

(FY 2012) PIA: System Information		*Green Highlight = Must Answer Question		*Yellow Highlight = Required to Sign PIA	
Program or System Name (as shown in SMART):		CDCO>AITC>VA>OM>PAID			
OMB Unique System / Application / Program Identifier (AKA: UPID #):		029-00-01-19-01-1330-00			
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)"		<p>PAID is an automated payroll application that processes bi-weekly salary and incentive checks for approximately 235,000 VA employees totaling \$320 million in net pay. Processing includes regulatory and individually authorized withholding deductions, leave balances, retirement, promotions, reassignments, bond and savings allotments. Employee master records are updated nightly to reflect promotions, reassignments, voluntary deductions, mandatory deductions, and employees' leave balances. The PAID system/application encompasses personnel, payroll, and related fiscal operations. This system is affected by the Office of Personnel Management (OPM) mandates; Federal and state legislation; executive orders; Office of Management and Budget (OMB) directives; and regulations of the Treasury Department, Internal Revenue Service (IRS), and the Social Security Administration (SSA). On-Line Data Entry (OLDE) is considered to be the "front-end" process to PAID. OLDE automates the manual code sheet processing by providing comprehensive data editing using the PAID Master Records (PMR). OLDE provides all VA stations the capability to enter, edit and correct PAID HR and Payroll transactions in an on-line interactive mode. Veterans Benefits Administration (VBA) inputs timecards through PAID OLDE. Veterans Health Administration (VHA), VA Central Office (VACO), AITC, and Financial Services Center (FSC) use the Enhanced Time &amp; Attendance System (ETA) to input timecards. FUM is a module of PAID that creates financial data sets for a smaller group of users. The PAID application gives the HR and fiscal offices direct and timely access to their personnel and payroll data stored at the Austin IT Center (AITC). Upon completion of the bi-weekly payroll processing, the PAID data and accounting master files are loaded to the Integrated Database Management System (IDMS). Authorized VA customers may access the database in an online query mode through a series of formatted screens. Through the extract file option, the customer can request that an extract data set be created containing the facility data they are authorized to view. The extract data sets can be browsed through the time-sharing option (TSO), transmitted to a personal computer, or inputted to batch programs executed on the AITC computers. In response to the President's mandate for e-Government, the VA is working with the Defense Finance and Accounting System (DFAS) personnel to move the processing of VA payroll to DFAS. This process entails a major modification to existing PAID applications and data sets. All changes required to accommodate the e-Payroll project (moving payroll processing to DFAS) are required to adhere to the same configuration change process as all other modifications to PAID.</p>			
Facility or Program Office Name:		Austin Information Technology Center (AITC)			
Title:		Name:		Phone:	
Privacy Officer:		Amy Howe		512-326-6217	
Information Security Officer:		Neil Cruz		(202) 461-6254	
System Owner/Delegate:		John Rucker		512-326-6422	
Chief Information Officer:		John Rucker		512-326-6422	
Information Owner:		Roy Coles		202-461-6105	
Other Titles: Program Manager		Linda Elsby		512-326-6677	
Person Completing Document:		Terry Armstrong		512-326-9674	
Other Titles:					
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)				08/2009	

PAID is a department-wide system that encompasses personnel, payroll, and related fiscal (3) VA Documents

- Department of Veterans Affairs, VA Handbook 6500, Cyber Security, December, 2003.
- Department of Veterans Affairs, VA Directive and Handbook 6214, VA Information Technology Security Certification and Accreditation Program (ITSCAP)
- VA Information Security Management Plan, October 10, 2000
- VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology, July 13, 2000
- VA Directive 6301, Electronic Mail Records, April 28, 2000

operations. The system is affected by the Office of Personnel Management (OPM) mandates; Federal and state legislation; executive orders; Office of Management and Budget (OMB) directives; and regulations of the Treasury Department, Internal Revenue Service (IRS), and Social Security Administration (SSA).

(1) National Level Documents

- Privacy Act, 5 United States Code 552a, 1974
- Computer Fraud and Abuse Act of 1986 (Public Law (P.L.) 99-474), 18 United States Code 1030
- Computer Security Act of 1987 (P.L. 100-235)
- Freedom of Information Act (P.L.93-579)
- PL 103-356, Government Management Reform Act, 1997
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191
- Clinger-Cohen Act of 1996 (P.L. 104-106), August 8, 1996
- 38 U.S.C. 3305, Confidentiality of Medial Records – Assurance Records
- 38 U.S.C 4132, Confidentiality of Certain Medical Records

(2) Other Government Regulations and Documents

- NIST Special Pub 800-12, An Introduction to Computer Security; The NIST Handbook.
- NIST Special Pub 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.
- NIST Special Pub 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998.

What specific legal authorities authorize this program or system:

What is the expected number of individuals that will have their PII stored in this system:	289261	
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.	Operational since 1965	
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	
<b>FISMA QUESTIONS</b>		
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	<input checked="" type="radio"/> Yes <input type="radio"/> No	
6. What is the System of Records Notice (SORN) for this system?	27VA047	
7. Has this SORN been reviewed or updated within the last three years?	Yes three years ago	
Date of Report (MM/YYYY):	16-Dec-11	
<b>Any check mark in the boxes below will require a full PIA. Please continue to the next TAB and complete the remaining questions.</b>		
<b>If there is no Personally Identifiable Information on your system, please complete TAB 2 &amp; TAB 12. ( See Comment for Definition of PII)</b>		
<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?			
<a href="#">Directions</a>			

(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?

<input checked="" type="radio"/> Yes	<input type="radio"/> No	<input type="radio"/> Not Sure
<input checked="" type="radio"/> Yes	<input type="radio"/> No	

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

27VA047

LIST OF SORN NUMBER(S) :

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 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?

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

	(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 checked="" type="radio"/> Yes <input type="radio"/> No
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	<input checked="" type="radio"/> Yes <input type="radio"/> No
<a href="#">routine use(s)</a>	

(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	VHA DHCPS	<input type="radio"/> Yes <input checked="" type="radio"/> No	Payments	<input type="radio"/> Yes <input checked="" type="radio"/> No	Other (Explain in Tab 8)
Other Veteran Organization	N/A	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Other Federal Government Agency	DFAS	<input type="radio"/> Yes <input checked="" type="radio"/> No	Compensation	<input type="radio"/> Yes <input checked="" type="radio"/> No	Other (Explain in Tab 8)
State Government Agency	State/City Govt	<input type="radio"/> Yes <input checked="" type="radio"/> No	Compensation	<input type="radio"/> Yes <input checked="" type="radio"/> No	Other (Explain in Tab 8)
Local Government Agency	State Govt	<input type="radio"/> Yes <input checked="" type="radio"/> No	Compensation	<input type="radio"/> Yes <input checked="" type="radio"/> No	Other (Explain in Tab 8)
Research Entity		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
<input checked="" 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:		DFAS, SSA, VHA DHCPS,			
(FY 2012) PIA: Secondary Use					
Will PII data be included with any secondary use request?		<input type="radio"/> Yes <input checked="" type="radio"/> No			
Check all that apply		<input type="checkbox"/> Mental Health	<input type="checkbox"/> HIV	<input type="checkbox"/> Drug/Alcohol Counseling	
		<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 8) <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 8)		
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?		
<p>PAID data is retained on line for all active VA employees at the AITC. After one Pay Period for a VA employee who is no longer an active employee and 26 Pay Periods for a DFAS employee, the data is archived on tape, transferred to a records facility for two more years, and disposed of in accordance with disposition authorization approved by the Archivist of the United States.</p>		
Explain why the information is needed for the indicated retention period?		
<p>Answer: The PAID data is used to process payroll data; sometimes corrections for past actions need to be accomplished.</p>		
What are the procedures for eliminating data at the end of the retention period?		
<p>Answer: Paper documents may be shredded or burned and record destruction is documented in accordance with NARA guidelines. Selected destruction methods for other data media comply with NCSC-TG-025 Version-2/VA Policy. If a degausser is not available, the media is destroyed by smelting, pulverization or disintegration. Other IT equipment and electronic storage media are sanitized in accordance with procedures of the NSA/Central Security Service Media Declassification and Destruction Manual and certified that the data has been removed or that it is unreadable. Certification identifies the Federal Information Processing (FIP) item cleared. FIP equipment is not excessed, transferred, discontinued from rental or lease, exchanged, or sold without certification.</p>		
Where are these procedures documented?		
<p>Answer: The disposition authority is documented in Record Control Schedule 10-1, Section XLIII-1 and XLIII-2. Disposition instructions and procedures for electronic media are documented in NCSC-TG-025 Version-2/VA Policy, VA Form 0751, Information Technology Equipment Sanitization Certificate.</p>		
How are data retention procedures enforced?		
<p>Answer: No records are disposed/destroyed without the approval of the facility's Record Control Manager. All records are disposed of in accordance with VA Policy and disposition authority (RCS 10-1). Archived and retired records are maintained in accordance with VA Policy.</p>		
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 8)		
(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 8) <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?  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)

<input checked="" type="checkbox"/> Biological Release	<input checked="" type="checkbox"/> Fire	<input checked="" type="checkbox"/> Lightning Strike	<input checked="" type="checkbox"/> Terrorism
<input type="checkbox"/> Blizzard	<input checked="" type="checkbox"/> Flood	<input checked="" type="checkbox"/> Malicious Code	<input checked="" type="checkbox"/> Thunderstorm
<input checked="" type="checkbox"/> Burglary/Break In	<input checked="" type="checkbox"/> Hacker, Cracker	<input checked="" type="checkbox"/> Password Privacy Negligence	<input checked="" type="checkbox"/> Tornado
<input checked="" type="checkbox"/> Civil Unrest	<input checked="" type="checkbox"/> Hail	<input checked="" type="checkbox"/> Personnel Unavailable	<input type="checkbox"/> Tsunami
<input checked="" type="checkbox"/> Component Failure	<input checked="" type="checkbox"/> HAZMAT Release/Spill	<input checked="" type="checkbox"/> Power Failure	<input checked="" type="checkbox"/> User Negligence
<input type="checkbox"/> Dam Failure	<input checked="" type="checkbox"/> Human Health Emergency	<input checked="" type="checkbox"/> Sabotage	<input checked="" type="checkbox"/> User Sabotage
<input checked="" type="checkbox"/> Dust/Debris	<input checked="" type="checkbox"/> Hurricane	<input checked="" type="checkbox"/> System Intrusion, Break-Ins	<input checked="" type="checkbox"/> Vibration
<input checked="" type="checkbox"/> Earthquake	<input checked="" type="checkbox"/> HVAC Failure	<input checked="" type="checkbox"/> System Misconfiguration	<input checked="" type="checkbox"/> Volcano
<input type="checkbox"/> Extreme Cold	<input checked="" type="checkbox"/> Indoor Humidity	<input checked="" type="checkbox"/> System Penetration	<input checked="" type="checkbox"/> Water Damage
<input checked="" type="checkbox"/> Extreme Heat	<input type="checkbox"/> Landslide	<input checked="" 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 checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Configuration Management	<input checked="" type="checkbox"/> Media Protection	<input checked="" type="checkbox"/> System and Services Acquisition
<input checked="" type="checkbox"/> Audit and Accountability	<input checked="" type="checkbox"/> Contingency Planning	<input checked="" type="checkbox"/> Personnel Security	<input checked="" type="checkbox"/> System and Communication Protection
<input checked="" type="checkbox"/> Awareness and Training	<input checked="" type="checkbox"/> Identification and Authentication	<input checked="" type="checkbox"/> Physical and Environmental Protection	<input checked="" type="checkbox"/> System and Information Integrity
<input checked="" type="checkbox"/> Security Assessment and Authorization	<input checked="" type="checkbox"/> Incident Response	<input checked="" type="checkbox"/> Risk Assessment	<input checked="" type="checkbox"/> Planning
			<input checked="" 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:

PAID is a legacy system that has been operational since 1965. Restricted access and security was part of the original design to maintain the integrity of financial data and vendor data. The system is 100% contained behind the firewall of the VA's Austin Information Technology Center. State of the art data security audits and safeguards are used to protect the systems that operate at this facility. Data can only be accessed by VA employees. The personnel accessing the data must complete all of the VA's required background checks and receive specific permission from their servicing Information Security Officer (ISO) before being granted the accesses required to view Privacy Information contained within PAID.

**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 5 Line 4** - Info passed is internal to VA and needed to process employee payroll.

**Tab 5 line 8** - e-Government Act of 2002

**Tab 5 line 10** - Transfer withholding tax info to effect payment of taxes to city and/or state governments and to create W-2's.

**Tab 5 line 12** - Transfer unemployment compensation information to State agencies to compile unemployment compensation data.

**Tab 5 line 16** - Transfer payroll info to credit quarterly posting for social security. Transfer retirement record info to provide a history of service and retirement deductions. Transfer personnel data to provide the OPM with a readily accessible major data source for meeting work force info needs of OPM, national planning agencies, the Congress, the White House, and the public. Employee Express (EEX) allows an employee to update their own personal information which is then transferred into the PAID application for payroll purposes. OPM mandated the establishment of certain employee benefits; this automated process exchanges limited employee data for employee to use those benefits.

(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 Tranking 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 Grouper	Get Well Networks	Mental Health
Beneficiary Travel	DRM Plus	GMED	MHPT
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)	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
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:	Neil Cruz	(202) 461-6254	neil.cruz@va.gov
Digital Signature Block			
System Owner/Delegate:	John Rucker	512-326-6422	John.Rucker@va.gov
Digital Signature Block			
Chief Information Officer:	John Rucker	512-326-6422	John.Rucker@va.gov
Digital Signature Block			
Other Titles: Program Manager	Linda Elsby	512-326-6677	Linda.Elsby@va.gov
Digital Signature Block			
Date of Report:	16-Dec-11		
OMB Unique Project Identifier	029-00-01-19-01-1330-00		
Project Name	CDCO>AITC>VA>OM>PAID		
<p>The Signature Process:</p> <ul style="list-style-type: none"> <li>• Complete the PIA form.</li> <li>• Name the PIA Excel FORM ["FY12-Region # - Facility Name - Facility # -Date(mmddyyyy).xls"] <ul style="list-style-type: none"> <li>• Example: "FY12-Region3-Lexington VAMC-596-10302008.xls"</li> <li>• Submit the completed PIA Excel form to SMART Database.</li> </ul> </li> <li>• Fix errors the reviewers sent back, rename the file and submit to SMART Database <ul style="list-style-type: none"> <li>• If no errors, convert form into PDF with Nuance PDF Professional.</li> </ul> </li> <li>• Name the PIA PDF form ["FY12-Region #-Facility Name- Facility # -Date(mmddyyyy).xls"] <ul style="list-style-type: none"> <li>• Obtain digital signatures on the "Final Signatures tab"</li> <li>• Submit signed PIA PDF form to the SMART Database.</li> </ul> </li> </ul>			

(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:	John Rucker	512-326-6422	John.Rucker@va.gov
Digital Signature Block 			
Chief Information Officer:	John Rucker	512-326-6422	John.Rucker@va.gov
Digital Signature Block 			
Other Titles:	0	0	0
Digital Signature Block			
Date of Report:	0-Jan-00		
OMB Unique Project Identifier	0		
Project Name	00000		