

Welcome to the PIA for FY 2011!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp

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 and 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 received full credit for submission.

(FY 2011) PIA: System Identification

Program or System Name: Muskogee Regional Office Local Area Network (LAN)
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00
 Description of System/ Application/ Program:

The Muskogee 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: Muskogee Regional Office

Title:	Name:	Phone:	Email:
Privacy Officer:	Joe Tillman	918-781-6655	joseph.tillman@va.gov
Information Security Officer:	Ron Thomas	918-781-7517	ronald.thomas4@va.gov
System Owner/ Chief Information Officer:	Kevin Causley	202-461-9170	kevin.causley@va.gov
Facility CIO, Muskogee VARO	Eddie Keefe	202-781-7711	eddie.keefe@va.gov
Other Titles: Information Security Officer	Scott Allen	918-781-7520	scott.allen2@va.gov
Person Completing Document:	Ron Thomas, ISO	918-781-7517	ronald.thomas4@va.gov
Other Titles: Field Liaison Staff	Mary Barley,	202-461-9175	mary.barley@va.gov
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: 1,610,000 - 1,996,000
 Identify what stage the System / Application / Program is at: Operations/Maintenance
 The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation. 12 years
 Is there an authorized change control process which documents any changes to existing applications or systems? Yes
 If No, please explain:
 Has a PIA been completed within the last three years? Yes
 Date of Report (MM/YYYY): 05/2011

Please check the appropriate boxes and continue to the next TAB and complete the remaining 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?

- 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):

58VA21/22

2. Name of the System of Records:

Compensation, Pension, Education, Voc ational Rehabilitation

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

<http://www.gpoaccess.gov/privacyact/index.html>

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)	ALL	To determine Benefit eligibility	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	To determine Benefit eligibility	All	All
Service Information	ALL	To determine Benefit eligibility	All	All
Medical Information	Paper & Electronic	To determine Benefit eligibility	All	All
Criminal Record Information	Paper & Electronic	To determine Benefit eligibility	All	All
Guardian Information	Paper & Electronic	To determine Benefit eligibility	All	All
Education Information	ALL	To determine Benefit eligibility	All	All
Benefit Information	ALL	To determine Benefit eligibility	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	Other (Explain)	Voluntary	DD214, VA Files Data Base (VBA Benefits Network, Veteran VAMC CAPRI/Social Security Administration, Private Physicians/Medical Facilities, Veteran
Medical Information	Yes	Other (Explain)	Voluntary	
Criminal Record Information	Yes	Veteran	Mandatory	Written notice
Guardian Information	Yes	Other (Explain)	Mandatory	other local (court systems) and the veteran
Education Information	Yes	Veteran	Mandatory	
Benefit Information	Yes	Other (Explain)	Mandatory	VBA-Education, Vocational Rehabilitation, Veteran Service Center & Pension Management Center, VA Insurance & other Federal Agency (Social Security Administration)
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	NCA,VHA	Yes	Veterans data for benefits	Both PII & PHI	Determined by higher authority
Other Veteran Organization	VSOs	Yes	All Veterans Data for benefits	Both PII & PHI	Determined by higher authority--power of attorney
Other Federal Government Agency	SSA / DOD / US Treasury	No	All Veterans Data for benefits	Both PII & PHI	Determined by higher authority
State Government Agency	OK Dept. of Veterans Affairs	Yes	All Veterans Data for benefits	Both PII & PHI	Determined by higher authority--power of attorney
Local Government Agency	N/A				
Research Entity	N/A				
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system?		Yes
Please enter the name of the system:	TIMS (The Image Management 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:	<input checked="" type="checkbox"/> Through a Written Request <input checked="" type="checkbox"/> Submitted in Person <input checked="" type="checkbox"/> 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.

(FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Limited to information needed to determine benefit eligibility

How is data checked for completeness?

Answer: Compared to verifiable documents / computer records

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

Answer: Comparison to associated verifiable information such as DOD, SSA & VHA records, and information requested c

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

Answer: Compared to verifiable documents / computer records

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

Answer: n/a

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: indefinite

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

Answer: Considered data of National Historical value

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

Answer: N/A

Where are these procedures documented?

Answer: Records Management System created by higher authority

How are data retention procedures enforced?

Answer: By Records Management Officer enforcing Records Management System created by higher authority

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

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

Answer:

(FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

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

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

Answer:

No

l of the vetera

Yes

No

(FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured. Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.. Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

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

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

Answer: RO does not have the ability to conduct this type of testing. Completed by higher authority.

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: Required systems are in place and reviewed annually.

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)

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

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

Answer: (Other Controls) N/A

PIA: PIA Assessment

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

Answer: Users required to log on with a strong password and authorized access is limited based on the concept of least privilege

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, personal security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow the NIST SP800-53 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of the Muskogee VARO common security controls. These issues are identified and described in the system security plans for the individual information systems.

Please add additional controls:

(FY 2011) PIA: Additional Comments

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

(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	x Automated Medical Information Exchange II (AIME II)
Appraisal System	x Benefits Delivery Network (BDN)	x Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	x Automated Standardized Performace Elements Nationwide (ASPEN)
x Awards	x Common Security User Manager (CSUM)	x Centralized Accounts Receivable System (CARS)
Awards	x Compensation and Pension (C&P)	x Committee on Waivers and Compromises (COWC)
Baker System	x Control of Veterans Records (COVERS)	x Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Control of Veterans Records (COVERS)	x Compensation & Pension Training Website
x BDN Payment History	Control of Veterans Records (COVERS)	x Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
x BIRLS	x Courseware Delivery System (CDS)	x Distribution of Operational Resources (DOOR)
x C&P Payment System	Dental Records Manager	x Educational Assistance for Members of the Selected Reserve Program CH 1606
x C&P Training Website	x Education Training Website	x Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	x Enterprise Wireless Messaging System (Blackberry)
x Corporate Database	x 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)
x FOCAS	x Fiduciary Beneficiary System (FBS)	x Modern Awards Process Development (MAP-D)
Inforce	x Fiduciary STAR Case Review	x Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	x Financial and Accounting System (FAS)	x Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	x Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	x Personnel Information Exchange System (PIES)
LGY Home Loans	x LGY Centralized Fax System	x Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	x Loan Guaranty Training Website	x Reinstatement Entitelment Program for Survivors (REAPS)
x Montgomery GI Bill	Master Veterans Record (MVR)	x Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Asisstant	x Service Member Records Tracking System
Omicell	x National Silent Monitoring (NSM)	x Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	x Systematic Technical Accuracy Review (STAR)
RAI/MDS	x Rating Board Automation 2000 (RBA2000)	x Training and Performance Support System (TPSS)
x Right Now Web	Rating Board Automation 2000 (RBA2000)	x VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	Rating Board Automation 2000 (RBA2000)	x VA Reserve Educational Assistance Program
Script Pro	x Records Locator System	x Veterans Appeals Control and Locator System (VACOLS)
x SHARE	x Review of Quality (ROQ)	x Veterans Assistance Discharge System (VADS)
SHARE	x Search Participant Profile (SPP)	x Veterans Exam Request Info System (VERIS)
SHARE	x Spinal Bifida Program Ch 18	x Veterans Service Representative (VSR) Advisor
Sidexis	x State Benefits Reference System	x Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	x State of Case/Supplemental (SOC/SSOC)	x Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

- | | | |
|-------------------------|--|---|
| VBA Data Warehouse | Telecare Record Manager | x Web Automated Folder Processing System (WAFPS) |
| x VBA Training Academy | x VBA Enterprise Messaging System | x Web Automated Reference Material System (WARMS) |
| Veterans Canteen Web | x Veterans On-Line Applications (VONAPP) | x Web Automated Verification of Enrollment |
| VIC | x Veterans Service Network (VETSNET) | x Web-Enabled Approval Management System (WEAMS) |
| x VR&E Training Website | Web Electronic Lender Identification | x Web Service Medical Records (WebSMR) |
| x Web LGY | | x Work Study Management System (WSMS) |

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

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

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

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

(FY 2011) PIA: VISTA Minor Applicat

Which of these are sub-components of your system?

	ASISTS	Beneficiary Travel	x	Accounts Receivable	
	Bed Control	Care Management		ADP Planning (PlanMan)	
x	CAPRI	Care Tracker		Bad Code Med Admin	
	CMOP	Clinical Reminders		Clinical Case Registries	
	Dental	CPT/ HCPCS Codes		Clinical Procedures	
	Dietetics	DRG Grouper		Consult/ Request Tracking	x
x/ VR&E	Fee Basis	DSS Extracts		Controlled Substances	
	GRECC	x Education Tracking		Credentials Tracking	
	HINQ	Engineering		Discharge Summary	
	IFCAP	Event Capture		Drug Accountability	
	Imaging	Extensible Editor		EEO Complaint Tracking	
	Kernal	Health Summary	x	Electronic Signature	x
	Kids	Incident Reporting		Event Driven Reporting	
	Lab Service	Intake/ Output		External Peer Review	
	Letterman	Integrated Billing		Functional Independence	
	Library	Lexicon Utility		Gen. Med. Rec. - I/O	x
	Mailman	List Manager		Gen. Med. Rec. - Vitals	
	Medicine	Mental Health		Generic Code Sheet	
	MICOM	MyHealthEVet		Health Level Seven	
	NDBI	National Drug File		Hospital Based Home Care	
	NOIS	Nursing Service		Inpatient Medications	
	Oncology	Occurrence Screen		Integrated Patient Funds	
	PAID	Patch Module		MCCR National Database	
	Prosthetics	Patient Feedback		Minimal Patient Dataset	
	QUASER	Police & Security		National Laboratory Test	
	RPC Broker	Problem List		Network Health Exchange	
	SAGG	Progress Notes		Outpatient Pharmacy	
	Scheduling	Record Tracking		Patient Data Exchange	
	Social Work	Registration		Patient Representative	
	Surgery	Run Time Library		PCE Patient/ HIS Subset	
	Toolkit	Survey Generator		Security Suite Utility Pack	
	Unwinder	Utilization Review		Shift Change Handoff Tool	
	VA Fileman	Visit Tracking		Spinal Cord Dysfunction	
	VBECS	VistALink Security		Text Integration Utilities	
	VDEF	Women's Health		VHS & RA Tracking System	
	VistALink			Voluntary Timekeeping	

Explain any minor application that are associated with your installation that does n 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?

ions

Adverse Reaction Tracking
Authorization/ Subscription
Auto Replenishment/ Ward Stock
Automated Info Collection Sys
Automated Lab Instruments
Automated Med Info Exchange

Capacity Management - RUM
Capacity Management Tools
Clinical Info Resource Network
Clinical Monitoring System
Enrollment Application System
Equipment/ Turn-in Request
Gen. Med.Rec. - Generator
Health Data and Informatics
ICR - Immunology Case Registry
Income Verification Match
Incomplete Records Tracking
Interim Mangement Support
Master Patient Index VistA
Missing Patient Reg (Original) A4EL
Order Entry/ Results Reporting
PCE Patient Care Encounter
Pharmacy Benefits Mangement
Pharmacy Data Management
Pharmacy National Database
Pharmacy Prescription Practice
Quality Assurance Integration
Quality Improvement Checklist
Radiology/ Nuclear Medicine
Release of Information - DSSI
Remote Order/ Entry System
Utility Management Rollup
CA Verified Components - DSSI
Vendor - Document Storage Sys
Visual Impairment Service Team ANRV
Voluntary Timekeeping National

ot appear in the list above. Please provide

--

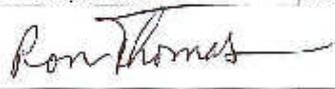
--

--

(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

(FY 2011) PIA: Final Signatures			
Facility Name:	Muskogee Regional Office Local Area Network (LAN)		
Title:	Name:	Phone:	Email:
Privacy Officer:	Joe Tillman	918-781-5655	jctillman@va.gov
			
Information Security Officer:	Ron Thomas	918-781-7517	ronald_thomas@va.gov
			
System Owner/ Chief Information Officer:	Kevin Causley	202-461-9170	kevin.causley@va.gov
Facility C O, Muskogee VARD	Eddie Koefe	202-781-7711	eddie.koefe@va.gov
			
Other Title: Field Liaison Staff	Mary Barley	202-461-9175	mary.barley@va.gov
Date of Report:	5/26/11		
OMB Unique Project Identifier	029-00-02-00-01-1120-00		
Project Name	Muskogee Regional Office Local Area Network (LAN)		

