

(FY 2010) PIA: System Identification

Program or System Name: **Region 5 > VBA > St Paul Region > VARO St. Paul > LAN**

OMB Unique System / Application /
Program Identifier (AKA: UPID #): **029-00-02-00-01-1028-00-404-139**

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

Facility Name: St. Paul Regional Office

Title:	Name:	Phone:	Email:
Privacy Officer:	Xavier Williams / Jon Power	612-970-8902	xavier.williams@va.gov
Information Security Officer:	Bryan Steenerson	612-970-5643	jon.power@va.gov
Chief Information Officer:	Pete Kostohryz	612-970-5204	bryan.steenerson@va.gov
Person Completing Document:	Bryan Steenerson / Jon Power	612-970-5220	pete.kostohryz@va.gov
System Owner:	Kevin C. Causley	612-970-5204	bryan.steenerson@va.gov
		202-4619170	kevin.causley@va.gov

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy
Services: (MM/YYYY) 08/2008

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: Storing 1,000 – 5,000 individuals while working on their case files

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. The St. Paul LAN has been in operation since 1992.

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):

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 skip to TAB 12. (See Comment for Definition of PII)

(FY 2010) PIA: System of Records

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

Yes

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

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

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

17VA26, 37VA27, 55VA26, 58VA21/22/28

17VA26 Loan Guaranty Fee Personnel and Program Participant Records-VA.
37VA27 VA Supervised Fiduciary/Beneficiary and General Investigative Records-VA.
55VA26 Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records-VA. 58VA21/22/28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

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

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?

No

Is a Privacy notice provided?

Yes

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

Yes

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

Yes

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

Yes

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

Yes

(FY 2010) 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)				

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	Yes	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 2010) 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	Veteran's Health Administration / National Cemetary Administration	Yes	(1) 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. (2) CAPRI enables data flow between VBA and VHA.	Both PII & PHI	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4
Other Veteran Organization	Veteran Service Organizations	Yes	Co-located Veterans Service Organizations (VSOs) –Co-located Veterans Service Organizations at VBA regional offices have been given on-line read only access to BDN, BDN Shell, Covers, Share, State Benefits 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 Veterans Service Organizations (VSOs) –Remote Veterans Service Organizations have been given on-line read only access to SHARE and MAPD. The remote VSOs access veteran data securely through VA’s Virtual Private Network. On-line access is real time and may be accessed by the County/State/National Service Organization 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.	Both PII & PHI	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4
Other Federal Government Agency		No			
State Government Agency		No			
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	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4
Other Project / System					
Other Project / System					

(FY 2010) 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 2010) 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:

(FY 2010) 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: Per VA Directive 6500, user access is restricted to a need to know basis. The end user access is restricted by the level of authority they require to perform their jobs. The systems include authorization at the application and function level. Users may have inquiry, update (sometimes sub-divided), or verifier authority to different screens.

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

Answer: Most of the major applications that run on the LAN have built in alerts that are flagged if anyone tries to access any veteran data outside of their individual authorization permissions. These alert messages are compiled into daily reports that are provided to the Information Security Officer 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.

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

Answer: Most of the major applications that run on the LAN have built in alerts that are flagged if anyone tries to access any veteran data outside of their individual authorization permissions. These alert messages are compiled into daily reports that are provided to the Information Security Officer 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.

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

Answer:

(FY 2010) 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 end of FY2010. The update will evaluate existing data retention practices against current best practices and 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 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 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.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)

Yes

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

Answer:

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

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

No

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

Answer:

(FY 2010) 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 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.

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

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

Answer: (Other Risks)

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

- | | |
|---|--|
| <input checked="" type="checkbox"/> Risk Management | <input checked="" type="checkbox"/> Audit and Accountability |
|---|--|

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

Answer: (Other Controls)

PIA: PIA Assessment

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

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

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

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

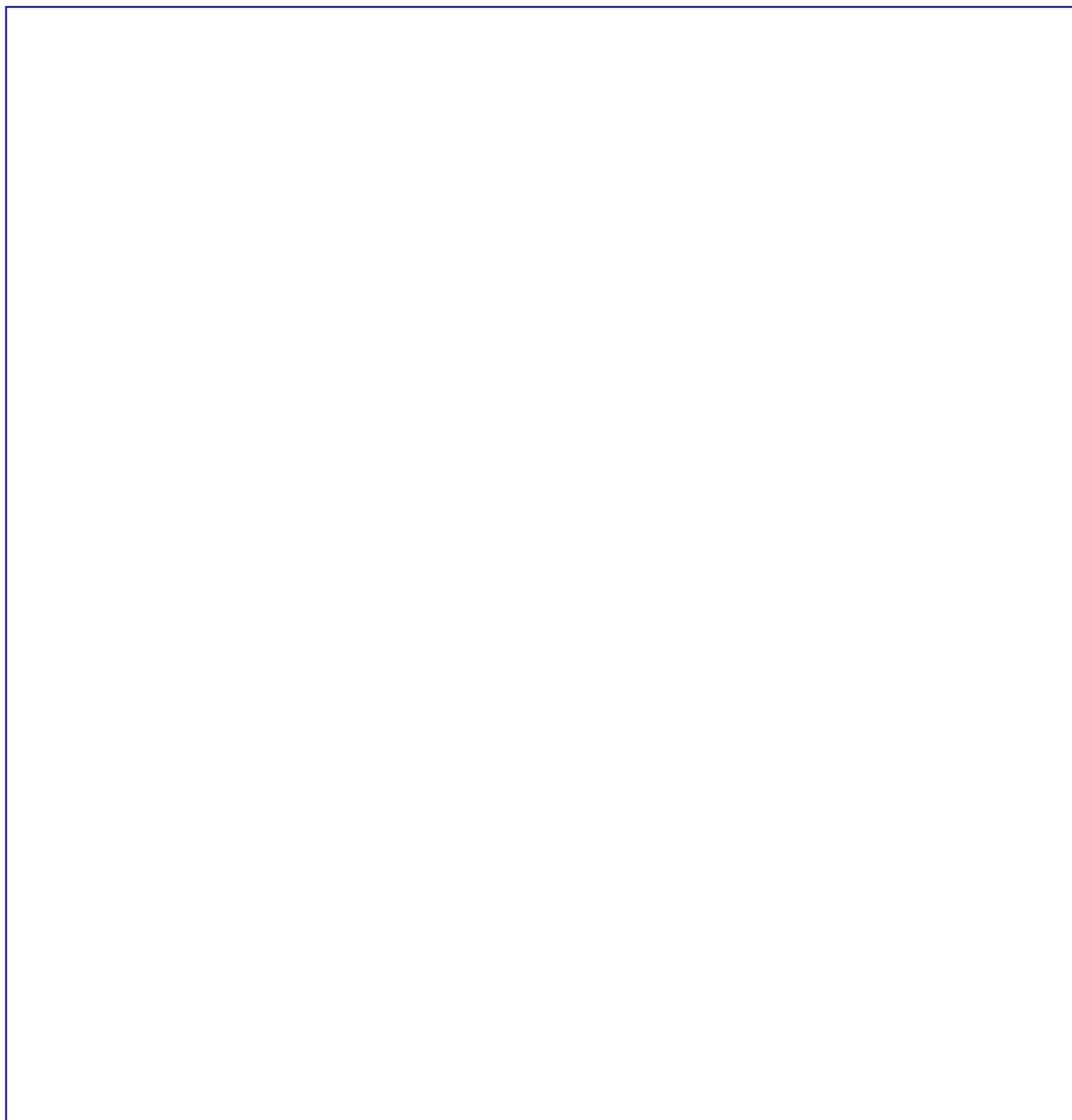
The controls are being considered for the project based on the selections from the previous assessments?

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

Please add additional controls:

(FY 2010) PIA: Additional Comments

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

A large, empty rectangular box with a thin black border, intended for users to enter their additional comments. The box is currently blank.

(FY 2010) PIA: VBA Minor Applications

Explain what minor application that are associated with your installation? (Check all that apply)

	Records Locator System	x	Education Training Website	x	Appraisal System	Baker System	x	Veterans Assistance Discharge System (VADS)	
x	Veterans Assistance Discharge System (VADS)	x	VR&E Training Website		Web Electronic Lender Identification	Dental Records Manager	x	VBA Training Academy	
x	LGY Processing	x	VA Reserve Educational Assistance Program	x	CONDO PUD Builder	Sidexis	x	Veterans Service Network (VETSNET)	
x	Loan Service and Claims	x	Web Automated Verification of Enrollment	x	Centralized Property Tracking System	Priv Plus	x	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)	
x	LGY Home Loans	x	Right Now Web	x	Electronic Appraisal System	Mental Health Asisstant	x	BIRLS	
x	Search Participant Profile (SPP)	x	VA Online Certification of Enrollment (VA-ONCE)	x	Web LGY	Telecare Record Manager	x	Centralized Accounts Receivable System (CARS)	
x	Control of Veterans Records (COVERS)		Automated Folder Processing System (AFPS)		Access Manager	Omicell	x	Compensation & Pension (C&P)	
x	SHARE	x	Personal Computer Generated Letters (PCGL)		SAHSHA	Powerscribe Dictation System		Corporate Database	
x	Modern Awards Process Development (MAP-D)	x	Personnel Information Exchange System (PIES)		VBA Data Warehouse	EndoSoft	x	Control of Veterans Records (COVERS)	
x	Rating Board Automation 2000 (RBA2000)	x	Rating Board Automation 2000 (RBA2000)	x	Distribution of Operational Resources (DOOR)	x	Compensation and Pension (C&P)	Data Warehouse	
x	State of Case/Supplemental (SOC/SSOC)	x	SHARE	x	Enterprise Wireless Messaging System (Blackberry)	x	Montgomery GI Bill	x	INS - BIRLS
x	Awards	x	State Benefits Reference System	x	VBA Enterprise Messaging System		Vocational Rehabilitation & Employment (VR&E) CH 31		Mobilization
x	Financial and Accounting System (FAS)		Training and Performance Support System (TPSS)	x	LGY Centralized Fax System		Post Vietnam Era educational Program (VEAP) CH 32	x	Master Veterans Record (MVR)
x	Eligibility Verification Report (EVR)	x	Veterans Appeals Control and Locator System (VACOLS)	x	Review of Quality (ROQ)		Spinal Bifida Program Ch 18	x	BDN Payment History
x	Automated Medical Information System (AMIS)290	x	Veterans On-Line Applications (VONAPP)		Automated Sales Reporting (ASR)	x	C&P Payment System		
x	Web Automated Reference Material System (WARMS)		Automated Medical Information Exchange II (AIME II)	x	Electronic Card System (ECS)		Survivors and Dependents Education Assistance CH 35		
x	Automated Standardized Performace Elements Nationwide (ASPEN)	x	Committee on Waivers and Compromises (COWC)	x	Electronic Payroll Deduction (EPD)		Reinstatement Entitelment Program for Survivors (REAPS)		
x	Inquiry Routing Information System (IRIS)	x	Common Security User Manager (CSUM)	x	Financial Management Information System (FMI)		Educational Assistance for Members of the Selected Reserve Program CH 1606		
x	National Silent Monitoring (NSM)	x	Compensation and Pension (C&P) Record Interchange (CAPRI)		Purchase Order Management System (POMS)		Reserve Educational Assistance Program CH 1607		
x	Web Service Medical Records (WebSMR)	x	Control of Veterans Records (COVERS)		Veterans Canteen Web	x	Compensation & Pension Training Website		
x	Systematic Technical Accuracy Review (STAR)	x	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)		Inventory Management System (IMS)	x	Web-Enabled Approval Management System (WEAMS)		
x	Fiduciary STAR Case Review	x	Fiduciary Beneficiary System (FBS)		Synquest		FOCAS		

x	Veterans Exam Request Info System (VERIS)	x	Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS		Work Study Management System (WSMS)
x	Web Automated Folder Processing System (WAFPS)		Inforce	ASSISTS	x	Benefits Delivery Network (BDN)
	Courseware Delivery System (CDS)	x	Awards	MUSE	x	Personnel and Accounting Integrated Data and Fee Basis (PAID)
	Electronic Performance Support System (EPSS)		Actuarial	Bbraun (CP Hemo)	x	Personnel Information Exchange System (PIES)
x	Veterans Service Representative (VSR) Advisor		Insurance Self Service	VIC	x	Rating Board Automation 2000 (RBA2000)
x	Loan Guaranty Training Website		Insurance Unclaimed Liabilities	BCMA Contingency Machines	x	SHARE
x	C&P Training Website		Insurance Online	Script Pro	x	Service Member Records Tracking System

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 wish to include.

Minor app #1	Name	Description	Comments
	<input type="checkbox"/>	Is PII collected by this min or application?	
	<input type="checkbox"/>	Does this minor application store PII?	
		If yes, where?	
	Who has access to this data?		

Minor app #2	Name	Description	Comments
	<input type="checkbox"/>	Is PII collected by this min or application?	
	<input type="checkbox"/>	Does this minor application store PII?	
		If yes, where?	
	Who has access to this data?		

Minor app #3	Name	Description	Comments
	<input type="checkbox"/>	Is PII collected by this min or application?	
	<input type="checkbox"/>	Does this minor application store PII?	
		If yes, where?	
	Who has access to this data?		

(FY 2010) PIA: VISTA Minor Applications

Explain what minor application that are associated with your installation? (Check all that apply)

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS	OUTPATIENT PHARMACY	SOCIAL WORK
ADP PLANNING (PLANMAN) ADVERSE REACTION TRACKING ASISTS	DSS EXTRACTS EDUCATION TRACKING EEO COMPLAINT TRACKING	INTAKE/OUTPUT INTEGRATED BILLING INTEGRATED PATIENT FUNDS	PAID PATCH MODULE PATIENT DATA EXCHANGE	SPINAL CORD DYSFUNCTION SURGERY SURVEY GENERATOR
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT SUPPORT	PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	KERNEL	PATIENT REPRESENTATIVE	TOOLKIT
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KIDS	PCE PATIENT CARE ENCOUNTER	UNWINDER
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	LAB SERVICE	PCE PATIENT/IHS SUBSET	UTILIZATION MANAGEMENT ROLLUP
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LETTERMAN	PHARMACY BENEFITS MANAGEMENT	UTILIZATION REVIEW
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LEXICON UTILITY	PHARMACY DATA MANAGEMENT	VA CERTIFIED COMPONENTS - DSSI
BED CONTROL	EXTENSIBLE EDITOR	LIBRARY	PHARMACY NATIONAL DATABASE	VA FILEMAN
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIST MANAGER	PHARMACY PRESCRIPTION PRACTICE	VBECs
CAPACITY MANAGEMENT - RUM	FEE BASIS	MAILMAN	POLICE & SECURITY	VDEF
CAPRI	FUNCTIONAL INDEPENDENCE	MASTER PATIENT INDEX VISTA	PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE	PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
CARE MANAGEMENT CLINICAL CASE REGISTRIES	GEN. MED. REC. - I/O GEN. MED. REC. - VITALS	MEDICINE MENTAL HEALTH	PROSTHETICS QUALITY ASSURANCE INTEGRATION	VISIT TRACKING VISTALINK
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM	QUALITY IMPROVEMENT CHECKLIST	VISTALINK SECURITY
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET	QUASAR	VISUAL IMPAIRMENT SERVICE TEAM ANRV
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHVET	RADIOLOGY/NUCLEAR MEDICINE	VOLUNTARY TIMEKEEPING
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original) A4EL	RECORD TRACKING	VOLUNTARY TIMEKEEPING NATIONAL
CMOP	HEALTH SUMMARY	NATIONAL DRUG FILE	REGISTRATION	WOMEN'S HEALTH
CONSULT/REQUEST TRACKING	HINQ	NATIONAL LABORATORY TEST	RELEASE OF INFORMATION - DSSI	CARE TRACKER
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NDBI	REMOTE ORDER/ENTRY SYSTEM	
CPT/HCPCS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NETWORK HEALTH EXCHANGE	RPC BROKER	
CREDENTIALS TRACKING	IFCAP	NOIS	RUN TIME LIBRARY	

DENTAL
DIETETICS

IMAGING
INCIDENT REPORTING

NURSING SERVICE
OCCURRENCE SCREEN

SAGG
SCHEDULING

DISCHARGE SUMMARY

INCOME VERIFICATION MATCH

ONCOLOGY

SECURITY SUITE UTILITY PACK

DRG GROUPER

INCOMPLETE RECORDS
TRACKING

ORDER ENTRY/RESULTS
REPORTING

SHIFT CHANGE HANDOFF
TOOL

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?

Minor app #1 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?

Minor app #2 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?

Minor app #3 Does this minor application store PII?

If yes, where?

Who has access to this data?

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

Name	Description	Comments

Minor app #1

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

Minor app #2

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

Minor app #3

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?

Who has access to this data?

(FY 2010) PIA: Final Signatures

Facility Name: St. Paul Regional Office

Title:	Name:	Phone:	Email:
Privacy Officer:	Xavier Williams / Jon Power	612-970-8902 612-970-5643	xavier.williams@va.gov jon.power@va.gov
Information Security Officer:	Bryan Steenerson	612-970-5204	bryan.steenerson@va.gov
Chief Information Officer:	Pete Kostohryz	612-970-5220	pete.kostohryz@va.gov
Person Completing Document:	Bryan Steenerson / Jon Power	612-970-5204	bryan.steenerson@va.gov
System / Application / Program Manager:	Kevin C. Causley	202-4619170	kevin.causley@va.gov

Date of Report: 01/00/1900

OMB Unique Project Identifier 029-00-02-00-01-1028-00-404-139

Project Name Region 5 > VBA > St Paul Region >

VARO St. Paul > LAN