

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://www.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.

All PIA Validation Letters should be emailed to christina.pettit@va.gov to receive full credit for submission.

(FY 2011) PIA: System Identification

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

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 provided 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:	VBA Providence Regional Office		
Title:	Name:	Phone:	Email:
Privacy Officer:	Susan Q. McKinney	401-223-3655	susan.mckinney@va.gov
Information Security Officer:	Richard Ciampa	401-223-3778	rick.ciampa@va.gov
Facility Chief Information Officer	Terry Hague	410-223-3725	terry.hague@va.gov
System Owner/ Delegation of Authority	Kevin C Causley	202-461-9170	kevin.causley@va.gov
Other Titles:	Mary Barley	202-461-9175	mary.barley@va.gov
Person Completing Document:	Susan Q. McKinney	401-223-3655	susan.mckinney@va.gov

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. **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): **06/2011**

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

2. Name of the System of Records:

Loan Guaranty Home, Condominium and Manufactured Home Loan Applicant Records, Specially Adapted Housing Applicant Records, and Vendee Loan Applicant Records--VA, Compensation, Pension, Education and Rehabilitation Records-VA, Veterans and Beneficiaries Identification Records Location Subsystem--VA. 36VA00 Veterans and Armed Forces Personnel United States Government Life Insurance Records-VA. 46VA00 Veterans, Beneficiaries and Attorneys United States Government Insurance Award Records- VA. 53VA00 Veterans Mortgage Life Insurance-VA, Veterans and Beneficiaries Identification and Records Location (BIRLS) and Compensation, Pension, Education, and Rehabilitation (covers BDN and Corporate databases)

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

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

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

Yes

Does the System of Records Notice require modification or updating?

No

(Please Select Yes/No)

Is PII collected by paper methods?

Yes

Is PII collected by verbal methods?

Yes

Is PII collected by automated methods?

Yes

Is a Privacy notice provided?

Yes

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

Yes

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

Yes

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

Yes

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

Yes

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Paper & Electronic	Information will be used to communicate with individuals about their benefits.	All	All
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	Information is collected to provide all entitled benefits in the most complete and effective manner. Systems can contain dependent data of veteran such as personal information including name and address, age, school status, relationship to the veteran and medical status. Additional benefit may be payable for dependents as well.	All	All
Service Information	Paper & Electronic	Information is collected to provide all entitled benefits in the most complete and effective manner. The benefit systems contains veteran service data such as: Reserve and Guard Participation, retired pay or severance pay, hazardous agent exposure, Branch of service, duty date, released date, type of discharge, separation reason. All service data is collected to determine eligibility to specific benefits.	All	All
Medical Information	Paper & Electronic	Information is collected to provide all entitled benefits in the most complete and effective manner. The benefit systems contains medical information such as: hazardous agent exposure, branch of service, duty date, released date, type of discharge, separation reason, medical records, military clinical records, government health records, vocational rehabilitation and employment records. All medical data is collected to determine eligibility to specific benefits.	All	All
Criminal Record Information	Paper & Electronic	Information is collected to provide all entitled benefits in the most complete and effective manner. The benefits systems contain criminal data such as: line of duty investigations to include police reports; incarceration at federal, state or local facility, fugitive felon status, and/or investigative reports for some accidents. Data may be used to determine basic entitlement and continued eligibility that could be reduced as a result of incarceration.	All	All
Guardian Information	Paper & Electronic	Information is collected to provide all entitled benefits in the most complete and effective manner. The benefits systems contain guardian data such as: court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accounting and other dependent information. Medical information would also be used to determine various guardian decisions; e.g., court ordered due to veteran unable to care for dependent.	All	All

Education Information	Paper & Electronic	Information is collected to provide all entitled benefits in the most complete and effective manner. The benefit systems also contain veteran educational records such as: education program approval information, approved courses, effective dates, types of training, facility code, objective code and training type.	All	All	
Benefit Information	ALL	<p>PRIVACY ACT INFORMATION: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is voluntary; however, no allowance of compensation or pension may be granted unless this form is completed fully as required by law. Giving us you and your dependents' Social Security numbers is mandatory. Applicants are required to provide their SSN and the SSN of any dependents for whom benefits are claimed under Title 38 USC 5101 (c)(1). The VA will</p>	All	All	
Other (Explain)					
Bank account information, employment history, gross income and net worth information, etc..	ALL	Intended use is to determine, award, and pay eligible individuals VA benefits.	All	All	
Rehabilitation Information	ALL	Information is collected to provide all entitled benefits in the most complete and effective manner. The benefit systems also contain veteran service and employment records that are required to support entitlement to vocational rehabilitation benefits. Information including awards and monetary amounts based on receipt of SSA disability income, supplemental income, and retirement benefits. Intended to determine entitlement to VA compensation and pension benefits.	All	All	
Social Security Administration (SSA) information	ALL	Information is collected to provide all entitled benefits in the most complete and effective manner. The benefit systems also contain veteran service and employment records that are required to support entitlement to vocational rehabilitation benefits. Information including awards and monetary amounts based on receipt of SSA disability income, supplemental income, and retirement benefits. Intended to determine entitlement to VA compensation and pension benefits.	All	All	
Data Type	Is Data Type Stored on your system?	Source	(If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran		Voluntary	Most of the information provided is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit. Veteran Personal data (Name, Address, Social Security Number, Family/Dependents, Marital Status, Medical Status, Birth Information, Death Information) and Veteran Dependent Data (personal information including name and address, age, school status, relationship to the veteran, medical status) is used to (1) communicate with the Veteran about his/her benefits, to notify of change in account status and advise about new options and (2) to determine eligibility and process entitlement.

Family Relation (Spouse, children, parents, grandparents, etc)

Yes

Veteran

Voluntary

Most of the information provided is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit. Veteran Personal data (Name, Address, Social Security Number, Family/Dependents, Marital Status, Medical Status, Birth Information, Death Information) and Veteran Dependent Data (personal information including name and address, age, school status, relationship to the veteran, medical status) is used to (1) communicate with the Veteran about his/her benefits, to notify of change in account status and advise about new options and (2) to determine eligibility and process entitlement.

Service Information

Yes

Other Federal Agency (Identify)

Mandatory

Agency requests to other federal and state agencies to include reserve or national guard units and to the federal records management center. Department of Defense provides (1) Service Data: reserve and guard participation, retired pay or severance pay, hazardous agent exposure, branch of service, active duty date, released date, type of discharge, separation reason; and (2) Medical Records: Military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations. Other Federal agencies that provide information that is used to determine eligibility and to process entitlements are the Department of Labor, Department of Treasury, Federal Bureau of Prisons, Department of Health and Human Services, Defense Manpower Data Center, Federal Parent Locator Service, General Accounting Office, Office of Inspector General, Office of Personnel Management, and Bureau of Census, Federal Housing Administration, Internal Revenue Service, Department of Housing and Urban Development. Most of the information provided is kept in a central database not located at this facility but any c be stored on the LAN at any given time during or after the processing of a VBA benefit.

Medical Information

Yes

Other (Explain)

Mandatory

Agency requests are made to the Veteran's Health Administration (VHA) through CAPRI in the VISTA database. Private treatment records requests are made at the request of the veteran either directly or through a records release form provided to Veteran's Benefits Administration (VBA). Most of the information provided is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.

Criminal Record Information

Yes

Other (Explain)

Mandatory

To request veteran information from the state Bureau of Prisons and Police Records: Incarceration at federal state or local facility, fugitive felon status, investigative reports for some accidents. Benefits are suspended for incarcerated veterans. The benefits systems contain criminal data such as: line of duty investigations to include police reports; incarceration at federal, state or local facility, fugitive felon status, and/or investigative reports for some accidents.

Guardian Information	Yes	Veteran	Mandatory	American Red Cross and Blind American Veterans provide information that is used to determine eligibility and to process entitlements. Blind American Veterans also exchange information in their capacity as fiduciaries for the veteran or the veteran's dependents. Guardianship Information may include court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accountings. It may also include Veteran Dependent Data: Personal information including name and address, age, school status, relationship to the veteran, medical status. Most of the information provided is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.
Education Information	Yes	State Agency (Identify)	Voluntary	Educational institutions (schools) provide information on veteran's enrollment and attendance. Information is used to process education benefits. Other information is collected from public sources (i.e., websites or databases) in order to locate and contact the veteran and develop information to support the veteran's claim. Most of the information provided is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	Most of the information provided is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit. To determine eligibility for veterans benefits, all VA IT systems such as BIRLS, VA Insurance System, Corporate Databases, and information from VISTA (Veterans Health Administration system) are used. Veteran Personal data (Name, Address, Social Security Number, Family/Dependents, Marital Status, Medical Status, Birth Information, Death Information) and Veteran Dependent Data (personal information including name and address, age, school status, relationship to the veteran, medical status) is used to (1) communicate with the Veteran about his/her benefits, to notify of change in account status and advise about new options and (2) to determine eligibility and process entitlement.
SSA Bank account information, employment history, gross income and net worth information, etc..	No	Other Federal Agency (Identify)	Mandatory	The Social Security Administration also verifies if a veteran is deceased and provides income verification, SSN match.
Rehabilitation Information	Yes	Veteran VA Files / Databases (Identify file)	Voluntary Mandatory	Most of the information provided is kept in a central database not located at this facility but any of this information could be stored on the LAN at any given time during or after the processing of a VBA benefit.

(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	<p>(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. ** Data that is shared – information about a veteran’s service connected disability (affected extremity, original effective date of the disability rating and the current (most recent) date the rating was changed, and the effective date of the combined service connected evaluation) (2) CAPRI enables data flow between VBA and VHA. ** Data that is shared – PII information to include but not limited to veteran’s name, address, contact information, and medical records (treatment records, lab information, appointment information)</p>	Both PII & PHI	VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II,

VBA IRM HANDBOOK 5.00.02HB2

Other Veteran Organization	Co-located Veterans Service Organizations (VSO's)	Yes	<p>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. ** Data that is shared - Name, Address, Social Security Number, Family/Dependents, marital status, medical status, birth information, death information, service data; Reserve or Guard Participation, retired pay or severance pay, hazardous agent exposure, branch of service, duty date, released date, type of discharge, separation reason, medical records, military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations to include police reports; incarceration at federal, state or local facility, fugitive felon status, and/or investigative reports for some accidents. The records may also contain additional veteran information such: Guardian information; court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accounts. The benefit systems accessed through the LAN also contain veteran educational records such as: education program approval information, approved courses, effective dates, types of training, facility code, objective code and training type. Income verification is also used for veteran pension based</p>	VA Directive 6500, M20-4, Both PII & PHI Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II,
Other Federal Government Agency		No		N/A
State Government Agency		No		N/A
Local Government Agency		No		N/A
Research Entity		No		N/A

Other Veteran Organization	Remote Veterans Service Organizations	Yes	<p>Remote Veterans Service Organizations (VSOs) –Remote Veterans Service Organizations have been given on-line read only access to SHARE and MAP-D. The remote VSOs access veteran data securely through VA’s Virtual Private Network. On-line access is real time and may be accessed by 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. The above service organizations include all accredited service organizations. The following site has a complete list of recognized veterans service organizations - http://www.va.gov/ogc/recognizedvsos.asp. ** Data that is shared - Name, Address, Social Security Number, Family/Dependents, marital status, medical status, birth information, death information, service data; Reserve or Guard Participation, retired pay or severance pay, hazardous agent exposure, branch of service, duty date, released date,</p>	Both PII & PHI VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II,
Other Project / System		Yes	<p>Data in the VBA Corporate database and the Benefits Delivery Network database are accessed primarily to support the applications running on the LAN. ** Data that is shared - Name, Address, Social Security Number, Family/Dependents, marital status, medical status, birth information, death information, service data; Reserve or Guard Participation, retired pay or severance pay, hazardous agent exposure, branch of service, duty date, released date, type of discharge, separation reason, medical records, military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations to include police reports; incarceration at federal, state or local facility, fugitive felon status, and/or investigative reports for some accidents. The records may also contain additional veteran information such: Guardian information; court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accounts. The benefit systems accessed through the LAN also contain veteran educational records such as: education program approval information, approved courses, effective dates, types of training, facility code, objective code and training type. Income verification is also used for veteran pension based decisions and entitlements. All users of the system are responsible for the privacy of this information. Users are trained annually on their privacy responsibilities.</p>	Both PII & PHI VBA IRM Handbook 5.00.02HB4

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

Describe process for authorizing access to this data.

Answer: All VBA employees that are authorized to access and process veterans claims are provided specific password that allow them to obtain or access data within the VBA Corporate system. In addition, Veterans Service Organizations and attorney's that have power-of-attorney over the veteran have restricted read-only access. 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. The criteria, procedures, controls, and responsibilities regarding access are documented on VA Directive 6500, M20-4, Part II, VBA IRM Handbook 5.00.02HB2 and M20-4, Part II, VBA IRM Handbook 5.00.02HB4. Per VA Directive 6500, user access is restricted to a need to know basis (with the veteran's signature), the VA will process the request and send the requesting information back to the veteran via mail.

(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: Data is checked for completeness by system audits, manual verifications and annual questionnaires through automated veteran letters. These letters ask specific 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. Additionally, 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 with the 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 correct 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: In general, Data is retained on all VBA systems indefinitely.

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

Answer: To process veteran claims for benefits.

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
<http://www.benefits.va.gov/WARMS/docs/admin20/rcc/part1/sec08.doc>

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 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:

(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? No

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? No

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

Answer: 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.

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

Answer: (Other Risks)

7. Security

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) The NIST SP 800-53 Moderate Baseline Security Controls are implemented. All security controls are implemented through a cohesive security structure that is geared to maintaining risk to information and information resources to acceptable levels. In addition to documented risk management, other management level controls such as system security planning, certification and accreditation and security reviews are also implemented to assure that controls reflect management policies at operational levels including at the enterprise, business line and project level. Operational and technical controls such as contingency planning, input/output settings, data integrity and validation measures and logical access controls, are implemented on the various network, system, server and application levels to assure that information is secured in transit, process and storage. For example, the VA employs a virtual private network to assure the privacy of information in transit. This system works in conjunction with strong authentication measures to ensure and authenticate the identification of VA network users. Moreover, the VA employs a comprehensive incident response unit to respond to unwanted incursions and institutes enterprise level anti-virus system to protect mission critical applications on the desktop. Also, the VA security program is an iterative program with repeatable processes that, in an ongoing basis, will mitigate vulnerabilities, minimize security exposures and maintain security and operating risk at acceptable levels. A security plan has been developed that documents the procedures required ensuring the integrity, confidentiality, and availability to VA information. Specifically, personnel security, physical protection, production input/output controls, contingency planning, system hardware and software maintenance controls, security awareness and training, and incident response capabilities are discussed in detail. The details contained within these sections include specific activities and procedures, which ultimately ensure that the integrity, confidentiality, and availability to VA information contained within the system is protected as required by Federal policy. All files, records, reports, and other papers and documents pertaining to any claim under any of the laws administered by the Department of Veterans Affairs and the names and addresses of present or former members of the Armed Forces, and their dependents, in the possession of the Department shall be confidential and privileged. Other controls used to mitigate risks include: Audit logs are examined regularly for possible incidents, physical access controls exist with layers of physical security defense in place, the local fire department is close, and there are physical and environmental controls in place such as sprinklers and smoke detectors. Fire drills are conducted on a regular basis. Employees are educated regularly on security awareness and electronically agree to a Rules of Behavior on an annual basis. Certain preapproved employees could work from their homes, or off site offices. Benefit processing workload could be shifted to other Regional Offices. Employees could be temporality relocated to satellite offices or other Regional Offices, depending on the emergency. Authorized changes to LAN environment are instituted as directed by Hines. Windows 2000 implementation provides standardized least privilege and access permission management controls. Background investigations are conducted on all employees.

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

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

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

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

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

Please add additional controls:

A standardized Department methodology based on the direction in National Institute of Standards and Technology (NIST) guidance is used to continuously monitor, test and evaluate security for this LAN. The approximately 60 common security controls provided by the Office of Information and Technology (OIT), or other respective VA Program Office, are tested every year. Security testing evaluates approximately one-third of the remaining 90 controls on an annual basis, with the entire respective application NIST Special Publication (SP) 800-53 security control baseline—at the Federal Information Processing Standard (FIPS) 199 level of moderate--being tested over each three-year period. The testing supports certification and re-accreditation requirements, as well as Federal Information Security Management Act (FISMA) requirements to annually test the operational, management, and technical controls of each Department system. The specific controls identified for testing are selected by OIT Operations, with advice from the VA Office of Cyber Security (OCS), and include key controls that provide integrity and confidentiality (such as access, authentication, configuration management, and media controls). The tests are conducted using the criteria in NIST SP 800-53A, Second Public Draft, Guide for Assessing the Security Controls in Federal Information Systems, and tailored to the VA operational environment. Testing of operational systems is primarily conducted by the OIT Compliance and Inspection Management Office, which was chartered to conduct security control assessments across the VA enterprise, as well as independent contractors. For test results that indicate a security control is not operating as intended, a Plan of Action and Milestones (POA&Ms) is developed and entered into the Department's Security Management and Reporting Tool (SMART). The PO&AM identifies the activities and timelines for correction of the security weakness, and is managed by the respective application information security officer, with progress monitored by the application program manager. The VA Chief Information Officer receives quarterly reporting on the status of all POA&Ms, with that information also being included in required updates to the Office of Management and Budget as part of the FISMA reporting process. On an annual basis, the VA Chief Information Officer (CIO), in conjunction with system owners and information owners, and with advice from the VA Office of Inspector General (OIG), evaluate the Department's overall IT security posture. This evaluation includes identification of significant security performance gaps, the prioritization of key POA&M weakness areas for immediate remediation action, as well as the designation of certain security areas that would benefit from enterprise-wide management of a single security solution, thereby effectively targeting those areas for action that would most improve the Department's security posture in the near-term.

(FY 2011) PIA: Additional Comments

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

(FY 2011) PIA: VBA Minor Applications

Which of these are sub-components of your system?

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	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)
Awards	X Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	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)	X Compensation & Pension Training Website
BDN Payment History	X Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
X BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	X Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wireless Messaging System (Blackberry)
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	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	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)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitlement Program for Survivors (REAPS)
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)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	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)	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	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	X Web Automated Reference Material System (WARMS)
Veterans Canteen Web	X Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	X Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
X VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		Work Study Management System (WSMS)

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

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

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

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

(FY 2011) PIA: VISTA Minor Applications

Which of these are sub-components of your system?

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
X CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	Health Level Seven	Master Patient Index VistA
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
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
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
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 Committee on Waiver and Compromises	Military/Vet Eye Injury Registry	VHAHUNFPC1
CP&E	Mumps AudioFAX	VISTA RAD
Crystal Reports Enterprise	NOAHLINK	Whiteboard
Data Innovations	Omnicell	
DELIVEREX	Onvicord (VLOG)	
	Optifill	

DICTATION-Power Scribe
DRM Plus
DSIT
DSS Quadramed
EDS Whiteboard (AVJED)
EKG System
Embedded Fragment Registry

P2000 ROBOT
PACS database
Personal Computer Generated
Letters
PICIS OR
PIV Systems
Q-Matic
QMSI Prescription Processing

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide 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?

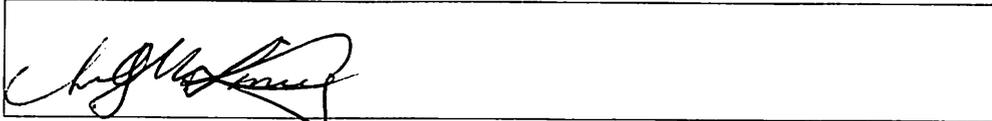
Name
Description
Comments
Is PII collected by this minor application?
Does this minor application store PII?
If yes, where?
Who has access to this data?

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?

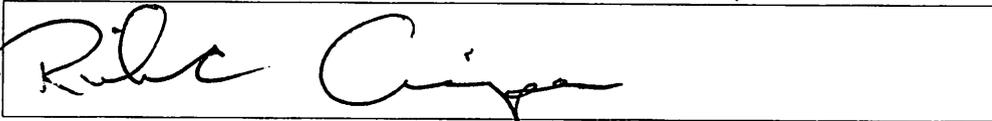
(FY 2011) PIA: Final Signatures

Facility Name: **Region 5 > VBA > St. Paul Region > VARO Providence > LAN**

Privacy Officer: **Susan Q. McKinney** 401-223-3655 susan.mckinney@va.gov



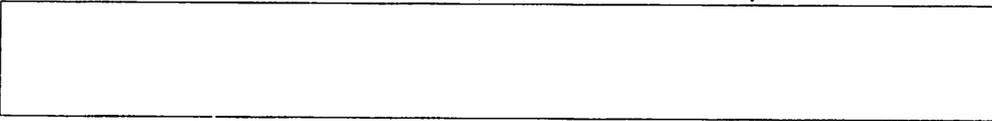
Information Security Officer: **Richard Ciampa** 401-223-3778 rick.ciampa@va.gov



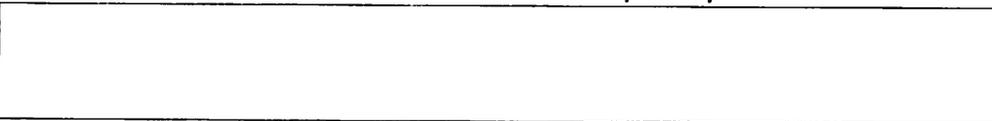
Facility Chief Information Officer **Terry Hague** 410-223-3725 terry.hague@va.gov



System Owner/ Delegation of Authority **Kevin C Causley** 202-461-9170 kevin.causley@va.gov



Other Titles: C&A Coordinator **Mary Barley** 202-461-9175 mary.barley@va.gov



Date of Report: **06/2011**
OMB Unique Project Identifier **029-00-02-00-01-1120-00**

Project Name **Region 5 > VBA > St. Paul Region >
VARO Providence > LAN**