

## **Welcome to the PIA for FY 2011!**

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

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

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

### **Directions:**

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

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

PIA Website: [http://vawww.privacy.va.gov/Privacy\\_Impact\\_Assessments.asp](http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp)

### **Roles and Responsibilities:**

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

### **Definition of PII (Personally Identifiable Information)**

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

### **Macros Must Be Enabled on This Form**

**Microsoft Office 2003:** To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

**Microsoft Office 2007:** To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable

All Macros; 2) Click OK

**Final Signatures**

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

**Privacy Impact Assessment Uploaded into SMART**

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to [christina.pettit@va.gov](mailto:christina.pettit@va.gov) to received full credit for submission.

## (FY 2011) PIA: System Identification

Program or System Name: CDCO>AITC>VA>AITC>AITE Site and General Support System (GSS)  
 OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

Description of System/ Application/ Program: Operating under the organizational purview of the VA Office of Information and Technology (OI&T), the AITC GSS provides a full complement of technical architectures and infrastructure necessary to accommodate wide variety of customer needs. Information technology (IT) services include, but are not limited to: local and wide area network management, facilities for data warehousing, archival storage, fully supported electronic commerce/electronic data interchange, comprehensive disaster recovery programs, output preparation and distribution, and full service desk.

Facility Name: Corporate Data Center Operations/Austin Information Technology Center

Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	(512) 326-6217	<a href="mailto:Amy.Howe1@va.gov">Amy.Howe1@va.gov</a>
Information Security Officer:	Charles Aponte	(512) 326-6593	<a href="mailto:Charles.Aponte2@va.gov">Charles.Aponte2@va.gov</a>
Acting Chief, Systems Security /Program Manager	Steven Gosewehr	(512) 326-6021	<a href="mailto:Steven.Gosewehr@va.gov">Steven.Gosewehr@va.gov</a>
System Owner/Chief Information Officer	John Rucker	(512) 326-6422	<a href="mailto:John.Rucker@va.gov">John.Rucker@va.gov</a>
Information Owner:			
Person Completing Document:	Marques Pharms	(512) 326-6941	<a href="mailto:Marques.Pharms@va.gov">Marques.Pharms@va.gov</a>
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)			12/2009
Date Approval To Operate Expires:			07/2013

What specific legal authorities authorize this program or system: Under the authority of the Government Management Reform Act of 1994 and the VA and Housing and Urban Development and Independent Agencies Appropriations Act of 1997.

What is the expected number of individuals that will have their PII stored in this system: 300,000+ VA Employees

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. 07/2008

Is there an authorized change control process which documents any changes to existing applications or systems? Yes

If No, please explain:

Has a PIA been completed within the last three years? Yes

Date of Report (MM/YYYY): 02/2011

**Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.**

- Have any changes been made to the system since the last PIA?
- Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- Does this system/application/program collect, store or disseminate PII/PHI data?
- Does this system/application/program collect, store or disseminate the SSN?

**If there is no Personally Identifiable Information on your system , please complete TAB 7 & TAB 12. ( See Comment for Definition of PII)**

### (FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above no, please skip to row 15.	Yes
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	See Tab 8 "Additional Comments"
2. Name of the System of Records:	See Tab 8 "Additional Comments"
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	See Tab 8 "Additional Comments"
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	No
	<b><i>(Please Select Yes/No)</i></b>
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	Yes
Is PII collected by automated methods?	Yes
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	Yes
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	Provided for hire (benefits info), Background investigation docs (paper & electronic), Individual is advised the information is needed to validate eligibility	All	Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Provided for hire (benefits info), Background investigation docs (paper & electronic), Individual is advised the information is needed to validate eligibility	All	Written
Service Information	Paper & Electronic	Provided for hire (benefits info), individual is also advised on the need to have the Veteran documents to validate eligibility.	Verbal & Written	Verbal & Written
Medical Information	Paper & Electronic	For Human Capital Management matters, information is sent to the Department of Labor.	Written	Written
Criminal Record Information	Paper & Electronic	Provided for hire & Individual is advised on why the information is needed – OF-306 for investigative purposes.	Written	Written
Guardian Information	Paper & Electronic	Provided for hire & Individual is advised on why the information is needed – OF-306 for investigative purposes.	Written	Written
Education Information	Paper & Electronic	Provided for hire & individual is advised of why the information is needed to validate education.	Written	Written
Benefit Information	Paper & Electronic	Provided for hire (benefits info) & individual is advised of why the information is needed to enroll in benefit programs.	Written	Written
Background Information	Paper & Electronic	Credit report information and documents detailing background investigations.	Written	Written

<b>Data Type</b>	<b>Is Data Type Stored on your system?</b>	<b>Source requested, identify the specific file, entity and/or name of agency)</b>	<b>(If</b>	<b>Is data collection Mandatory or Voluntary?</b>	<b>Additional Comments</b>
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)		Mandatory	PAID, OLDE, FUM & others needed to verify eligibility for appointing authority.
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)		Mandatory	PAID, OLDE, FUM
Service Information	Yes	VA Files / Databases (Identify file)		Mandatory	PAID, OLDE, FUM
Medical Information	No	VA Files / Databases (Identify file)		Mandatory	PAID, OLDE, FUM
Criminal Record Information	Yes	VA Files / Databases (Identify file)		Mandatory	PAID, OLDE, FUM
Guardian Information	Yes	VA Files / Databases (Identify file)		Mandatory	PAID, OLDE, FUM
Education Information	Yes	VA Files / Databases (Identify file)		Mandatory	PAID, OLDE, FUM & mandatory if using education as qualifying criteria.
Benefit Information	Yes	VA Files / Databases (Identify file)		Mandatory	PAID, OLDE, FUM & used for enrollment in benefits and advisement to insurance agencies of any changes to employee's benefits.

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VHA DHCPS, Other VA HR Offices, Security Investigation Center; Hines HR, other VA stations supported by Human Capital Management	No	Personnel information for VA employees between the gaining/losing HR Offices , Leave Administration, Evidence Files, Usually shared via encrypted email	PII	Info passed is internal to VA and needed to process employee payroll & personnel information for VA employees between the gaining/losing HR Offices, Leave Administration, Evidence Files. Files are shared via PKI encrypted email.
Other Veteran Organization	Same as above	Yes	Same	PII	Same
Other Federal Government Agency	Same as above	Yes	Personnel information for VA employees between the gaining/losing HR Offices	PII	Same
State Government Agency	No	No	N/A		N/A
Local Government Agency	No	No	N/A		N/A
Research Entity	No	No	N/A		N/A
Other Project / System	FIOA/EEO/IG	No	Announcement/applicant information		N/A
Other Project / System					
Other Project / System					

(FY 2011) PIA: Access to Records

Does the system gather information from another system?	Yes
Please enter the name of the system:	eOPF, e-QIP, PAID, EEX, GRB, Assist, Online, E-mail.
Per responses in Tab 4, does the system gather information from an individual?	
If information is gathered from an individual, is the information provided:	<input checked="" type="checkbox"/> Through a Written Request <input checked="" type="checkbox"/> Submitted in Person <input checked="" type="checkbox"/> Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	No

---

## (FY 2011) PIA: Secondary Use

---

Will PII data be included with any secondary use request?

Yes

- Drug/Alcohol Counseling       Mental Health       HIV  
 Research     Sickle Cell       Other (Please Explain)

Other (explained) - Higher authority or legal counsel made need information as it would pertain to any adverse or legal action being taken against employees. Reasonable Accommodation requests may require obtaining and use of this type of information. OPM may request additional copies of certain forms. These requests are usually sent via mail, email, or a telephone call. Documents are sent directly to OPM via fax.

if yes, please check all that apply:

Describe process for authorizing access to this data.

**Answer #1** ( For PAID) - SORN # 27VA047, describes the following record access procedures: Employees or representatives designated in writing seeking information regarding access to and contesting of VA records may write, call or visit the VA office of employment. Record source categories: Personnel records information received from employees, VA officials, other Government and State Agencies.

**Answer #2** (For Human Capital Management) - HR authorized access to federal employee personnel files, Title 5, Code of Federal Regulations (CFR) Part 297. OPM has published notices for Government wide systems of records that cover the Official Personnel Folder (OPM/GOVT-1) and the Employee Medical Folder (OPM/GOVT-10).

These notices include descriptions of routine uses that allow release of records without the employee's prior written consent to specific officials outside the employing agency for specific purposes.

---

## (FY 2011) PIA: Program Level Questions

---

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

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Data elements are limited to active employees of the VA and input by valid VA representatives.

---

How is data checked for completeness?

Answer: Employee review and data dedits within EEX and OLDE input subsystems check the data for completeness and logic checks before being passed to the Edit and update subsystem. Completeness is also checked through a verification and validation process.

---

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

Answer: EEX and OLDE input transactions update PAID daily. All employees have access to their service record information, and they may utilize EEX or contact their HR/Payroll agents to updated information. Human Capital Management personnel periodically purge data not being use.

---

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

Answer: Data edits are placed within the EEX and OLDE input subsystems that check the entered data for relevance, authenticity and accuracy before being passed to the Edit and Update subsystem. In the Edit and Update subsystem, the data is again edited and checked for relevance and authenticity before being added to the PAID records.

---

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

Answer:

---

## (FY 2011) PIA: Retention & Disposal

---

What is the data retention period?

**Answer #1-** PAID data is retained on line for all active VA employees at the Austin Information Technology Center. 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. **Answer #2 -** Investigative information is generally deleted once the investigation has closed (6 months to a year), Type of data dictates. NARA policy applies to all.

---

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

Answer #1 - The PAID data is used to process payroll data; sometimes corrections for past actions need to be accomplished. Answer #2 - NARA retention requirements and compliance as well as audits.

---

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

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.

---

Where are these procedures documented?

Answer #1 - 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. Answer #2 - The Guide to Personnel Recordkeeping, published by OPM, Title 5 Code of Federal Regulations part 293 .

---

How are data retention procedures enforced?

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.

---

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

Yes

---

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

Answer:

---

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

---

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

No

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

Answer:

---

## (FY 2011) PIA: Security

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

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

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

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

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

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

Answer:

Is adequate physical security in place to protect against unauthorized access? Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: **As it applies to the PAID environment;** The DFAS system is housed at the AITC and is a part of the PAID system. At the project level, security is provided by the Austin Information Technology Center (AITC). PAID operates within the AITC LAN environment, and was granted a full Authority to Operate on April 2, 2007 and is included in AITC password management and user authentication processes. Access is granted to individuals with AITC TSO access and written authorization from their supervisor. Facility staff determines level of access for individuals to view and report on their data. In addition, in accordance with the contract between the contractor and the government, all contractors with access to PAID information are required to meet the AITC contractor security requirements.

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

- |   |   |  |
|---|---|--|
| <input checked="" type="checkbox"/> Air Conditioning Failure          | <input checked="" type="checkbox"/> Data Disclosure                       | <input checked="" type="checkbox"/> Hardware Failure   |
| <input checked="" type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Data Integrity Loss                   | <input checked="" type="checkbox"/> Identity Theft     |
| <input checked="" type="checkbox"/> Blackmail                         | <input checked="" type="checkbox"/> Denial of Service Attacks             | <input checked="" type="checkbox"/> Malicious Code     |
| <input checked="" type="checkbox"/> Bomb Threats                      | <input type="checkbox"/> Earthquakes                                      | <input checked="" type="checkbox"/> Power Loss         |
| <input type="checkbox"/> Burglary/Break In/Robbery                    | <input type="checkbox"/> Eavesdropping/Interception                       | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input type="checkbox"/> Cold/Frost/Snow                              | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) | <input checked="" type="checkbox"/> Storms/Hurricanes  |
| <input checked="" type="checkbox"/> Communications Loss               | <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor)  | <input type="checkbox"/> Substance Abuse               |
| <input checked="" type="checkbox"/> Computer Intrusion                | <input checked="" type="checkbox"/> Flooding/Water Damage                 | <input checked="" type="checkbox"/> Theft of Assets    |
| <input checked="" type="checkbox"/> Computer Misuse                   | <input type="checkbox"/> Fraud/Embezzlement                               | <input checked="" type="checkbox"/> Theft of Data      |
| <input checked="" type="checkbox"/> Data Destruction                  |   | <input type="checkbox"/> Vandalism/Rioting             |

Answer: (Other Risks) Insider Threat (professional Criminals, disgruntled personnel, foreign agents, terrorists, physical security), External Threat (external hacker, worms & viruses, Trojans, malware), Environmental Threat (Tornadoes, Man Made threats).

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

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

Answer: (Other Controls)

## PIA: PIA Assessment

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

Answer: As it applies to the PAID File and Print server; Documents produced or carried by the file and print server are interspersed with documents containing PII. Much of why this is used is to create and test changes to the PAID system. These actions are reliant upon real time examples of problems. These examples always contain PII. With the current execution of about 1500 Change Orders per year and with more than half referencing PII as part of the problem statement, the staging has to be conducted on the file/print server since PII cannot exist in the USD system. A lot of the information comes from DFAS, which is a part of the PAID system. This 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.

---

*Please add additional controls:*

## (FY 2011) PIA: Additional Comments

---

Per Tab 3 - Lines 6 thru 8, the following is submitted:

---

[http://www.rms.oit.va.gov/SOR\\_Records/121VA19.pdf](http://www.rms.oit.va.gov/SOR_Records/121VA19.pdf) - National Patient Databases-VA  
<http://edocket.access.gpo.gov/2009/pdf/E9-19489.pdf> - Customer User Provisioning Systems (CUPS) - VA  
<http://edocket.access.gpo.gov/2009/pdf/E9-17910.pdf> - Veterans Information Solutions (VIS) - VA  
<http://edocket.access.gpo.gov/2009/pdf/E9-17776.pdf> - Veterans Affairs/Department of Defense Identity Respository (VADIR) - VA  
[http://www.rms.oit.va.gov/SOR\\_Records/27VA047.asp](http://www.rms.oit.va.gov/SOR_Records/27VA047.asp) - Personnel and Accounting Pay System - VA  
[http://www.rms.oit.va.gov/SOR\\_Records/33VA113.asp](http://www.rms.oit.va.gov/SOR_Records/33VA113.asp) - National Prosthetic Patient Database (NPPD) - VA  
[http://www.rms.oit.va.gov/SOR\\_Records/37VA27.asp](http://www.rms.oit.va.gov/SOR_Records/37VA27.asp) -VA Supervised Fiduciary/Beneficiary and General Investigative Records-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/38VA21.asp](http://www.rms.oit.va.gov/SOR_Records/38VA21.asp) - Veterans and Beneficiaries Identification Records Location Subsystem-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/45VA21.asp](http://www.rms.oit.va.gov/SOR_Records/45VA21.asp) - Veterans Assistance Discharge System - VA  
[http://www.rms.oit.va.gov/SOR\\_Records/55VA26.asp](http://www.rms.oit.va.gov/SOR_Records/55VA26.asp) - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records - VA  
<http://edocket.access.gpo.gov/2009/pdf/E9-14302.pdf> - Compensation, Pension, Education and Vocational Rehabilitation and Employment Records - VA  
[http://www.rms.oit.va.gov/SOR\\_Records/60VA21.asp](http://www.rms.oit.va.gov/SOR_Records/60VA21.asp) - Repatriated American Prisoners of War-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/65VA122.asp](http://www.rms.oit.va.gov/SOR_Records/65VA122.asp) - Community Placement Program - VA  
[http://www.rms.oit.va.gov/SOR\\_Records/67VA30.asp](http://www.rms.oit.va.gov/SOR_Records/67VA30.asp) - PROS/KEYS User-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/69VA131.asp](http://www.rms.oit.va.gov/SOR_Records/69VA131.asp) - Ionizing Radiation Registry-VA  
<http://edocket.access.gpo.gov/2009/pdf/E9-28387.pdf> - Health Professional Scholarship-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/76VA05.asp](http://www.rms.oit.va.gov/SOR_Records/76VA05.asp) - General Personnel Records (Title 38)-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/79VA19.asp](http://www.rms.oit.va.gov/SOR_Records/79VA19.asp) - Veterans Health Information Systems and Technology Architecture (VistA) Records-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/86VA00S1.pdf](http://www.rms.oit.va.gov/SOR_Records/86VA00S1.pdf) - Workers' Compensation Occupational Safety and Health Management Information S  
[http://www.rms.oit.va.gov/SOR\\_Records/88VA244.asp](http://www.rms.oit.va.gov/SOR_Records/88VA244.asp) - Accounts Receivable Records (Formally known as 88VA20A6)-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/89VA16.pdf](http://www.rms.oit.va.gov/SOR_Records/89VA16.pdf) - Income Verification Records-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/93VA131.asp](http://www.rms.oit.va.gov/SOR_Records/93VA131.asp) - Gulf War Registry-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/97VA105.asp](http://www.rms.oit.va.gov/SOR_Records/97VA105.asp) - Consolidated Data Information System-VA  
<http://edocket.access.gpo.gov/2009/pdf/E9-7160.pdf> - Automated Safety Incident Surveillance and Tracking System-VA  
<http://edocket.access.gpo.gov/2009/pdf/E9-12954.pdf> - Patient Advocate Tracking System (PATS)-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/105VA131.asp](http://www.rms.oit.va.gov/SOR_Records/105VA131.asp) - Agent Orange Registry-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/107VA008B.pdf](http://www.rms.oit.va.gov/SOR_Records/107VA008B.pdf) - Program Evaluation Research Data Records-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/108VA119.asp](http://www.rms.oit.va.gov/SOR_Records/108VA119.asp) - Spinal Cord Dysfunction-Registry (SCD-R)-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/146VA005Q3.pdf](http://www.rms.oit.va.gov/SOR_Records/146VA005Q3.pdf) - Department of Veterans Affairs Identity Management System (VAIDMS)-VA  
[http://www.rms.oit.va.gov/SOR\\_Records/145VA005Q3.pdf](http://www.rms.oit.va.gov/SOR_Records/145VA005Q3.pdf) - Department of Veterans Affairs Personnel Security File System (VAPSFs)-VA

## (FY 2011) PIA: VBA Minor Applications

<b>Which of these are sub-components of your system?</b>
--

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

VBA Data Warehouse  
VBA Training Academy  
Veterans Canteen Web  
VIC  
VR&E Training Website  
Web LGY

Telecare Record Manager  
VBA Enterprise Messaging System  
Veterans On-Line Applications (VONAPP)  
Veterans Service Network (VETSNET)  
Web Electronic Lender Identification

Web Automated Folder Processing System (WAFPS)  
Web Automated Reference Material System (WARMS)  
Web Automated Verification of Enrollment  
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 2011) PIA: VISTA Minor Applications

**Which of these are sub-components of your system?**

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	Health Level Seven	Master Patient Index VistA
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
PAID	Patch Module	Text Integration Utilities	Pharmacy Benefits Mangement
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	Progress Notes	Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Verified Components - DSSI
VBECS	VistALink Security	Text Integration Utilities	Vendor - Document Storage Sys
VDEF	Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistALink		Voluntary Timekeeping	Voluntary Timekeeping National

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 2011) PIA: Minor Applications

**Which of these are sub-components of your system?**

1184 Web	Agent Cashier	x	Administrative Data Repository (ADR)
A4P	Air Fortress		Automated Access Request
ADT	Auto Instrument		Bed Board Management System
BDN 301	Cardiff Teleform		Cardiology Systems (stand alone servers from the network)
CP&E	CHECKPOINT		Clinical Data Repository/Health Data Repository
DRM Plus	Data Innovations		Combat Veteran Outreach
DSIT	DELIVEREX		Committee on Waiver and Compromises
ENDSOFT	DSS Quadramed		Crystal Reports Enterprise
EYECAP	EKG System		DICTATION-Power Scribe
Genesys	ePROMISE		EDS Whiteboard (AVJED)
ICB	Lynx Duress Alarm		Embedded Fragment Registry
KOWA	Mumps AudioFAX		Enterprise Terminology Server & VHA Enterprise Terminology Services
MHTP	Onvicord (VLOG)		Financial and Accounting System (FAS)
NOAHLINK	P2000 ROBOT		Financial Management System (FMS)
Omnicell	PACS database		Health Summary Contingency
Optifill	PIV Systems		Microsoft Active Directory
PICIS OR	Remedy Application		Microsoft Exchange E-mail System
Q-Matic	Traumatic Brain Injury		Military/Vet Eye Injury Registry
RAFT	VAMedSafe		Personal Computer Generated Letters
RALS	VBA Data Warehouse		QMSI Prescription Processing
SAN	VHAHUNAPP1		Scanning Exam and Evaluation System
Sentillion	VHAHUNFPC1		Tracking Continuing Education
Stellant	VISTA RAD		VA Conference Room Registration
Stentor	Whiteboard		

Explain any minor application that are associated with your installation that does not appear in the list above. Please

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 2011) PIA: Final Signatures

Facility Name: CDCO>AITC>VA>AITC>AITE Site and General Support System (GSS)

Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	(512) 326-6217	Amy.Howe1@va.gov

Digital Signature Block

System Owner/Chief Information Officer	John Rucker	(512) 326-6422	John.Rucker@va.gov
--	-------------	----------------	--------------------

Digital Signature Block

Information Security Officer:	Charles Aponte	(512) 326-6593	<a href="mailto:Charles.Aponte2@va.gov">Charles.Aponte2@va.gov</a>
-------------------------------	----------------	----------------	--

Digital Signature Block

Date of Report: 02/2011

OMB Unique Project Identifier 0

Project Name CDCO>AITC>VA>AITC>AITE Site and General Support System (GSS)

