

(FY 2010) PIA: System Identification

Program or System Name: Region 5 > VBA > St Petersburg >
VARO St. Louis RMC >LAN

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00
An Access system developed to incoming calls or requests for information from veterans, VA personnel and military service members and document our

Description of System / Application / Program: responses.

Facility Name: St. Louis RMC

Title:	Name:	Phone:	Email:
Privacy Officer:	Lattissua Tyler	314-538-4586	lattissua.tyler@va.gov
Information Security Officer:	Dave Ricker	515-323-7568	david.ricker@va.gov
Chief Information Officer:	John Maney	314-538-4590	john.maney@va.gov
Person Completing Document:	Lattissua Tyler	313-538-4586	lattissua.tyler@va.gov
System Owner:	Kevin C. Causley	202-461-9170	kevin.causley@va.gov
C&A Coordinator:	Mary D. Barley	202-461-9175	mary.barley@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, United States Code, section 501(a) and Chapters 11, 13, 15, 18, 23,30, 31, 32, 34, 35, 36, 39, 51, 53, 55.

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

1,000,000 to 9,999,999

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.

01/2000

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):

Click on 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): 55VA26, 58VA21/22/28, 38VA21, 36VA00, 46VA00, 53VA00
 Manufactured Home Loan Applicant Records, Specially Adapted Housing Applicant Records, Vendeo Loan Applicant Records-VA, Compensation, Pension, Education and Rehabilitation Records-VA, Veterans and Beneficiaries Identification 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 Awards Records-VA. 53VA00 Veterans Mortgage Life Insurance-VA. Veterans and Beneficiaries Identification and
- 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.va.gov/oi/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 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 & employment	Verbal & Written	Verbal & Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Benefits & employment	Verbal & Written	Verbal & Written
Service Information	ALL	Benefits & employment	Verbal & Written	Verbal & Written
Medical Information	ALL	Benefits & employment	Verbal & Written	Verbal & Written
Criminal Record Information	ALL	Benefits & employment	Verbal & Written	Verbal & Written
Guardian Information	ALL	Benefits & employment	Verbal & Written	Verbal & Written
Education Information	ALL	Benefits & employment	Verbal & Written	Verbal & Written
Benefit Information	ALL	Benefits & employment	Verbal & Written	Verbal & Written
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	On the form
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	On the form
Service Information	Yes	Veteran	Voluntary	On the form
Medical Information	Yes	Veteran	Voluntary	On the form
Criminal Record Information	Yes	Veteran	Voluntary	
Guardian Information	Yes	Veteran	Voluntary	On the form
Education Information	Yes	Veteran	Voluntary	On the form
Benefit Information	Yes	Veteran	Voluntary	On the form
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	NA	No			No one has access to the system, other than RMC.
Other Veteran Organization	NA	No			
Other Federal Government Agency	NA	No			
State Government Agency	NA	No			
Local Government Agency	NA	No			
Research Entity	NA	No			
Other Project / System					
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** Hand written phone slip

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request? **No**

Drug/Alcohol Counseling Mental Health HIV

Research Sickle Cell Other (Please Explain)

if yes, please check all that apply:

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: the system has specific tabs to complete. Must be in a specific format. No other data can be entered.

How is data checked for completeness?

Answer: supervisors and quality assurance team validate a percentage of the information employees input

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

Answer: The data is purged after 4 years.

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

Answer: supervisors and quality assurance team validate a percentage of the information employees input

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: purged after four years

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

Answer: to validate our responses to requests for copies or system updates

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

Answer: IRM staff is responsible for purging/removing data

Where are these procedures documented?

Answer: NA

How are data retention procedures enforced?

Answer: IRM requests confirmation that data is no longer need from Division Chief

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

No

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: The VA RMC has developed an IT Contingency plan which address possible risks to the Network system and ways to mitigate risks. ATRS program is an access program is a part of the network.

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

- | | |
|---|--|
| <input type="checkbox"/> Air Conditioning Failure | <input type="checkbox"/> Hardware Failure |
| <input checked="" type="checkbox"/> Chemical/Biological Contamination | <input type="checkbox"/> Malicious Code |
| <input type="checkbox"/> Blackmail | <input type="checkbox"/> Computer Misuse |
| <input type="checkbox"/> Bomb Threats | <input checked="" type="checkbox"/> Power Loss |
| <input checked="" type="checkbox"/> Cold/Frost/Snow | <input type="checkbox"/> Sabotage/Terrorism |
| <input type="checkbox"/> Communications Loss | <input type="checkbox"/> Storms/Hurricanes |
| <input type="checkbox"/> Computer Intrusion | <input type="checkbox"/> Substance Abuse |
| <input type="checkbox"/> Data Destruction | <input type="checkbox"/> Theft of Assets |
| <input type="checkbox"/> Data Disclosure | <input checked="" type="checkbox"/> Theft of Data |
| <input type="checkbox"/> Data Integrity Loss | <input type="checkbox"/> Vandalism/Rioting |
| <input type="checkbox"/> Denial of Service Attacks | <input type="checkbox"/> Errors (Configuration and Data Entry) |
| <input checked="" type="checkbox"/> Earthquakes | <input type="checkbox"/> Burglary/Break In/Robbery |
| <input type="checkbox"/> Eavesdropping/Interception | <input type="checkbox"/> Identity Theft |
| <input type="checkbox"/> Fire (False Alarm, Major, and Minor) | <input type="checkbox"/> Fraud/Embezzlement |
| <input checked="" 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 type="checkbox"/> Audit and Accountability |
| <input type="checkbox"/> Access Control | <input type="checkbox"/> Configuration Management |
| <input checked="" type="checkbox"/> Awareness and Training | <input type="checkbox"/> Identification and Authentication |
| <input checked="" type="checkbox"/> Contingency Planning | <input type="checkbox"/> Incident Response |
| <input type="checkbox"/> Physical and Environmental Protection | <input type="checkbox"/> Media Protection |
| <input type="checkbox"/> Personnel Security | |
| <input type="checkbox"/> Certification and Accreditation Security Assessments | |

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, controls to mitigate misuse of information and possible privacy notice

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's 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.

(FY 2010) PIA: VBA Minor Applications

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

Records Locator System	Education Training Website	Appraisal System
Veterans Assistance Discharge System (VADS)	VR&E Training Website	Web Electronic Lender Identification
LGY Processing	VA Reserve Educational Assistance Program	CONDO PUD Builder
Loan Service and Claims	Web Automated Verification of Enrollment	Centralized Property Tracking System
LGY Home Loans	Right Now Web	Electronic Appraisal System
Search Participant Profile (SPP)	VA Online Certification of Enrollment (VA-ONCE)	Web LGY
Control of Veterans Records (COVERS)	Automated Folder Processing System (AFPS)	Access Manager
SHARE	Personal Computer Generated Letters (PCGL)	SAHSHA
Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	VBA Data Warehouse
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry)
Awards	State Benefits Reference System	VBA Enterprise Messaging System
Financial and Accounting System (FAS)	Training and Performance Support System (TPSS)	LGY Centralized Fax System
Eligibility Verification Report (EVR)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)
Automated Medical Information System (AMIS)29D	Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Compensation and Pension (C&P)	Purchase Order Management System (POMS)
Web Service Medical Records (WebSMR)	Record Interchange (CAPRI)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)	Control of Veterans Records (COVERS)	Inventory Management System (IMS)
Fiduciary STAR Case Review	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Synquest
Veterans Exam Request Info System (VERIS)	Fiduciary Beneficiary System (FBS)	RAI/MDS
Web Automated Folder Processing System (WAFPS)	Hearing Officer Letters and Reports System (HOLAR)	ASSISTS
Courseware Delivery System (CDS)	Inforce	MUSE
Electronic Performance Support System (EPS)	Awards	Bbraun (CP Hemo)
Veterans Service Representative (VSR) Advisor	Actuarial	VIC
Loan Guaranty Training Website	Insurance Self Service	BCMA Contingency Machines
C&P Training Website	Insurance Unclaimed Liabilities	Script Pro
	Insurance Online	

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.

Minor app #1	Name		Description	Comments
	NA			
		<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?		

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET) Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Priv Plus Mental Health Assistant	BIRLS
Telecare Record Manager	Centralized Accounts Receivable System (CARS)
Omnicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill Vocational Rehabilitation & Employment (VR&E) CH 31 Post Vietnam Era educational Program (VEAP) CH 32	INS - BIRLS Mobilization Master Veterans Record (MVR)
Spinal Bifida Program Ch 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitlement Program for Survivors (REAPS) Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607 Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS Work Study Management System (WSMS)	
Benefits Delivery Network (BDN) Personnel and Accounting Integrated Data and Fee Basis (PAID) Personnel Information Exchange System (PIES) Rating Board Automation 2000 (RBA2000)	
SHARE Service Member Records Tracking System	

(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
ADP PLANNING (PLANMAN)	DSS EXTRACTS	INTAKE/OUTPUT
ADVERSE REACTION TRACKING	EDUCATION TRACKING	INTEGRATED BILLING
ASISTS	EEO COMPLAINT TRACKING	INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT SUPPORT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	KERNEL
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KIDS
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	LAB SERVICE
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LETTERMAN
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LEXICON UTILITY
BED CONTROL	EXTENSIBLE EDITOR	LIBRARY
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIST MANAGER
CAPACITY MANAGEMENT - RUM	FEE BASIS	MAILMAN
CAPRI	FUNCTIONAL INDEPENDENCE	MASTER PATIENT INDEX VISTA
CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE
CARE MANAGEMENT	GEN. MED. REC. - I/O	MEDICINE
CLINICAL CASE REGISTRIES	GEN. MED. REC. - VITALS	MENTAL HEALTH
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHEVET
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original)
CMOP	HEALTH SUMMARY	A4EL
CONSULT/REQUEST TRACKING	HINQ	NATIONAL DRUG FILE
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NATIONAL LABORATORY TEST
CPT/HCPCS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NDBI
CREDENTIALS TRACKING	IFCAP	NETWORK HEALTH EXCHANGE
DENTAL	IMAGING	NOIS
DIETETICS	INCIDENT REPORTING	NURSING SERVICE
DISCHARGE SUMMARY	INCOME VERIFICATION MATCH	OCCURRENCE SCREEN
DRG GROUPER	INCOMPLETE RECORDS TRACKING	ONCOLOGY
		ORDER ENTRY/RESULTS REPORTING

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.

Minor app #1	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?			

Minor app #2	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?			

Minor app #3	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?			

OUTPATIENT PHARMACY	SOCIAL WORK
PAID	SPINAL CORD DYSFUNCTION
PATCH MODULE	SURGERY
PATIENT DATA EXCHANGE	SURVEY GENERATOR
PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	TOOLKIT
PCE PATIENT CARE	UNWINDER
ENCOUNTER	UTILIZATION MANAGEMENT ROLLUP
PCE PATIENT/IHS SUBSET	UTILIZATION REVIEW
PHARMACY BENEFITS	VA CERTIFIED COMPONENTS - DSSI
MANAGEMENT	VA FILEMAN
PHARMACY DATA	
MANAGEMENT	
PHARMACY NATIONAL DATABASE	
PHARMACY PRESCRIPTION	VBECs
PRACTICE	VDEF
POLICE & SECURITY	
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	VISIT TRACKING
QUALITY ASSURANCE	VISTALINK
INTEGRATION	VISTALINK SECURITY
QUALITY IMPROVEMENT	VISUAL IMPAIRMENT SERVICE TEAM
CHECKLIST	ANRV
QUASAR	VOLUNTARY TIMEKEEPING
RADIOLOGY/NUCLEAR	VOLUNTARY TIMEKEEPING NATIONAL
MEDICINE	
RECORD TRACKING	
REGISTRATION	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI	CARE TRACKER
REMOTE ORDER/ENTRY	
SYSTEM	
RPC BROKER	
RUN TIME LIBRARY	
SAGG	
SCHEDULING	
SECURITY SUITE UTILITY PACK	
SHIFT CHANGE HANDOFF	
TOOL	

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

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

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

(FY 2010) PIA: Final Signatures

Facility Name:

St. Louis RMC

Title:

Name:

Phone:

Email:

Privacy Officer:

Lattissua Tyler

314-538-4586

lattissua.tyler@va.gov

for Anthony Studer
Digital Signature Block

Information Security Officer:

Dave Ricker

515-323-7568

david.ricker@va.gov

Dave Ricker
Digital Signature Block

Digital Signature Block

Chief Information Officer:

John Maney

314-538-4590

john.maney@va.gov

John A. Maney
Digital Signature Block

Person Completing Document:

Lattissua Tyler

313-538-4586

lattissua.tyler@va.gov

for Anthony Studer
Digital Signature Block

System / Application / Program Manager:

Kevin C. Causley

202-461-9170

kevin.causley@va.gov

Digital Signature Block

Date of Report:

01/00/1900

OMB Unique Project Identifier

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

Project Name

Region 5 > VBA > St Petersburg >

VARO St. Louis RMC > LAN