(FY 2012) PIA: System Information	*Green Highlight = Must Answer Question		*Yellow Highlight = Required to Sign PIA
8	CDCO > AITC > VHA > VSSC Services > LAN		
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-02-00-01-1120-00		
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)"	The VHA Support Services Center (VSSC) LAN is a system comprised of servers, printers, Storage Area Networks (SAN), tape drives and switches that support the display of management reports to the Department of Veterans Affairs (VA). The vision of the VSSC is to create tools and knowledge that will foster the operation of high-value, high quality, safe, and patient-centered healthcare systems for Veterans. The system includes a wide variety of tools and applications including but not limited to SQL databases, SAS data processing systems, web presentation, and report utilities for analyzing data sets. The data provided by these reports assists management in VA medical centers and in Headquarters to better manage scarce veteran resources. Through its portal the VSSC: • Supports clinical and resource planning and operations based on unique patient data. • Provides extensive data analysis services, datasets, tools, and supporting documentation. • Provides data in the following domains: Advance Clinic Access, Capital and Planning, Customer Satisfaction, Quality & Performance, Resource Management, Special Populations & Clinical Programs, Special Projects, Workload, and Executive Summaries. • Provides extensive Customer Support options including on-line training resources, Help Desk, Newsletter, Subscription Ready Reports, Search capabilities, Frequently Asked Questions (FAQs), and numerous subject specific portals. The VSSC LAN is also host to the Homeless Operational, Management and Evaluation System (HOMES). HOMES is a new patient record system that is used to enter and track homeless Veteran data as they enter and move through our VA homeless system of care. Historically, when a Veteran entered the homeless program, the homeless staff was required to enter and then re-enter similar data whenever the Veteran transitioned to another level of care or homeless residential and case management programs. The HOMES system allows for a single entry that can be used to satisfy the Northeast Program Evaluation Center (NEPEC) requirements and the Computerized Patient Record System (CPRS). Any entry into the system will also be available to all homeless staff across all VISNs.		
Facility or Program Office Name:	Austin Information Technology Center (AITC)		
Title:	**Name:**	**Phone:**	**Email:**
Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov
Information Security Officer:	James Alden	781-687-2768	james.alden@va.gov
System Owner/Delegate:	David Kubacki	512-326-6408	david.kubacki@va.gov
Chief Information Officer:	David Kubacki	512-326-6408	david.kubacki@va.gov
Information Owner:			
Other Titles:			
Person Completing Document:	Analida Aguilar	512-326-6042	analida.aguilar@va.gov
Other Titles:			
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)			11/2010
What specific legal authorities authorize this program or system:	Title 38, United States Code, section 7301(a).		
What is the expected number of individuals that will have their PII stored in this system:			1,000,000-9,000,000
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.			14 years
Is there an authorized change control process which documents any changes to existing applications or systems?			◉ Yes ○ No ○ N/A : First PIA
If No, (Explain on Tab 8)			
Is there a contingency plan in place to process information when the system is down?			◉ Yes ○ No ○ N/A : First PIA
Has a PIA been completed within the last three years?			◉ Yes ○ No ○ N/A : First PIA
FISMA QUESTIONS			
1. Is this a new system?	○ Yes ◉ No		
2. Does this system contain Federal information in identifiable form?	◉ Yes ○ No		
3. Does the system include information on the public?	◉ Yes ○ No		
4. Is there a Privacy Impact Assessment (PIA) that covers this system?	◉ Yes ○ No ○ National Security System under 40 U.S.C. 11103, a PIA is not required for this system		

5. Is Federal-owned information in this system retrieved by name or unique identifier?	◉ Yes ○ No			
6. What is the System of Records Notice (SORN) for this system?	121VA19			
7. Has this SORN been reviewed or updated within the last three years?	Yes three years ago			
Date of Report (MM/YYYY):			1-Feb-12	
Any check mark in the boxes below will require a full PIA. Please continue to the next TAB and complete the remaining questions.				
If there is no Personally Identifiable Information on your system , please complete TAB 2 & TAB 12. (See Comment for Definition of PII)				
☑ 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?				
Directions				

(FY 2012) PIA: System of Records

*Green Highlight = Must Answer Question

1. Is a SORN (System of Records Notice) Required? — (●) Yes ( ) No ( ) Not Sure
2. Is there a SORN already in place? — (●) Yes ( ) No

***If Yes, select all of the appropriate SORN number(s):
***If Not Sure, contine to question 3

***Click to add. Delete SORN by highlighting SORN and comma if included and press the Delete key or place focus on area to delete all SORNs.

LIST OF SORN NUMBER(S) : 121VA19

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

3. If records are retrieved using any of the following entities, A SORN will be required (Please check all that apply)

- [x] Full Name
- [ ] Maiden Name
- [ ] Mother's Maiden Name
- [ ] Alias
- [x] Social Security Number
- [ ] Passport Number
- [ ] Driver's License Number
- [x] Taxpayer Identification Number
- [ ] Financial Account Number
- [ ] Credit Card Number
- [x] Street Address
- [ ] Email Address
- [ ] Photographic Image
- [ ] Fingerprints
- [ ] Handwriting
- [ ] Other Biometric Data
- [x] Other (Explain on Tab 8)

4. Based on Question 3, is a SORN required? — (●) Yes ( ) No

***If Yes, has the process begun to obtain/acquire a SORN — ( ) Yes (●) No

Location where the specific applicable System of Records Notice may be accessed: http://www.rms.oit.va.gov/SOR_Records.asp

(FY 2012) PIA: Data Collection And Storage *Green Highlight = Must Answer Question

Please fill in each column for the data types selected.

Data Type	Collection Method	What are the subjects told about the intended use of their information?	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)	Electronic/File Transfer	See Tab 8	Provided By Another System	Provided By Another System
Family Relation (spouse, children, parents, grandparents, etc)	Electronic/File Transfer	See Tab 8	Provided By Another System	Provided By Another System
Service Information	Electronic/File Transfer	See Tab 8	Provided By Another System	Provided By Another System
Medical Information	Electronic/File Transfer	See Tab 8	Provided By Another System	Provided By Another System
Criminal Record Information	N/A	N/A	N/A	N/A
Guardian Information	N/A	N/A	N/A	N/A
Education Information	Electronic/File Transfer	See Tab 8	Provided By Another System	Provided By Another System
Benefit Information	Electronic/File Transfer	See Tab 8	Provided By Another System	Provided By Another System
Other (Explain on Tab 8)	N/A	N/A	N/A	N/A

Data Type	Storage Method	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	(●) Yes ( ) No	VA Files/Databases (see Tab 8)	(●) Mandatory ( ) Voluntary	Automated
Family Relation (spouse, children, parents, grandparents, etc)	(●) Yes ( ) No	VA Files/Databases (see Tab 8)	(●) Mandatory ( ) Voluntary	Automated
Service Information	(●) Yes ( ) No	VA Files/Databases (see Tab 8)	(●) Mandatory ( ) Voluntary	Automated
Medical Information	(●) Yes ( ) No	VA Files/Databases (see Tab 8)	(●) Mandatory ( ) Voluntary	Automated
Criminal Record Information	( ) Yes (●) No		(●) Mandatory ( ) Voluntary	
Guardian Information	( ) Yes (●) No		(●) Mandatory ( ) Voluntary	
Education Information	(●) Yes ( ) No	VA Files/Databases (see Tab 8)	(●) Mandatory ( ) Voluntary	Automated
Benefit Information	(●) Yes ( ) No	VA Files/Databases (see Tab 8)	(●) Mandatory ( ) Voluntary	Automated
Other (Explain on Tab 8)	( ) Yes (●) No		(●) Mandatory ( ) Voluntary	

	(Please Select Yes/No)
Proximity and Timing: Is the privacy notice provided at the time of data collection?	( ) Yes (●) No
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	( ) Yes (●) No
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	( ) Yes (●) No
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	( ) Yes (●) No
routine use(s)	

(FY 2012) PIA: Data Sharing
*Green Highlight = Must Answer Question

** Any connection external to VA requires an ISA/MOU per VA 6500. This section below must be consistent with your System Security Plan Interconnection Security Agreement section.

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	See Tab 8	(●) Yes ( ) No	Other (Explain in Tab 8)	(●) Yes ( ) No	N/A
Other Veteran Organization	N/A	(●) Yes ( ) No		( ) Yes (●) No	
Other Federal Government Agency	Department of Defense, US Air Force	(●) Yes ( ) No	Other (Explain in Tab 8)	(●) Yes ( ) No	N/A
State Government Agency	N/A	(●) Yes ( ) No		( ) Yes (●) No	
Local Government Agency	N/A	(●) Yes ( ) No		( ) Yes (●) No	
Research Entity	N/A	(●) Yes ( ) No		( ) Yes (●) No	
[ ] Other Project/ System (Explain on Tab 8)					

(FY 2012) PIA: Access to Records

Does the system gather information from another system?	(●) Yes ( ) No	
Please enter the name of the system:	Veterans Health Information Systems and Technology Architecture (VistA), VA's Pharmacy Benefits Management (PBM), VA's Office of Enterprise Architecture Management (OEAM)	

(FY 2012) PIA: Secondary Use

Will PII data be included with any secondary use request?	( ) Yes (●) No	[ ] Mental Health	[ ] HIV	[ ] Drug/Alcohol Counseling	
Check all that apply		[ ] Sickle Cell	[✓] Other (Explain on Tab 8)	[ ] Research	

(FY 2012) PIA: Records Management *Green Highlight = Must Answer Question

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?

○ Yes (Explain on Tab 8) ◉ No

Is the data collected to only what is necessary to provide requested service?

◉ Yes ○ No (Explain on Tab 8)

Has the data provided been verified as complete?

☐ Veteran Verified ☑ Received From Database ☐ Verification Unknown

(FY 2012) PIA: Retention & Disposal

What is the data retention period?

Records are disposed of in accordance with GRS 20, which provides for deletion of data files when the agency determines that files are no longer needed for administrative, legal, audit, or other operationl purposes. (see tab 8)

RCS 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf

RCS VB-1, Part II Revised for VBA: www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/part2.pdf

National Archives and Records Administration: www.nara.gov

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

Answer: Information is needed for the indicated RCS 10-1 retention period for operational purposes in support of VHA's healthcare operations, management, oversight, performance and evaluation.

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

Answer: VA Directive and Handbook 6300, Records and Information Management, contains the policies and responsibilities for creation, collection, maintenance, use, disposition, protection, and release and exchange of record information. VA Handbook 6300.1, Records Management Procedures, Chapter 6 - describes the VA's Record Disposition Program.

Where are these procedures documented?

Answer: VA Directive 6300, VA Handbook 6300.1, VA Directive and Handbook 6500, NARA guidance for Electronic Records Management.

How are data retention procedures enforced?

Answer: Per VA Directive 6300, is the responsibility of the VA Chief Information Officer (CIO) to establish policies and procedures for administering the Records Management (RM) program; to establish, coordinate, and maintain a VA-wide RM program to ensure that all records, including electronic and microform media, and information are received, created, maintained, protected, released, and disposed of as required by the laws and regulations established by VA Dir 6300. VA Handbook 6300.1, Records Management Procedures, contains mandatory VA procedures for the proper management of records effectively and efficiently throughout their llfe cycle. Procedures are enforced by Records Management staff and VA Records officers.

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

◉ Yes ○ No (Explain on Tab 8)

(FY 2012) PIA: Children's Online Privacy Protection Act (COPPA)

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

○ Yes (Explain on Tab 8) ◉ No

(FY 2012) PIA: Security *Green Highlight = Must Answer Question

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	○ No (Explain on Tab 8)
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	◉ Yes	○ No (Explain on Tab 8)
Is security monitoring conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	◉ Yes	○ No (Explain on Tab 8)
Is security assessment conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	◉ Yes	○ No (Explain on Tab 8)
Is adequate physical security in place to protect against unauthorized access?	◉ Yes	○ No (Explain on Tab 8)

*Ensure PE 2, PE-3, PE-6, PE-7, PE-8 have been addressed appropriately for your categorization

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

☐ Biological Release	☐ Fire	☐ Lightning Strike	☐ Terrorist
☐ Blizzard	☐ Flood	☐ Malicious Code	☐ Thunderstorm
☐ Burglary/Break In	☐ Hacker, Cracker	☑ Password Privacy Negligence	☐ Tornado
☐ Civil Unrest	☐ Hail	☐ Personnel Unavailable	☐ Tsunami
☑ Component Failure	☐ HAZMAT Release/Spill	☐ Power Failure	☐ User Negligence
☐ Dam Failure	☐ Human Health Emergency	☐ Sabotage	☐ User Sabotage
☐ Dust/Debris	☐ Hurricane	☐ System Intrusion, Break-Ins	☐ Vibration
☐ Earthquake	☐ HVAC Failure	☑ System Misconfiguration	☐ Volcano
☐ Extreme Cold	☐ Indoor Humidity	☐ System Penetration	☐ Water Damage
☐ Extreme Heat	☐ Landslide	☐ System Tampering	☐ Winter Weather Hazards

*If any other risks identified, explain in Tab 8

Based upon the risks identified above, Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

☑ Access Control	☑ Configuration Management	☑ Media Protection	☑ System and Services Acquisition
☑ Audit and Accountability	☑ Contingency Planning	☑ Personnel Security	☑ System and Communication Protection
☑ Awareness and Training	☑ Identification and Authentication	☑ Physical and Environmental Protection	☑ System and Information Integrity
☑ Security Assessment and Authorization	☑ Incident Response	☑ Risk Assessment	☑ Planning ☑ Maintenance

Answer: (Other Controls) Explain on Tab 8

PIA: PIA Assessment

Based upon NIST 800-60, volume II; List the Information data types chosen as a basis for your FIPS 199 System Categorization.

Answer: Population Health Mgmt & Consumer Safety, Health Care Administration, Health Care Research and Practitioner Education, General Purpose Data and Statistics, Knowledge Dissemination, Capital Planning, Strategic Planning

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 minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

(FY 2012) 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.

Tab 3, line 25: This data is collected electronically from VistA. PII data that is collected would be name, address, SSNs, medical benefit and eligibility information, information related to medical examination or treatment, diagnoses, medical facilities providing examination or treatment, information related to military service and status, Veteran homeless program, patient aggregate workload data such as admissions, discharges, and outpatient visits, resource utilization such as laboratory tests, x-rays, etc. All data collected is for the purpose of healthcare operations, management, oversight, performance and evaluation. **Tab 4, lines 7, 11, 13:**
VSSC does not collect PII from individuals but uses PII already collected from Privacy Act compliant systems. VSSC electronically receives SAS files from VistA systems that contain PII for use with the VSSC system. **Tab 4, lines 29, 31, 33, 35, 43:** VSSC collects information from numerous VA sources as specified in the SORN, primarily from VA Medical Centers through VistA. VistA is the source of data for many VHA datasets such as: VHA Medical SAS datasets, VHA Decision Support System (DSS) National Data extracts, Pharmacy Benefits Management (PBM) data, and VISN data warehouses.

Tab 5, line 4:
Through its portal, the VSSC provides access to a broad range of data with the main purpose of delivering services, information, and analysis to VBA and VHA customers in areas such as business operations, capital and planning, clinical care, customer service, quality and performance, resource management, and special focus programs. In the delivery of these services, VSSC shares information with numerous VA entities, such as the Veterans Benefits Administration (VBA), the VA Research Division of the Office of Public Health, VHA Center for Engineering & Occupational Health (CEOSH), VHA Office of Quality and Performance (OQP), VHA Office of Patient Care Services (PCS).

Tab 5, line 8:
Data that is transferred includes the following: enrollee and patient demographics (excluding patient names and real social security numbers); purchased care data including type of healthcare resource purchased, volume of resource purchased, dollars spent and vendor name; in-house AF and VA workload for inpatients and outpatients including diagnoses, discharges and encounters and physician staffing numbers by provider specialty.

Tab 6, line 16:
Data in VSSC and data used to create reports come from other core sources. If needed, the amalgamate of data can be re-built from the original sources, making retention a less crucial issue. There is not an operating procedure covering a data retention period. Instead, discretion is left up to the individual programmers and their assessment of the individual products as to how much history to maintain.

(FY 2012) 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)
Agent Orange		Automated Medical Information System (AMIS)290
Appraisal System	Centralized Property Tracking System	Automated Standardized Performace Elements Nationwide (ASPEN)
ASSISTS	Common Security User Manager (CSUM)	Broome Closet
Awards	Compensation and Pension (C&P)	Centralized Accounts Receivable System (CARS)
Baker System	Control of Veterans Records (COVERS)	Committee on Waivers and Compromises (COWC)
Bbraun (CP Hemo)	Courseware Delivery System (CDS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
	Dental Records Manager	Compensation & Pension Training Website
	Education Training Website	
C&P Payment System	Electronic Appraisal System	Distribution of Operational Resources (DOOR)
C&P Training Website	Electronic Card System (ECS)	Educational Assistance for Members of the Selected Reserve Program CH 1606
CONDO PUD Builder	Electronic Payroll Deduction (EPD)	Electronic Performance Support System (EPSS)
	Eligibility Verification Report (EVR)	Enterprise Wireless Messaging System (Blackberry)
	Fiduciary Beneficiary System (FBS)	Financial Management Information System (FMI)
EndoSoft	Fiduciary STAR Case Review	Hearing Officer Letters and Reports System (HOLAR)
FOCAS	Financial and Accounting System (FAS)	Inquiry Routing Information System (IRIS)
Inforce	Insurance Unclaimed Liabilities	Modern Awards Process Development (MAP-D)
INS - BIRLS	Inventory Management System (IMS)	
Insurance Online	Interactive Voce Response (IVR)	Personal Computer Generated Letters (PCGL)
Insurance Self Service	LGY Centralized Fax System	Personnel Information Exchange System (PIES)
LGY Home Loans	Loan Service and Claims	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Guaranty Training Website	Purchase Order Management System (POMS)
MES		Reinstatement Entitlement Program for Survivors (REAPS)
Mobilization	Mental Health Assistant	Reserve Educational Assistance Program CH 1607
Montgomery GI Bill	National Silent Monitoring (NSM)	RightFax
MUSE	Powerscribe Dictation System	Service Member Records Tracking System
Omnicell	Rating Board Automation 2000 (RBA2000)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Records Locator System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Remittance Processing System	Training and Performance Support System (TPSS)
Right Now Web	Review of Quality (ROQ)	VA Online Certification of Enrollment (VA-ONCE
SAHSHA	Search Participant Profile (SPP)	VA Reserve Educational Assistance Program
Script Pro	Spinal Bifida Program Ch 18	
SHARE	State Benefits Reference System	Veterans Assistance Discharge System (VADS)
Sidexis	State of Case/Supplemental (SOC/SSOC)	Veterans Exam Request Info System (VERIS)
Synquest	Telecare Record Manager	Veterans Insurance Claims Trancking and Response System (VICTARS)
	VBA Enterprise Messaging System	Veterans Service Representative (VSR) Advisor
VBA Training Academy		Vocational Rehabilitation & Employment (VR&E) CH 31
Veterans Canteen Web		
VETSNET Housekeeping	Web Electronic Lender Identification	Web Automated Folder Processing System (WAFPS)
		Web Automated Reference Material System (WARMS)
VR&E Training Website		Web Automated Verification of Enrollment
Web LGY		Web-Enabled Approval Management System (WEAMS)
		Web Service Medical Records (WebSMR)
		Work Study Management System (WSMS)

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

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

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

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

(FY 2012) PIA: Minor Applications A-M

Which of these are sub-components of your system?

1184 Web	**Citrix**	**Electronic Signature**	**Imaging**
A4P	**Clinical Case Registries**	**Embedded Fragment Registry**	**Incentive Awards**
ACCu Care	**Clinical Data Repository/Health Data Repository**	**ENCORE 2**	**Incident Reporting**
ACCU Check	**Clinical Info Resource Network**	**ENDSOFT**	**Income Verification Match**
ACCU Med	**Clinical Monitoring System**	**Engineering**	**Incomplete Records Tracking**
Adobe Acrobat	**Clinical Notes Templates**	**Enrollment Application System**	**Inpatient Medications**
ADP Planning (PlanMan)	**Clinical Procedures**	**Enterprise Terminology Server & VHA Enterprise Terminology Services**	**Intake/ Output**
ADT	**Clinical Reminders**	**ePROMISE**	**Integrated Billing**
Adverse Reaction Tracking	**Clippership**	**Equipment/ Turn-in Request**	**Integrated Patient Funds**
Agent Cashier	**Combat Veteran Outreach**	**Event Capture**	**Interim Mangement Support**
Air Fortress	**Committee on Waiver and Compromises**	**Event Driven Reporting**	**Inventory Management System**
ASISTS	**Consult/ Request Tracking**	**Extensible Editor**	**Kernal**
Authorization/ Subscription	**Controlled Correspondence**	**External Peer Review**	**Kids**
Auto Instrument	**Controlled Substances**	**EYECAP**	**KOWA**
Auto Replenishment/ Ward Stock	**CP&E**	**Fee Based Claims System**	**Lab Service**
AUTOCAD	**CPRS**	**Fee Basis**	**Laboratory Electronic Data Interchange**
Automated Access Request	**CPT/ HCPCS Codes**	**Financial and Accounting System (FAS)**	**Letterman**
Automated Info Collection Sys	**Credentials Tracking**	**Financial Management System (FMS)**	**Lexicon Utility**
Automated Lab Instruments	**Credit Card Authentication**	**Functional Independence**	**Library**
Automated Med Info Exchange	**Data Innovations**	**Gen. Med. Rec. - I/O**	**List Manager**
Automated Sales Reporting	**DELIVEREX**	**Gen. Med. Rec. - Vitals**	**Lynx Duress Alarm**
AutoMed	**Dental**	**Gen. Med.Rec. - Generator**	**Mailman**
Bad Code Med Admin	**DICTATION-Power Scribe**	**GENDEX**	**MCCR National Database**
Barcode Medication Administration Contingency Plan (BCU)	**Dietetics**	**Generic Code Sheet**	**Meadows (MDWS)**
BCMA Contingency Workstations	**Discharge Summary**	**Genesys**	**Medicine**
BDN 301	**DRG Grouper**	**Get Well Networks**	**Mental Health**
Beneficiary Travel	**DRM Plus**	**GMED**	**MHTP**
Big Fix	**Drug Accountability**	**GRECC**	**MICOM**
CA Vertified Components - DSSI	**DSIT**	**Health Data and Informatics**	**Microsoft Exchange E-mail System**
Capacity Management - RUM	**DSS Extracts**	**Health Level Seven**	**Military/Vet Eye Injury Registry**
Capacity Management Tools	**DSS Quadramed**	**Health Summary**	**Minimal Patient Dataset**
CAPRI	**EDS Whiteboard (AVJED)**	**Health Summary Contingency**	**Missing Patient Reg (Original) A4EL**
Cardiff Teleform	**Education Tracking**	**HINQ**	**Mumps AudioFAX**
Cardiology Systems (stand alone servers from the network)	**EEO Complaint Tracking**	**Hospital Based Home Care**	**MyHealthEVet**
Care Management	**EKG System**	**ICB**	
CareTracker	**Electronic Card System (ECD)**	**ICR - Immunology Case Registry**	
CHECKPOINT	**Electronic Payroll Deduction (EPD)**	**IFCAP**	

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 2012) PIA: VISTA Minor Applications N-Z

Which of these are sub-components of your system?

National Cemetery Association	**Pharmacy Data Management**	**Scanning Exam and Evaluation System**	**VBECS**
National Drug File	**Pharmacy National Database**	**Scheduling**	**VDEF**
National Laboratory Test	**Pharmacy Prescription Practice**	**Security Suite Utility Pack**	**Vendor - Document Storage Sys**
NDBI	**PICIS OR**	**Sentillion**	**Veterans Canteen Web**
Network Health Exchange	**Police & Security**	**Shift Change Handoff Tool**	**Veterans Information Solution**
NOAHLINK	**Problem List**	**ShoreTel**	**VHAHUNAPP1**
NOIS	**Progress Notes**	**Social Work**	**VHAHUNFPC1**
Nursing Service	**Prosthetics**	**Stellant**	**VHS & RA Tracking System**
Occurrence Screen	**Purchase Order Management System**	**Stentor**	**Visit Tracking**
Omnicell	**Pyxis**	**Surgery**	**VISTA RAD**
Oncology	**Q-Matic**	**Survey Generator**	**VISTA RO**
Onvicord (VLOG)	**QMSI Prescription Processing**	**Telecare Record Manager**	**VistALink**
Optifill	**Quality Assurance Integration**	**Temp Trak**	**VistALink Security**
Order Entry/ Results Reporting	**Quality Improvement Checklist**	**Text Integration Utilities**	**Visual Impairment Service Team ANRV**
Outpatient Pharmacy	**QUASER**	**Tickler Database**	**Vitria BusinessWare**
P2000 ROBOT	**Radiology/ Nuclear Medicine**	**Toolkit**	**VIXS**
PACS database	**RAFT**	**TopCon**	**Voluntary Timekeeping**
Patch Module	**RALS**	**TraceMaster**	**Voluntary Timekeeping National**
Patient Data Exchange	**Record Tracking**	**Tracking Continuing Education**	**WEB HINQ**
Patient Feedback	**Registration**	**Traumatic Brain Injury**	**Whiteboard**
Patient Representative	**Release of Information - DSSI**	**Unwinder**	**Women's Health**
PCE Patient Care Encounter	**Remote Order/ Entry System**	**Utility Management Rollup**	**Workload and Overtime**
Personal Computer Generated Letters	**RPC Broker**	**Utilization Review**	
Pharmacy Benefits Mangement	**Run Time Library**	**VA Conference Room Registration**	
	SAGG	**VA Fileman**	
	SAN	**VAMedSafe**	

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 2012) PIA: Final Signatures

*Green Highlight = Must Answer Question

Facility Name:	Austin Information Technology Center (AITC)		
Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov
Amy J. Howe Digital Signature Block	Digitally signed by Amy J. Howe DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=Employees, 0.9.2342.19200300.100.1.1=Amy.Howe1@va.gov, cn=Amy J. Howe Date: 2012.02.14 13:43:22 -06'00'		
Information Security Officer:	James Alden	781-687-2768	james.alden@va.gov
James B. Alden Digital Signature Block	Digitally signed by James B. Alden DN: CN = James B. Alden C = US O = U.S. Government OU = Department of Veterans Affairs Date: 2012.02.16 17:03:46 -05'00'		
System Owner/Delegate:	David Kubacki	512-326-6408	david.kubacki@va.gov
Digital Signature Block			
Chief Information Officer:	David Kubacki	512-326-6408	david.kubacki@va.gov
Digital Signature Block			
Other Titles:	0	0	0
Digital Signature Block			
Date of Report:	1-Feb-12		
OMB Unique Project Identifier	029-00-02-00-01-1120-00		
Project Name	CDCO > AITC > VHA > VSSC Services > LAN		

The Signature Process:

- Complete the PIA form.
- Name the PIA Excel FORM [“FY12-Region # - Facility Name - Facility # -Date(mmddyyyy).xls”]
- Example: “FY12-Region3-Lexington VAMC-596-10302008.xls”
- Submit the completed PIA Excel form to SMART Database.
- Fix errors the reviewers sent back, rename the file and submit to SMART Database
- If no errors, convert form into PDF with Nuance PDF Professional.
- Name the PIA PDF form [“FY12-Region #-Facility Name- Facility # -Date(mmddyyyy).xls”]
- Obtain digital signatures on the “Final Signatures tab”
- Submit signed PIA PDF form to the SMART Database.

(FY 2012) PIA: Final Signatures

*Green Highlight = Must Answer Question

Facility Name:	0		
Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	Amy.Howe1@va.gov
Digital Signature Block			
Information Security Officer:	0	0	0
Digital Signature Block			
System Owner/Delegate:	David Kubacki	512-326-6408	David.Kubacki@va.gov
Chief Information Officer:	David Kubacki	512-326-6408	David.Kubacki@va.gov
Other Titles:	0	0	0
Digital Signature Block			
Date of Report:	0-Jan-00		
OMB Unique Project Identifier	0		
Project Name	00000		

James B. Alden

Digitally signed by: James B. Alden
DN: CN = James B. Alden C = US O = U.S. Government OU = Department of Veterans Affairs
Date: 2012.02.16 17:11:01 -05'00'