500, M20-4 II and III
Other Federal Government Agency	Social Security Admin	No	Benefits	Both PII & PHI	VA Handbook 6500, M20-4 II and III
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System	Attorney	No	Veteran file	Both PII & PHI	VA Handbook 6500, M20-4 II and III
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system? Yes  
 Please enter the name of the system: Social Security Adim.  
 Per responses in Tab 4, 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 N/A

Is there a contingency plan in place to process information when the system is down? No

(FY 2011) 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  
 Answer:

## (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: 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: There is an automatic system that checks data entry for completeness and continual correspondence

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

Answer: The facility collect veteran's information on continual bases via electronic, verbal, and written corrpondance.

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

Answer: Their information is matched up against the supporting claims submitted by the veteran and/or family. SSN verified through the SSA

*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: indefinite

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

Answer: Veteran or family members might require data for historic and or benefits information at any time.

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

Answer: All active and terminated Veteran's records are retained indefinitely. Any and all eletronic media are sanitized in accordance with VA Handbook 6500.1. Procedure used are in accordance with VA Directive 6300

Where are these procedures documented?

Answer: The procedures are documented on a Records Control Schedule

How are data retention procedures enforced?

Answer: The Records Mangement Officer ensures that records are disposed of per the Records Control Schedule

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:

## (FY 2011) 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: N/A

## (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: FISMA assessment is performed annually and C&A process is performed every 3 years to meet the IT security Requirements and procedures.

Security controls are in place in accordance with NIST Guidelines and industry best practices.

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

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

Answer: (Other Risks)

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

- |  |   |   |
|--|---|---|
| <input checked="" type="checkbox"/> Access Control                                       | <input checked="" type="checkbox"/> Contingency Planning              | <input checked="" type="checkbox"/> Personnel Security                    |
| <input checked="" type="checkbox"/> Audit and Accountability                             | <input checked="" type="checkbox"/> Identification and Authentication | <input checked="" type="checkbox"/> Physical and Environmental Protection |
| <input checked="" type="checkbox"/> Awareness and Training                               | <input checked="" type="checkbox"/> Incident Response                 | <input checked="" type="checkbox"/> Risk Management                       |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments |   |   |
| <input checked="" type="checkbox"/> Configuration Management                             | <input checked="" type="checkbox"/> 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: An annual assessment of security controls is currently conducted and will continue to be conducted to ensure that IT security requirements are being met. This strategy implements Federal Regulations, VA IT security policy and guidelines, NIST Guidelines and industry best practices. Security is implemented in compliance with VA's guidelines, policies, and mandates.

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

*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

<b>Which of these are sub-components of your system?</b>
--

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)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	x Automated Standardized Performance 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)	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)	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	Educational Assistance for Members of the Selected Reserve Program CH 1606
x C&P Training Website	x Education Training Website	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	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	x Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	x Modern Awards Process Development (MAP-D)
Inforce	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	Inventory Management System (IMS)	x Personnel Information Exchange System (PIES)
x LGY Home Loans	LGY Centralized Fax System	x Post Vietnam Era educational Program (VEAP) CH 32
x LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitlement Program for Survivors (REAPS)
x Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Assistant	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)	Training and Performance Support System (TPSS)
Right Now Web	x Rating Board Automation 2000 (RBA2000)	VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	x Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program

Script Pro	Records Locator System	x Veterans Appeals Control and Locator System (VACOLS)
x SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
x SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
x SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sidexis	State Benefits Reference System	x Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	x State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
VBA Data Warehouse	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	x Veterans Service Network (VETSNET)	x Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	x Web Service Medical Records (WebSMR)
x Web LGY		x 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	x 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
x HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
x 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
Administrative Data Repository (ADR)	ePROMISE	Remedy Application
ADT	EYECAP	SAN
x Agent Cashier	Financial and Accounting System (FAS)	Scanning Exam and Evaluation System
Air Fortress	Financial Management System (FMS)	Sentillion
Auto Instrument	Genesys	Stellant
Automated Access Request	Health Summary Contingency	Stentor
x BDN 301	ICB	Tracking Continuing Education
Bed Board Management System	KOWA	Traumatic Brain Injury
Cardiff Teleform	Lynx Duress Alarm	VA Conference Room Registration
Cardiology Systems (stand alone servers from the network)	MHTP	VAMedSafe
CHECKPOINT	Microsoft Active Directory	VBA Data Warehouse
Clinical Data Repository/Health Data Repository	Microsoft Exchange E-mail System	VHAHUNAPP1
Combat Veteran Outreach	Military/Vet Eye Injury Registry	VHAHUNFPC1
Committee on Waiver and Compromises	Mumps AudioFAX	VISTA RAD
CP&E	NOAHLINK	Whiteboard
Crystal Reports Enterprise	Omnicell	
Data Innovations	Onvicord (VLOG)	
DELIVEREX	Optifill	
DICTATION-Power Scribe	P2000 ROBOT	
DRM Plus	PACS database	
DSIT	Personal Computer Generated Letters	
DSS Quadramed	PICIS OR	
EDS Whiteboard (AVJED)	PIV Systems	
EKG System	Q-Matic	
Embedded Fragment Registry	QMSI Prescription Processing	

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: Final Signatures

Facility Name: Region 5 > VBA > St. Petersburg Region > VARO Washington > LAN

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

Privacy Officer:	Risa Washington	202-530-9262	risa.washington@va.gov
------------------	-----------------	--------------	------------------------

------------------

Information Security Officer:	Michael A. Young	202-530-9311	Michael.Young8@va.gov
-------------------------------	------------------	--------------	-----------------------

------------------

System Owner:	Kevin Causley	202-461-9170	Kevin.Causley@va.gov
---------------	---------------	--------------	----------------------

------------------

C&A Project Officer	Mary Barley	202-461-9175	Mary.Barley@va.gov
---------------------	-------------	--------------	--------------------

------------------

Facility Chief Information Officer:	Leonard Ross	202-530-9315	Leonard.Ross@va.gov
-------------------------------------	--------------	--------------	---------------------

------------------

Date of Report: 5/20/11

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

Project Name Region 5 > VBA > St. Petersburg  
Region > VARO Washington > LAN