

## **Welcome to the PIA for FY 2010!**

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. More information can be found by reading VA 6508.

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://vaww.privacy.va.gov/Privacy\\_Impact\\_Assessments.asp](http://vaww.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 Privacy Impact Assessment Handbook 6202.2 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 Handbook 6202.2.
- 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 Handbook 6202.2 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

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 an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirectly 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**

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.

## (FY 2010) PIA: System Identification

---

Program or System Name: National Center for Veterans Analysis System (NCVAS)

OMB Unique System / Application / Program Identifier (AKA: UPID #): Unknown-not listed in SMART

The National Center for Veterans Analysis and Statistics (NCVAS) Analysis System (NAS) is an integrated set of COTS statistical, geospatial analysis, multidimensional data modeling and business intelligence capabilities. The NAS provides the computational and analytical toolset used by NCVAS to analyze statistics on Veteran population and Veteran Affairs programs to inform and enable improved outcomes for Veterans through better policies and improved efficiency and effectiveness of VA operations. The NAS is used to analyze a variety of VA demographic and operations data collected by other VA or other Federal Agency (ie. Census, Department of Defense) general support systems.

Description of System / Application / Program:

---

Facility Name: Austin Information Technology Center (AITC)

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:	James Graham	202-461-6894	<a href="mailto:james.graham@va.gov">james.graham@va.gov</a>
System Owner	Judy Downing	512-326-6000	<a href="mailto:judy.downing@va.gov">judy.downing@va.gov</a>
Person Completing Document:	Reyes Ruiz	512-326-6046	<a href="mailto:reyes.ruiz@va.gov">reyes.ruiz@va.gov</a>
Information Owner	Dat Tran	202-461-5788	<a href="mailto:dat.tran@va.gov">dat.tran@va.gov</a>
Project Manager	Jim Steele	512-326-6886	<a href="mailto:jim.steele@va.gov">jim.steele@va.gov</a>
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	N/A New System		
Date Approval To Operate Expires:	ATO Pending		

What specific legal authorities authorize this program or system: None. NCVAS was approved by SECVA on February 2008.

What is the expected number of individuals that will have their PII stored in this system: 3.8 Million

Identify what stage the System / Application / Program is at: Development/Acquisition

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. Late December 2009

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? N/A: First PIA

Date of Report (MM/YYYY): 11/2009

**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 skip to TAB 12. ( See Comment for Definition of PII)**



## (FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

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

- |   |   |
|---|---|
| 1. All System of Record Identifier(s) (number):   | 43VA008; 107VA008B; 128VA008; 149VA008A;<br>Non-Health Data Analyses and Projections for VA<br>Policy and Planning - VA; Health Program<br>Evaluation-VA;   |
| 2. Name of the System of Records:   | <a href="http://www.rms.oit.va.gov/SOR_Records/43VA008.pdf">http://www.rms.oit.va.gov/SOR_Records/43VA008.pdf</a> ;<br><a href="http://www.rms.oit.va.gov/SOR_Records/107VA008B.pdf">http://www.rms.oit.va.gov/SOR_Records/107VA008B.pdf</a> ;<br><a href="http://www.rms.oit.va.gov/SOR_Records/128VA008A.pdf">http://www.rms.oit.va.gov/SOR_Records/128VA008A.pdf</a> ; |
| 3. Location where the specific applicable System of Records Notice may be accessed (include the URL): | <a href="http://www.rms.oit.va.gov/SOR_Records/149VA008A.pdf">http://www.rms.oit.va.gov/SOR_Records/149VA008A.pdf</a> ;   |

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?

Yes

Does the System of Records Notice require modification or updating?

No

***(Please Select Yes/No)***

Is PII collected by paper methods?

No

Is PII collected by verbal methods?

No

Is PII collected by automated methods?

No

Is a Privacy notice provided?

No

Proximity and Timing: Is the privacy notice provided at the time of data collection?

No

Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?

No

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?

No

Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?

No

(FY 2010) 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)	N/A			
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)	N/A			

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)		
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)		
Service Information	Yes	VA Files / Databases (Identify file)		
Medical Information	Yes	VA Files / Databases (Identify file)		
Criminal Record Information	No			
Guardian Information	Yes	VA Files / Databases (Identify file)		
Education Information	Yes	VA Files / Databases (Identify file)		
Benefit Information	Yes	VA Files / Databases (Identify file)		
Other Federal Agency Information	Yes	Other Federal Agency (Identify)		
Memorial Affairs Information	Yes	VA Files / Databases (Identify file)		
Other (Explain)				

(FY 2010) 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	AITC, OPP	Yes			
Other Veteran Organization		No			
Other Federal Government Agency		No			
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system?

Yes

Please enter the name of the system:

The dominant Veterans Benefits Administration (VBA) databases include the Compensation and Pension Master Record (CPMR), VETSNET and the Beneficiary Identification and Records Locator Subsystem (BIRLS). Other VBA databases include created by the Education, Insurance, Loan Guaranty, and Vocational Rehabilitation and Employment Services as well as those stored by the Offices of Performance Analysis and Integrity and Business Process Integration / Select administrative Veterans Health Administration (VHA) data will derive from the Patient Treatment and Enrollment Files / National Cemetery Administration data will be extracted from the BOSS and AMASS systems / Defense data will gathered from VADIR / Future Federal agency data will come from unknown data systems.

Per responses in Tab 4, does the system gather information from an individual?

No

If information is gathered from an individual, is the information provided:

- Through a Written Request
- Submitted in Person
- Online via Electronic Form

Is there a contingency plan in place to process information when the system is down?

Yes

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request?

No

if yes, please check all that apply:

- Research
- Sickle Cell
- Mental Health
- HIV
- Other (Please Explain)

Describe process for authorizing access to this data.

Answer:

## (FY 2010) 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?**

Yes

If Yes, Please Specify: This PIA does not contain sensitive information. However, the NCVAS system will contain PII and PHI. Classification is at the high-level.

---

**Explain how collected data are limited to required elements:**

Answer: NCVAS does not collect data as it stores select information captured by other systems. Based upon tailored project information requests (PIRs) and data transfer agreements (DTAs), NCVAS receives only those data variables absolutely required for processing. Whole datasets are not imported.

---

**How is data checked for completeness?**

Answer: Received data is matched against the requirements set forth in PIRs and DTAs. This audit insures that all requested information is provided.

---

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

Answer: Given that each dataset's make-up will change on an annual basis, plans call for each received dataset to be replenished each FY.

---

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

Answer: Similar to the way the data is reviewed for completeness, all data is screened to ensure that it matches the requirements outlines in the associated PIRs and DTAs. Data is only accepted from established partnerships solidified with executed agreements.

---

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

Answer:

---

---

## (FY 2010) PIA: Retention & Disposal

---

**What is the data retention period?**

Answer: Currently, a litigation hold is in force and thus the retention of the said data will exceed existing retention periods. As the records are duplicates of master records, the retention period is transitory in nature. That is, the records can be destroyed when the databases are superseded or not longer needed. This retention period is controlled by the National Archives and Records Administration's (NARA's) General Records Schedule 20, Electronic Records.

---

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

Answer: Data is required to provide statistical and analytical services to the Department.

---

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

Answer: Given the existence of a litigation hold, this Office must maintain select data beyond the course of a normal retention period. When the litigation hold is lifted, NCVAS data will be disposed of in accordance with delineated VA, other Federal agency, and NARA retention guidelines.

---

**Where are these procedures documented?**

Answer: Individual NCVAS records fall under the Records Control Schedule of the source VA or other Federal agency that generated the data. Additional guidance is secured from NARA at [www.archives.gov](http://www.archives.gov). Select online locations follow: Department of Veterans Affairs' Records Management Guidance, VA Handbook 6300.1, Records Management Procedures [http://vaww1.va.gov/vapubs/viewPublication.asp?Pub\\_ID=19&FTtype=2](http://vaww1.va.gov/vapubs/viewPublication.asp?Pub_ID=19&FTtype=2); Veterans Health Administration's Records Control Schedule 10-1 <http://vaww1.va.gov/vhapublications/rcs10/rcs10-1.pdf>; Veterans Benefits Administration's Records Control Schedule VB-1, Part II <http://www.warms.vba.va.gov/admin20/rcs/part2/part2.pdf>; and assorted hardcopy versions of historic Department of Veterans Affairs' Central Office Records Control Schedule guidance maintained by the Privacy Officer assigned to the system owner.

---

**How are data retention procedures enforced?**

Answer: All received data is fully accounted for by businessline, variable, issuance date, and date of receipt in a master log. As the FY changes, new data is received, or needs change, the log is reviewed for actionable items. This status of actionable items is enforced by the privacy officer and system owner.

---

**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: VA's Records Control Schedule has been approved by NARA.

---

**(FY 2010) 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 2010) 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.. No

---

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? No

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? No

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

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

Answer: System is still in the development phase, once system becomes operational, questions 7-9 will be "yes".

---

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: System security documentation currently undergoing a certification and accreditation review by VA's Certification Program Office.

---

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

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

Answer: (Other Risks)

---

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

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

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: None.

**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 2010) PIA: Additional Comments

---

Add any additional comments on this tab for any question in the form you want to comment on. Please indicate the question you are responding to and then add your comments.

---

Tab 3, System of Records, Rows 16-23: Please note that NAS does not collect record-level data from any individual. Rather, it is composed of other VA organizational databases which were populated through the collection of data.

Tab 4, Notice, Rows 7-23: Please note that NAS does not collect record-level data from any individual. Rather, it is composed of other VA organizational databases which were populated through the collection of data.

Tab 4, Notice, Rows 33-45: These data types are not collected, but process generated.

Tab 5, Data Sharing and Access, Rows 4-18: Intent is for record-level data to be shared between OPP, AITC and Altarum during the development and production phases. Upon activation of the system, VA entities will only view aggregate data.

Tab 9, 10, 11: These tabs were left blank as the system does not interface with these applications.

(FY 2010) PIA: VBA Minor Applications

---

Explain what minor application that are associated with your installation? (Check all that apply)

Records Locator System	Education Training Website	Appraisal System
Veterans Assistance Discharge System (VADS)	VR&E Training Website	Web Electronic Lender Identification
LGY Processing	VA Reserve Educational Assistance Program	CONDO PUD Builder
Loan Service and Claims	Web Automated Verification of Enrollment	Centralized Property Tracking System
LGY Home Loans	Right Now Web	Electronic Appraisal System
Search Participant Profile (SPP)	VA Online Certification of Enrollment (VA-ONCE)	Web LGY
Control of Veterans Records (COVERS)	Automated Folder Processing System (AFPS)	Access Manager
SHARE	Personal Computer Generated Letters (PCGL)	SAHSHA
Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	VBA Data Warehouse
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry)
Awards	State Benefits Reference System	VBA Enterprise Messaging System
Financial and Accounting System (FAS)	Training and Performance Support System (TPSS)	LGY Centralized Fax System
Eligibility Verification Report (EVR)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)
Automated Medical Information System (AMIS)290	Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Automated Standardized Performance Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Compensation and Pension (C&P) Record Interchange (CAPRI)	Purchase Order Management System (POMS)
Web Service Medical Records (WebSMR)	Control of Veterans Records (COVERS)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Inventory Management System (IMS)
Fiduciary STAR Case Review	Fiduciary Beneficiary System (FBS)	Synquest
Veterans Exam Request Info System (VERIS)	Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS
Web Automated Folder Processing System (WAFPS)	Inforce	ASSISTS
Courseware Delivery System (CDS)	Awards	MUSE
Electronic Performance Support System (EPSS)	Actuarial	Bbraun (CP Hemo)
Veterans Service Representative (VSR) Advisor	Insurance Self Service	VIC
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines
C&P Training Website	Insurance Online	Script Pro

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.

Minor app #1	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?		

Minor app #2	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?		

Minor app #3	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?		

---

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET) Waco Indianapolis, Newark, Roanoke, Seattle
Priv Plus Mental Health Assistant	(WINRS) BIRLS
Telecare Record Manager	Centralized Accounts Receivable System (CARS)
Omnicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill Vocational Rehabilitation & Employment (VR&E) CH 31	INS - BIRLS Mobilization
Post Vietnam Era educational Program (VEAP) CH 32	Master Veterans Record (MVR)
Spinal Bifida Program Ch 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitlement Program for Survivors (REAPS) Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607 Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS Work Study Management System (WSMS)	
Benefits Delivery Network (BDN)	
Personnel and Accounting Integrated Data and Fee Basis (PAID) Personnel Information Exchange System (PIES) Rating Board Automation 2000 (RBA2000)	
SHARE Service Member Records Tracking System	

(FY 2010) PIA: VISTA Minor Applications

---

Explain what minor application that are associated with your installation? *(Check all that apply)*

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN) ADVERSE REACTION TRACKING ASISTS	DSS EXTRACTS EDUCATION TRACKING EEO COMPLAINT TRACKING	INTAKE/OUTPUT INTEGRATED BILLING INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT SUPPORT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	KERNEL
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KIDS
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	LAB SERVICE
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LETTERMAN
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LEXICON UTILITY
BED CONTROL	EXTENSIBLE EDITOR	LIBRARY
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIST MANAGER
CAPACITY MANAGEMENT - RUM	FEE BASIS	MAILMAN
CAPRI	FUNCTIONAL INDEPENDENCE	MASTER PATIENT INDEX VISTA
CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE
CARE MANAGEMENT CLINICAL CASE REGISTRIES	GEN. MED. REC. - I/O GEN. MED. REC. - VITALS	MEDICINE MENTAL HEALTH
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHVET
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original) A4EL
CMOP	HEALTH SUMMARY	NATIONAL DRUG FILE
CONSULT/REQUEST TRACKING	HINQ	NATIONAL LABORATORY TEST
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NDBI
CPT/HCPCS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NETWORK HEALTH EXCHANGE
CREDENTIALS TRACKING DENTAL DIETETICS	IFCAP IMAGING INCIDENT REPORTING	NOIS NURSING SERVICE OCCURRENCE SCREEN
DISCHARGE SUMMARY	INCOME VERIFICATION MATCH	ONCOLOGY
DRG GROUPER	INCOMPLETE RECORDS TRACKING	ORDER ENTRY/RESULTS REPORTING

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.

Minor app #1	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<input type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

Minor app #2	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<input type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

Minor app #3	Name		Description	Comments
		<input type="checkbox"/>	Is PII collected by this min or application?	
		<input type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		Who has access to this data?		

---

OUTPATIENT PHARMACY	SOCIAL WORK
PAID	SPINAL CORD DYSFUNCTION
PATCH MODULE	SURGERY
PATIENT DATA EXCHANGE	SURVEY GENERATOR
PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	TOOLKIT
PCE PATIENT CARE ENCOUNTER	UNWINDER
PCE PATIENT/IHS SUBSET	UTILIZATION MANAGEMENT ROLLUP
PHARMACY BENEFITS MANAGEMENT	UTILIZATION REVIEW
PHARMACY DATA MANAGEMENT	VA CERTIFIED COMPONENTS - DSSI
PHARMACY NATIONAL DATABASE	VA FILEMAN
PHARMACY PRESCRIPTION PRACTICE	VBECs
POLICE & SECURITY	VDEF
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	VISIT TRACKING
QUALITY ASSURANCE INTEGRATION	VISTALINK
QUALITY IMPROVEMENT CHECKLIST	VISTALINK SECURITY
QUASAR	VISUAL IMPAIRMENT SERVICE TEAM
RADIOLOGY/NUCLEAR MEDICINE	ANRV
RECORD TRACKING	VOLUNTARY TIMEKEEPING
REGISTRATION	VOLUNTARY TIMEKEEPING NATIONAL
RELEASE OF INFORMATION - DSSI	WOMEN'S HEALTH
REMOTE ORDER/ENTRY SYSTEM	CARE TRACKER
RPC BROKER	
RUN TIME LIBRARY	
SAGG	
SCHEDULING	
SECURITY SUITE UTILITY PACK	
SHIFT CHANGE HANDOFF TOOL	

(FY 2010) PIA: Minor Applications

---

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

---

Minor app #1	Name		Description		Comments
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

Minor app #2	Name		Description		Comments
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

Minor app #3	Name		Description		Comments
		<input type="checkbox"/>	Is PII collected by this min or application?		
		<input type="checkbox"/>	Does this minor application store PII?		
			If yes, where?		
		Who has access to this data?			

## (FY 2010) PIA: Final Signatures

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:	James Graham	202-461-6894	james.graham@va.gov
Digital Signature Block			
Chief Information Officer:	Judy Downing	512-326-6000	judy.downing@va.gov
Digital Signature Block			
Person Completing Document:	Reyes Ruiz	512-326-6046	reyes.ruiz@va.gov
Digital Signature Block			
System / Application / Program Manager:	Dat Tran	202-461-5788	dat.tran@va.gov
Digital Signature Block			

Date of Report: 11/1/2009  
 OMB Unique Project Identifier: Unknown-not listed in SMART  
 Project Name: National Center for Veterans Analysis System (NCVAS)

(FY 2010) PIA: Final Signatures

Facility Name:

Austin Information Technology Center (AITC)

Title	Name	Phone	Email
Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov

**AMY HOWE**  
Digital Signer  
Digitally signed by: AMY HOWE  
DN: CN = AMY HOWE O = Department of Veterans Affairs, Internal Staff  
Date: 2009.12.29 15:36:27 -0600

Information Security Officer: James Graham 202-461-6894 james.graham@va.gov

*James Graham*  
Digital Signature Block  
1-7-2010  
Judy Downing  
512-326-6000  
judy.downing@va.gov

Person Completing Document: Reyes Ruiz 512-326-6046 reyes.ruiz@va.gov

Digital Signature Block

System / Application / Program Manager: Dat Tran 202-461-5788 dat.tran@va.gov

Digital Signature Block

Date of Report: 11/1/2009  
OMB Unique Project Identifier: Unknown-not listed in SMART  
Project Name: National Center for Veterans Analysis System (NCVAS)