

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://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 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:	Development>CDCO>AITC> VBA>Ebenefits
OMB Unique System / Application / Program Identifier (AKA: UPID #):	OMB CONTROL NUMBER: 2900-0737

The President's Commission on Care for America's Returning Wounded Warriors, established by Executive Order 13426 in March 2007, recommended the creation of a web portal to provide wounded, injured and ill service members and veterans, their families, and their care providers with a single sign on, central access point to online benefits and related services. The VA eBenefits Portal Program was established to develop, implement, and operate a user-friendly web portal system that fulfills these recommendations. The eBenefits Portal will provide a single point of access through which active service members, veterans, family members, and their delegates can find information about military benefits, veterans' health, and other services, and utilize an array of related online features.

Description of System / Application / Program:

Facility Name: Austin Information
Technology Center (AITC)

Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	Amy.Howe1@va.gov
Information Security Officer:	Walter Whiteford	512-326-6294	Walter.Whiteford@va.gov
Chief Information Officer:	Judy Downing	512-326-6000	Judy.Downing@va.gov
Person Completing Document:	Justin Anderle	571-221-3423	Justin.Anderle@va.gov
Other Titles: Program Manager	Roy McBrayer	512-326-6588	Roy.McBrayer@va.gov
Other Titles: Project Manager	Don Vanderveer	512-326-6457	Don.Vanderveer@va.gov
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	N/A; first one		
Date Approval To Operate Expires:	12/2009		

What specific legal authorities authorize this program or system:

The eBenefits portal was commissioned to meet the recommendations of the Dole-Shalala commission.

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

Potentially all Veterans

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.

System operational for 1 month

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): | VADIR SORN 138VA005Q, DEERS SORN DPR34 |
| 2. Name of the System of Records: | DEERS, VADIR |
| 3. Location where the specific applicable System of Records Notice may be accessed (include the URL): | http://www.gpoaccess.gov/fr/index.html ,
http://defenselink.mil/privacy/notices |
-

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?

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 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)	Electronic/File Transfer	<p>Privacy Act Statement</p> <p>The material/information contained herein falls within the purview of the Privacy Act of 1974 and will be safeguarded in accordance with the applicable system of records notice and DLAR 540021.</p> <p>AUTHORITYS USC 301 & EO 9397</p> <p>PURPOSE/ROUTINE USE: Information you provide is used to verify your identity and usage of this website.</p> <p>DISCLOSURE - Voluntary. However, if you fail to provide the requested information, DMDC will not be able to verify your identity. If your identity is not verified, you will be unable to gain access to the website.</p>	Automated	Automated
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	VA File Database	<p>Privacy Act Statement</p> <p>The material/information contained herein falls within the purview of the Privacy Act of 1974 and will be safeguarded in accordance with the applicable system of records notice and DLAR 540021.</p> <p>AUTHORITYS USC 301 & EO 9397</p> <p>PURPOSE/ROUTINE USE: Information you provide is used to verify your identity and usage of this website.</p> <p>DISCLOSURE: Voluntary. However, if you fail to provide the requested information, DMDC will not be able to verify your identity. If your identity is not verified, you will be unable to gain access to the website.</p>	Automated	Automated
Medical Information	N/A			
Criminal Record Information	N/A			
Guardian Information	N/A			
Education Information	N/A			
Benefit Information	VA File Database	<p>Privacy Act Statement</p> <p>The material/information contained herein falls within the purview of the Privacy Act of 1974 and will be safeguarded in accordance with the applicable system of records notice and DLAR 540021.</p> <p>AUTHORITYS USC 301 & EO 9397</p> <p>PURPOSE/ROUTINE USE: Information you provide is used to verify your identity and usage of this website.</p> <p>DISCLOSURE: Voluntary. However, if you fail to provide the requested information, DMDC will not be able to verify your identity. If your identity is not verified, you will be unable to gain access to the website.</p>	Automated	Automated
Other (Explain)				

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)	No			
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	No			
Medical Information	No			
Criminal Record Information	No			
Guardian Information	No			
Education Information	No			
Benefit Information	No			
Other (Explain)				
Other (Explain)				
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	VBA	Yes	PII data to identify the user to the target service	PII	MOU
Other Veteran Organization					
Other Federal Government Agency	DoD	Yes	PII data to identify the user to the target service.	PII	MOU/Connection agreement
State Government Agency					
Local Government Agency					
Research Entity					
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: VADIR, DEERS,

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

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? Yes

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

if yes, please check all that apply:

Describe process for authorizing access to this data.

The data is accessed when the owner of the PII data requests the use of the data to receive or apply for benefits.

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?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

The data is collected in real time from authorized data sources. When a user applies for benefits of the status of benefits then the data is queried and the request is made on the users behalf.

Answer:

How is data checked for completeness?

Answer:

The user is able to review the data before submission of the forms. If the information is incorrect the user can request a correction or update from the data source via a helpdesk ticket.

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

Answer:

The user is able to review the data before submission of the forms. If the information is incorrect the user can request a correction or update from the data source via a helpdesk ticket.

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

Answer:

The data is collected from sources that are considered authoritative for the data set in question. We are only a consumer of the data. We have no purview into the data handling and verification of the source repositories.

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?

The data that is maintained on eBenefits is only profile information. We do not store or process PII class data after the user session is completed.

Answer:

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

The information is queried and processed on behalf of the user to simplify benefits requests and status requests.

Answer:

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

Answer:

At the end of a users session the data is purged from our system. And the random access memory is recycled.

Where are these procedures documented?

Answer:

The procedures are documented in the eBenefits architecture documents and in the System security Plan.

How are data retention procedures enforced?

Answer:

The data retention procedure are automated and designed into the system. The can only be changed by a system level change of the architecture and system design.

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

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

Answer: Information is not stored, there is no retention schedule.

(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.. 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: The eBenefits project meets FISMA requirements for securing federal information systems, via the mandated Certification and accreditation process.

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
- Contingency 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 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.

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 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.

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.

The eBenefits portal does not store any information about the user other than the information required to maintain a user profile. Any PII information that is required is queried in real time from authoritative data sources. After the user has completed their transactions and logged off the system any PII information is purged from the system. The connections between the eBenefits portal are maintained with 2 two SSL tunnels and secured by SSL encryption that meets FIPS 199 compliance.

(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	
X	LGY Processing		VA Reserve Educational Assistance Program		CONDO PUD Builder	
	Loan Service and Claims		Web Automated Verification of Enrollment		Centralized Property Tracking System	
X	LGY Home Loans		Right Now Web		Electronic Appraisal System	
	Search Participant Profile (SPP)		VA Online Certification of Enrollment (VA-ONCE)	X	Web LGY	
	Control of Veterans Records (COVERS)		Automated Folder Processing System (AFPS)		Access Manager	
	SHARE		Personal Computer Generated Letters (PCGL)	X	SAH/SHA	
	Modern Awards Process Development (MAP-D)	X	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	X	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)	
X	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)	X
	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	

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET)
Priv Plus	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Mental Health Assistant	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	INS - BIRLS
Vocational Rehabilitation & Employment (VR&E) CH 31	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	

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 ROES	Name		Description	Comments
	ROES (remote order entry System)		allows for the veteran to order DME (durable medical equipment)	The eBenefits portal provides an access method for the user to order durable medical equipment. The application itself is responsible for the data and it's handling.
		<input checked="" type="checkbox"/>	Is PII collected by this min or application?	
		<input checked="" type="checkbox"/>	Does this minor application store PII?	
			If yes, where?	
		<input type="checkbox"/>	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?	
		<input type="checkbox"/>	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?	
		<input type="checkbox"/>	Who has access to this data?	

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

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

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?		

(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:	Walter Whiteford	512-326-6294	Walter.Whiteford@va.gov
Digital Signature Block			
Chief Information Officer:	Judy Downing	512-326-6000	Judy.Downing@va.gov
Digital Signature Block			
Person Completing Document:	Justin Anderle	571-221-3423	Justin.Anderle@va.gov
Digital Signature Block			
System / Application / Program Manager:	Roy McBrayer	512-326-6588	Roy.McBrayer@va.gov
Digital Signature Block			

Date of Report: 11/1/2009

OMB CONTROL NUMBER: 2900-

OMB Unique Project Identifier 0737

Development>CDCO>AITC>VBA>Eb

Project Name enefits

(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 Signature Block

Digitally signed by: AMY HOWE
DN: CN = AMY HOWE O = Department of Veterans Affairs, Internal Staff
Date: 2010.01.14 10:41:26 -06'00'

Information Security Officer:	Walter Whiteford	512-326-6294	Walter.Whiteford@va.gov
-------------------------------	------------------	--------------	-------------------------

WHITEFO
RD,
WALTER
(SQAS)

Digital Signature Block

Digitally signed by: WHITEFORD, WALTER (SQAS)
DN: CN = WHITEFORD, WALTER (SQAS) O = Department of Veterans Affairs, Internal Staff
Date: 2010.01.14 15:30:28 -06'00'

Chief Information Officer:	Judy Downing	512-326-6000	Judy.Downing@va.gov
----------------------------	--------------	--------------	---------------------

Digital Signature Block

Person Completing Document:	Justin Anderle	571-221-3423	Justin.Anderle@va.gov
-----------------------------	----------------	--------------	-----------------------

Digital Signature Block

System / Application / Program Manager:	Roy McBrayer	512-326-6588	Roy.McBrayer@va.gov
---	--------------	--------------	---------------------

Digital Signature Block

Date of Report: 11/1/2009

OMB CONTROL NUMBER: 2900-

OMB Unique Project Identifier 0737

Development>CDCO>AITC>VBA>Eb

Project Name enefits