

**(FY 2011) PIA: System Identification**

Program or System Name: Region 5 > VBA > St Paul Region > VARO Hartford > LA  
 OMB Unique System / Application / Program Identifier (AKA: UPID #):

The Regional Office(RO) Local Area Network (LAN) ser  
 processed by various VBA Major Applications. This da  
 vocational rehabilitation and employment, insurance,  
 stored also includes data used for various administrat  
 access to file and print sharing services on the LAN. It  
 including email.

Description of System/ Application/ Program:

Facility Name: VARO Hartford

Title:	Name:	Phone:
Privacy Officer:	Leonardo Nunes	860-666-7370
Information Security Officer:	Insuk Yi	860-666-7326
System Owner:	Kevin C. Causley	202-461-9170
C&A Project Officer:	Mary D. Barley	202-461-9175
Person Completing Document:	Insuk Yi/Leonardo Nunes	

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 08/2010

Date Approval To Operate Expires: 08/29/2011

What specific legal authorities authorize this program or system: Title 38 of US Code.

What is the expected number of individuals that will have their PII stored in this system: Approx.  
 30000

Identify what stage the System / Application / Program is at: Operational

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.  
 12 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 questio**

- 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?

**If there is no Personally Identifiable Information on your system, please complete TAB 7 & TAB 12. ( 5**

N

029-00-02-00-01-1120-00

ves as the default repository for incidental data used and  
it is used in granting compensation, pension, education,  
and loan guaranty benefits to veterans. Information  
ive functions. The system provides RO employees local  
: also provides client access to various applications,

**Email:**

leonardo.nunes@va.gov  
insuk.yi@va.gov  
Kevin.Causley@va.gov  
mary.barley@va.gov

ons on this form.

rs, or others performing work for the VA?  
Identify whether PII data?

Identifier, symbol, or other PII data?

(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.

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

58VA21/11

58VA21/22 - Compensation, Pension, Education, and Rehabilitation Records - VA

[http://www.rms.oit.va.gov/SOR\\_Records/58VA21\\_22.asp](http://www.rms.oit.va.gov/SOR_Records/58VA21_22.asp)

---

Yes

---

No

*(Please Select Yes/No)*

Yes

Yes

Yes

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?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	Benefits	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Benefits	All
Service Information	ALL	Benefits	All
Medical Information	ALL	Benefits	All
Criminal Record Information	ALL	Benefits	All
Guardian Information	ALL	Benefits	All
Education Information	ALL	Benefits	All
Benefit Information	ALL	Benefits	All
Other (Explain) Financial, SSA	ALL	Benefits	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?
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

<b>Service Information</b>	<b>Yes</b>	<b>VA Files / Databases (Identify file)</b>	<b>Mandatory</b>
<b>Medical Information</b>	<b>Yes</b>	<b>VA Files / Databases (Identify file)</b>	<b>Mandatory</b>
<b>Criminal Record Information</b>	<b>Yes</b>	<b>State Agency (Identify)</b>	<b>Mandatory</b>
<b>Guardian Information</b>	<b>Yes</b>	<b>State Agency (Identify)</b>	<b>Mandatory</b>
<b>Education Information</b>	<b>Yes</b>	<b>State Agency (Identify)</b>	<b>Mandatory</b>
<b>Benefit Information</b>	<b>Yes</b>	<b>VA Files / Databases (Identify file)</b>	<b>Mandatory</b>
<b>Other (Explain)</b>			
<b>Other (Explain)</b>			
<b>Other (Explain)</b>			

**How is a privacy notice provided?**

All

All

All

All

All

All

All

All

All

---

**Additional Comments**

All - Verbally, written, or automated

**(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	Yes	Medical, benefits, personal information	Both PII & PHI	VA regulations, guidance
Other Veteran Organization	VSO	Yes	Medical, benefits, personal information	Both PII & PHI	VA regulations, guidance
Other Federal Government Agency		No			
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System		No			
Other Project / System		No			
Other Project / System		No			

**(FY 2011) PIA: Access to Records**

Does the system gather information from another system? No

Please enter the name of the system:

Per responses in Tab 4, 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

**(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 this data.

Answer: Users are granted individual 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 created which identify all access attempts both successful and unsuccessful to any information 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



## (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? 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 is checked for completeness by system audits, manual verifications and annual questionnaires through automated veteran letters. These questions for verification based on the existing entitlement or benefit the veteran is receiving. Also, data are updated with each veteran correspondence.

---

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

Answer: Data are updated as a result of returned mail, or returned direct deposits, or through contact with the veteran, beneficiary, or power of attorney. Verifications and system audits are performed.

---

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

Answer: All data are matched against supporting claims documentation submitted by the veteran, widow, or dependent. Certain data such as SSN is verified against Social Security Administration. Prior to any award or entitlement authorization(s) by the VBA, the veteran record is manually reviewed and data validated to ensure entitlement has been approved.

---

*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: Records are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States. Records Control Schedule (RCS) VB-1 provides more general guidance at <http://www.warms.vba.va.gov>. Examples, Claim related microfiche file copies of letter generated by Hines BDC during the running of certain special projects, to be selected by the Pension Service is destroyed by mutilation or shredding 25 years from the date of the letter. Another example is that the Routine claims materials (it is destroyed when 2 years old).

---

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

Answer: to comply with VA Handbook 6300.5 and Records Control Schedule (RCS) VB-1

---

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 on a permanent basis (beyond the actual death of the veteran). If incidental data is maintained in a user's personal folder on the network, that data is deleted from the system when the employment is terminated. Deleting this information is a form of media wiping, which is acceptable because the server is reused within VA. Once the server reaches end of life, the device is physically destroyed.

---

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.doc> 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:

---

### **(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:

---

---

lic? No

---

---

le letters ask specific  
nce.

---

---

rney. Additionally,

---

---

erified with the Social  
ensure correct

---

---

---

---

w/20rcs.html. For  
Compensation and  
m No. 08-002.200)

---

---

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Yes

\_\_\_\_\_

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: 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 checked="" type="checkbox"/> Data Disclosure                       | <input checked="" type="checkbox"/> Hardware Failure |
| <input type="checkbox"/> Chemical/Biological Contamination    | <input type="checkbox"/> Data Integrity Loss                              | <input checked="" type="checkbox"/> Identity Theft   |
| <input type="checkbox"/> Blackmail                            | <input type="checkbox"/> Denial of Service Attacks                        | <input checked="" type="checkbox"/> Malicious Code   |
| <input type="checkbox"/> Bomb Threats                         | <input type="checkbox"/> Earthquakes                                      | <input checked="" type="checkbox"/> Power Loss       |
| <input checked="" type="checkbox"/> Burglary/Break In/Robbery | <input type="checkbox"/> Eavesdropping/Interception                       | <input 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 checked="" type="checkbox"/> Communications Loss       | <input 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 checked="" 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: Reconsidered the collection methods by collecting only necessary data to perform the required duty.

**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 potential impact is low if the loss of confidentiality would be expected to have a minimal 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.

All security controls required for a Federal Information Processing Standard (FIPS) 199 level of moderate as documented in NIST Special Publication 800-53, are implemented or planned for this LAN. Documented security controls can be found in the Facility System Security Plan.

(FY 2011) PIA: VBA Minor Applications

**Which of these are sub-components of your system?**

Access Manager	Automated Sales Reporting (ASR)	x 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 Performance Elements Nationwide (ASPEN)
Awards	x Common Security User Manager (CSUM)	x Centralized Accounts Receivable System (CARS)
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	x 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)	x Financial Management Information System (FMI)
x Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	x 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	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	x Purchase Order Management System (POMS)
x Mobilization	x Loan Guaranty Training Website	x Reinstatement Entitlement Program for Survivors (REAPS)
x Montgomery GI Bill	x Master Veterans Record (MVR)	x Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Assistant	x Service Member Records Tracking System
Omicell	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)
Right Now Web	x Rating Board Automation 2000 (RBA2000)	x VA Online Certification of Enrollment (VA-ONCE)
x 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	x Review of Quality (ROQ)	x Veterans Assistance Discharge System (VADS)
x SHARE	x Search Participant Profile (SPP)	x Veterans Exam Request Info System (VERIS)
x SHARE	x Spinal Bifida Program Ch 18	x 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)

- |   |  |   |
|---|--|---|
| <input checked="" type="checkbox"/> VBA Data Warehouse          | <input checked="" type="checkbox"/> Telecare Record Manager                | <input checked="" 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) |
| <input checked="" type="checkbox"/> Veterans Canteen Web<br>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                                       | Web Service Medical Records (WebSMR)  |
|   |  | 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
x 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
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	x	Remedy Application
ADT		EYECAP		SAN
x Agent Cashier	x	Financial and Accounting System (FAS)		Scanning Exam and Evaluation System
x Air Fortress	x	Financial Management System (FMS)		Sentillion
x Auto Instrument		Genesys		Stellant
x Automated Access Request		Health Summary Contingency		Stentor
x BDN 301		ICB	x	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	x	Microsoft Active Directory	x	VBA Data Warehouse
Clinical Data Repository/Health Data Repository	x	Microsoft Exchange E-mail System		VHAHUNAPP1
Combat Veteran Outreach Committee on Waiver and Compromises		Military/Vet Eye Injury Registry		VHAHUNFPC1
x CP&E		Mumps AudioFAX		VISTA RAD
Crystal Reports Enterprise Data Innovations		NOAHLINK		Whiteboard
		Omnicell		
		Onvicord (VLOG)		

DELIVEREX		Optifill
DICTATION-Power Scribe		P2000 ROBOT
DRM Plus		PACS database
DSIT		Personal Computer Generated
	x	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 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

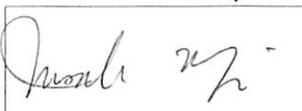
Facility Name: VARO Hartford

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

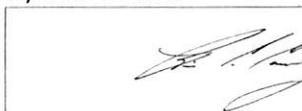
Privacy Officer:	Leonardo Nunes	860-666-7370	leonardo.nunes@va.gov
------------------	----------------	--------------	-----------------------

 Digital Signature Block

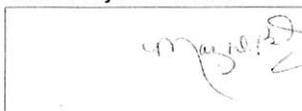
Information Security Officer:	Insuk Yi	860-666-7326	insuk.yi@va.gov
-------------------------------	----------	--------------	-----------------

 Digital Signature Block

System Owner:	Kevin C. 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,  
 dn=Kevin Causley  
 Date: 2011.05.18 10:28:38 -04'00'

C&A Project Officer:	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,  
 dn=Mary Barley  
 Date: 2011.05.18 10:29:33 -04'00'

Date of Report: 5/11/11  
 OMB Unique Project Identifier: 029-00-02-00-01-1120-00  
 Region 5 > VBA > St Paul Region >  
 Project Name: VARO Hartford > LAN