

(FY 2012) PIA: System Information	*Green Highlight = Must Answer Question	*Yellow Highlight = Required to Sign PIA	
Program or System Name (as shown in SMART):	MINOR APPLICATIONS > AITC> IFCAP		
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-01-11-01-1180-00		
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)"	<p>The IFCAP Server for Austin (IFC) consists of 3 applications or modules which utilize the VA VISTA legacy application. These are VA-wide systems, and IFC is the local Austin Information Technology Center (AITC) instance of these enterprise applications. The applications (or modules) in use locally at AITC currently include:</p> <p>1) AEMS-MERS - Engineering module, also known as Automated Engineering Management System/Medical Equipment Reporting System (AEMS/MERS), facilitates the management of information needed to effectively discharge key operational responsibilities normally assigned to VA facilities engineering organizations:</p> <ul style="list-style-type: none"> • Equipment Management • Work Control • Space/Facility Management • Project Planning and Submission • Project Tracking <p>The Engineering module is a resource that can be shared by medical center administrative staff. It safeguards against unauthorized editing of key data elements of non-expendable (NX) equipment records. Engineering maintains integration agreements with Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP), such that the status of work orders is automatically updated on the basis of orders for parts or service. The Engineering package or AEMS/MERS is also the VA's official record of inventory for capitalized personal property.</p> <p>2) IFCAP - The Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP) module automates a spectrum of VA financial activities. VA employees use IFCAP to manage budgets, order goods and services, maintain records of available funds, determine the status of a request, compare vendors and items to determine the best purchase, record the receipt of items into the warehouse, and pay vendors. IFCAP automates the written regulations and policy for VA funding and procurement. That is, it defines the formal transactions, orders, and payment actions to be taken on requests for goods and services. IFCAP provides information on supplies, equipment, vendors, procurement history, and control point activity.</p> <p>3) ETA - The Enhanced Time and Attendance System (ETA) automates time and attendance for employees, timekeepers, payroll, and supervisors. It provides employees the ability to request leave and display both the status of pending requests and leave balances and allows payroll to manage time and leave (T&L) units and tours of duty. It also provides timekeeping, supervisory certification, and overtime management.</p>		
Facility or Program Office Name:	Austin Information Technology Center (AITC)		
Title:	Name:	Phone:	
Privacy Officer:	Amy Howe	512-326-6217	Email: amy.howe1@va.gov
Information Security Officer:	Griselda Gallegos	512-326-6037	griselda.gallegos@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: System Administrator	Rolando Munoz	512-326-6253	rolando.munoz@va.gov
Person Completing Document:	Steven Bjarnason	512-326-7874	steven.bjarnason@va.gov
Other Titles: Project Manager	Linda Elsby	512-326-6677	linda.elsby@va.gov
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)	02/2009		
What specific legal authorities authorize this program or system: 2. System Information	<p>Vista (the overarching environment for the local instances of AEMS-MERS, IFCAP, and ETA modules): SORN cites 38 USC Sec 7301(a).</p> <p>AEMS-MERS module: 41 CFR 101 (Federal Property Management Regulations), Part 101-11 (Creation, Maintenance, and Use of Records), Sec. 103 (Procedures)</p> <p>IFCAP module: Federal Acquisition Regulation (FAR) and 41 USC 4 (Procurement Procedures)</p> <p>ETA module: 5 USC 55 (Pay Administration) Secs 5501 through 5597; 31 USC 33 - Sections 3327 (Depositing, Keeping, and Paying Money) and 3321 (Disbursing Authority in the Executive Branch); and 5 CFR 531 (Pay Under the General Schedule). The PAID system (the Major Application parent of ETA) SORN cites: Statutory provisions, Executive Order 12191 (45 FR 7997 (Feb. 6, 1980)) and other Executive Orders of the President, and rules and regulations of certain Federal regulatory departments and agencies.</p>		

What is the expected number of individuals that will have their PII stored in this system:	~ 2400 users (consisting of VistA users of CDCO instances for the AEMS-MERS, IFCAP, and ETA modules)		
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.	> 15 years		
Is there an authorized change control process which documents any changes to existing applications or systems?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> 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?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA		
Has a PIA been completed within the last three years?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA		
FISMA QUESTIONS			
1. Is this a new system?	<input type="radio"/> Yes <input checked="" type="radio"/> No		
2. Does this system contain Federal information in identifiable form?	<input checked="" type="radio"/> Yes <input type="radio"/> No		
3. Does the system include information on the public?	<input checked="" type="radio"/> Yes <input type="radio"/> No		
4. Is there a Privacy Impact Assessment (PIA) that covers this system?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> 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?	<input checked="" type="radio"/> Yes <input type="radio"/> No		
6. What is the System of Records Notice (SORN) for this system?	79VA19 , 27VA047		
7. Has this SORN been reviewed or updated within the last three years?	Yes two years ago		
Date of Report (MM/YYYY):	4-Jan-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)			
<input type="checkbox"/> Have any changes been made to the system since the last PIA?			
<input type="checkbox"/> Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?			
<input checked="" type="checkbox"/> Will this system/application/program retrieve information on the basis of name, unique identifier, symbol or other PII data?			
<input checked="" type="checkbox"/> Does this system/application/program collect, store, or disseminate PII/PHI data?			
<input checked="" type="checkbox"/> 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?
- 2. Is there a SORN already in place?

Yes No Not Sure

Yes No

***If Yes, select all of the appropriate SORN number(s):
 ***If Not Sure, continue 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) :

79VA19 , 27VA047

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)

<input checked="" type="checkbox"/> Full Name
<input type="checkbox"/> Maiden Name
<input type="checkbox"/> Mother's Maiden Name
<input checked="" type="checkbox"/> Alias
<input checked="" type="checkbox"/> Social Security Number
<input type="checkbox"/> Passport Number
<input type="checkbox"/> Driver's License Number
<input checked="" type="checkbox"/> Taxpayer Identification Number
<input checked="" type="checkbox"/> Financial Account Number
<input checked="" type="checkbox"/> Credit Card Number
<input checked="" type="checkbox"/> Street Address
<input checked="" type="checkbox"/> Email Address
<input type="checkbox"/> Photographic Image
<input type="checkbox"/> Fingerprints
<input type="checkbox"/> Handwriting
<input type="checkbox"/> Other Biometric Data
<input type="checkbox"/> Other (Explain on Tab 8)

- 4. Based on Question 3, is a SORN required?

Yes No

Yes No

***If Yes, has the process begun to obtain/acquire a SORN

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)	Paper & Electronic	Payments	Verbal	Automated
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	N/A			
Medical Information	N/A			
Criminal Record Information	N/A			
Guardian Information	N/A			
Education Information	N/A			
Benefit Information	N/A			
Other (Explain on Tab 8)				

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)	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Files/Databases (Identify File)	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Verbally
Family Relation (spouse, children, parents, grandparents, etc)	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Service Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Medical Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Criminal Record Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Guardian Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Education Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Benefit Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Other (Explain on Tab 8)	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated

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

(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	VA Financial Service Center (FSC)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Other (Explain in Tab 8)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Internal
Other Veteran Organization		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Other Federal Government Agency		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
State Government Agency		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Local Government Agency		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Research Entity		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
<input type="checkbox"/> Other Project/ System (Explain on Tab 8)					
(FY 2012) PIA: Access to Records					
Does the system gather information from another system?		<input checked="" type="radio"/> Yes <input type="radio"/> No			
Please enter the name of the system:		AEMS-MERS module: No PII (interfaces to IFCAP module of the Vista instance at AITC) IFCAP module: No PII (interfaces to Financial Management System (FMS) and AEMS-MERS (AITC instance)) ETA module: interface to Personnel and Accounting Integrated Data (PAID) System			
(FY 2012) PIA: Secondary Use					
Will PII data be included with any secondary use request?		<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="checkbox"/> Mental Health	<input type="checkbox"/> HIV	<input type="checkbox"/> Drug/Alcohol Counseling
Check all that apply		<input type="checkbox"/> Sickle Cell	<input type="checkbox"/> Other (Explain on Tab 8)	<input type="checkbox"/> 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?			
<input type="radio"/> Yes (Explain on Tab B) <input checked="" type="radio"/> No			
Is the data collected to only what is necessary to provide requested service?			
<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab B)			
Has the data provided been verified as complete?			
<input type="checkbox"/> Veteran Verified <input checked="" type="checkbox"/> Received From Database <input type="checkbox"/> Verification Unknown			
(FY 2012) PIA: Retention & Disposal			
What is the data retention period?			
Vista environment: User login ID's (aka Unique Identifiers), which are composed of Social Security Numbers (SSN) correlating to specific users/names, are stored until the corresponding account is removed from the system. Note: A limited number of personnel who have the appropriate menus, security keys, and system rights are able to view the UID.		RCS 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf	
ETA module: PII resides in the database for an indefinite period. Accounts are deactivated when personnel separate but the contents of the account (data containing PII) remain in tact and accounts are not currently removed.		RCS VB-1, Part II Revised for VBA:	
AEMS-MERS and IFCAP modules: do not store, process, or transmit PII.		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: Since the Master record for all ETA data is contained in the PAID system, there should be no reason for inactive records to exist beyond 30 days following separation of personnel. Guidance has not been provided to system administrator for the destruction/archiving procedures of inactive records to be in accordance with VA Office of Information and Technology (OI&T) Records Control Schedule (RCS) 005-1, Part I, Sections A and B.			
What are the procedures for eliminating data at the end of the retention period?			
Answer: Procedures do not exist.			
Where are these procedures documented?			
Answer: Procedures do not exist.			
How are data retention procedures enforced?			
Answer: Procedures do not exist, therefore the provisions of the retention schedules are not enforced.			
Has the retention schedule been approved by the National Archives and Records Administration (NARA)			
<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab B)			
(FY 2012) PIA: Children's Online Privacy Protection Act (COPPA)			
Will information be collected through the internet from children under age 13?			
<input type="radio"/> Yes (Explain on Tab B) <input checked="" type="radio"/> 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.	<input type="radio"/> Yes	<input checked="" type="radio"/> 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..	<input type="radio"/> Yes	<input checked="" type="radio"/> No (Explain on Tab 8)
Is security monitoring conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input type="radio"/> Yes	<input checked="" type="radio"/> No (Explain on Tab 8)
Is security assessment conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input type="radio"/> Yes	<input checked="" type="radio"/> No (Explain on Tab 8)
Is adequate physical security in place to protect against unauthorized access?	<input checked="" type="radio"/> Yes	<input type="radio"/> 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)

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

<input type="checkbox"/> Access Control	<input type="checkbox"/> Configuration Management	<input type="checkbox"/> Media Protection	<input type="checkbox"/> System and Services Acquisition
<input type="checkbox"/> Audit and Accountability	<input type="checkbox"/> Contingency Planning	<input type="checkbox"/> Personnel Security	<input type="checkbox"/> System and Communication Protection
<input type="checkbox"/> Awareness and Training	<input type="checkbox"/> Identification and Authentication	<input type="checkbox"/> Physical and Environmental Protection	<input type="checkbox"/> System and Information Integrity
<input type="checkbox"/> Security Assessment and Authorization	<input type="checkbox"/> Incident Response	<input type="checkbox"/> Risk Assessment	<input type="checkbox"/> Planning
<input type="checkbox"/> 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:

Information derived from NIST SP 800-60, Vol 2: Central Property Management; Income Information; Facilities, Fleet & Equipment Management; Compensation Management; Benefits Management; Employee Performance; Logistics Management; Services Acquisition; and Inventory Control.

<p>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)</p>	<input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
<p>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)</p>	<input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
<p>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)</p>	<input checked="" type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> 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.

"4. Data Collection And Storage": The current "Privacy Act Statement" exhibited at logon to the system does not meet the requirements for a "Privacy Notice" for purpose, authority, and disclosures.

"5. Data Sharing & Access": All data shared is ONLY done so within the VA and all interconnected systems co-located within the AITC Datacenter as VA owned , operated, and managed systems.

"6. Records Management": The retention periods for PII are not compliant with VA and National requirements for data retention for personnel records. Currently there are thousands of inactive records containing PII, going back over a decade, for personnel that are no longer employed.

"7. Security" first 4 questions: It cannot be determined that the system is following IT security requirements and procedures since there isn't a current System Security Plan (SSP) or Risk Assessment. Without an SSP a security assessment and risk assessment cannot be performed. Risks to the system have not been documented and assessed to determine if mitigation is possible or that compensating controls might be required.

(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 Performance 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	
	Education Training Website	Compensation & Pension 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)	
Script Pro	Spinal Bifida Program Ch 18	VA Reserve Educational Assistance Program
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)
		Veterans Service Representative (VSR) Advisor
VBA Training Academy	VBA Enterprise Messaging System	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 Groupier	Get Well Networks	Mental Health	
Beneficiary Travel	DRM Plus	GMED	MHTP	
Big Fix	Drug Accountability	GRECC	MICOM	
CA Verified 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)	X 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	Automated Engineering Management System - Medical Equipment Reporting System (AEMS-MERS)			
Description	See "System Information" tab of the PIA			
Comments				
Is PII collected by this minor application?	NO			
Does this minor application store PII?	NO			
If yes, where?				
Who has access to this data?				
Name	Enhanced Time and Attendance System (ETA)			
Description	See "System Information" tab of the PIA			
Comments				
Is PII collected by this minor application?	YES			
Does this minor application store PII?	YES			
If yes, where? AITC Datacenter				
Who has access to this data? The associated individuals, supervisors, managers, human resources, payroll personnel and system administrator				
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
Onicord (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	

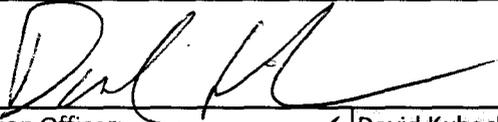
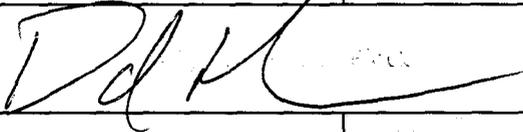
Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

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
Digital Signature Block			
Information Security Officer:	Griselda Gallegos	512-326-6037	griselda.gallegos@va.gov
Digital Signature Block			
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: System Administrator	Rolando Munoz	512-326-6253	rolando.munoz@va.gov
Digital Signature Block			
Date of Report:	4-Jan-12		
OMB Unique Project Identifier	029-00-01-11-01-1180-00		
Project Name	MINOR APPLICATIONS > AITC > IFCAP		
<p>The Signature Process:</p> <ul style="list-style-type: none"> • Complete the PIA form. • Name the PIA Excel FORM ["FY12-Region # - Facility Name - Facility # -Date(mmddyyyy).xls"] <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • If no errors, convert form into PDF with Nuance PDF Professional. • Name the PIA PDF form ["FY12-Region #-Facility Name- Facility # -Date(mmddyyyy).xls"] <ul style="list-style-type: none"> • 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		