

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: Burial Operations Support
System (BOSS)-2009

OMB Unique System / Application / Program
Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

BOSS was developed by NCA FTE at the Quantico Regional Processing Center (QRPC) to provide needed benefit delivery automation support to NCA facilities nationwide. NCA FTE continue to maintain and support it. The primary objective and business need was to automate all manual, paper-intensive record keeping, and information and forms processing associated with interments. BOSS provides nationwide burial location capability via the NCA Home Page and NCA Kiosk; linkage to Gravesite Reservation files; and a benefit crosscheck to facilitate timely First Notice of Death to VBA and its benefit delivery systems. BOSS increases the level of service provided to

Description of System / Application / Program: veterans and beneficiaries

Facility Name:

Title:	Name:	Phone:	Email:
Privacy Officer:	Willie Lewis	202-461-6746	willie.lewis@va.gov
Information Security Officer:	Judi Huffman	703-441-3064	judi.huffman@va.gov
Chief Information Officer:	William Barnes	703-441-0427	william.barnes@va.gov

Person Completing Document:	Willie Lewis	202-461-6746	willie.lewis@va.gov
Other Titles: Records Officer	Mechelle Powell	202-461-4114	mechelle.powell@va.gov
Other Titles: Project Manager	Kevin Guyan	703-441-3094	kevin.guyan@va.gov

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 03/2006
Date Approval To Operate Expires: 03/2009

BOSS supports legislative benefits outlined under: Title 38 Veterans' Benefits; Chapter 24 National Cemeteries and Memorials; Section 2402 Persons eligible for interment in national cemeteries.

What specific legal authorities authorize this program or system:
What is the expected number of individuals that will have their PII stored in this system:
1,000,000 - 9,999,999

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.
06/1996

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):

06/2009

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):

BOSS: 42VA41 AMAS: 48VA40B: 42VA411

2. Name of the System of Records:

BOSS: Veterans and Dependents National
Cemetery Interment AMAS: Veterans (Deceased)

3. Location where the specific applicable System of Records Notice may be
accessed (include the URL):

Headstone or Marker Records-VA Gravesite
Reservation

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?

Yes

(Please Select Yes/No)

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 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)	Paper & Electronic	Benefits	Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	Paper & Electronic	Benefits	Written	Written
Service Information	Paper & Electronic	Benefits	Written	Written
Medical Information				
Criminal Record Information				
Guardian Information				
Education Information				
Benefit Information	VA File Database	Benefits	Automated	Automated
Other (Explain)				

Other: BOSS/AMAS provides an electronic notification - First Notice of Death (FNOD) to VBA benefit systems: Compensation & Pension, Loan Guaranty, and Insurance & Education. FNOD contains privacy information needed for the sole purpose of identifying the deceased veteran, including social security number, claim number, and service number. VBA avoids paying millions of dollars in benefits to those no longer entitled according to federal regulation and speeds up processing of other benefits designed to help veteran families after the loss. FNOD serves to negate or reduce overpayments and subsequent collection activities.

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)	Mandatory	on the form
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	on the form
Service Information	Yes	VA Files / Databases (Identify file)	Mandatory	on the form
Medical Information				
Criminal Record Information				
Guardian Information				
Education Information				
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	on the form
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	Veteran Name, SSN, Address and Burial Location	PII	Assists with the proper management of benefit delivery.
Other Veteran Organization					
Other Federal Government Agency	Defense Manpower Data Center	Yes	Veteran Name, Address, SSN, Burial Location	PII	Assists with the administration of their database and file maintenance.
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: Automated Monument Application System (AMAS)

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**

- 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.

Answer: The system users at cemeteries have access to the personal information limited to what was entered by their facility. Except for the Veteran Information. That information is shared among all users. User access is restricted to the data of their facility and further limited by their position at the facility. Privacy information is housed on a centralized database. Access is provided by user id and password. User access is tracked and all users must take annual privacy training.

(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:

Answer: Functional requirements of the application were developed against NCA policy. The users are trained on the system. The system provides the necessary work flow process to limit the user to addressing only the necessary items.

How is data checked for completeness?

Answer: The system has edits and checks to verify entered data is not contradictory. The user is trained to also validate the information provided against system records or paper files.

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

Answer: The nature of the data makes it event specific and therefore it is to remain static.

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

Answer: The data related to eligibility must be validated against system records or paper files, i.e., DD214.

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?

Data is housed on line. Data is retained permanently.

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

Answer: Records have been approved by NARA to have sufficient historical value to warrant continued preservation by the Federal government.

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

Answer: Per the System of Record, records can be retained and disposed of in accordance with disposition authorization approved by the Archivist of the United States. NCA has elected not to eliminate any data; data is retained permanently.

Where are these procedures documented?

Answer: System of Record.

How are data retention procedures enforced?

Answer: NCA has elected to retain records permanently.

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: NARA is only interested in the records when they are to be retired from the system.

(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: Information is secured and protected via computer logins and passwords. A pass word is required for access to the VA and NCA network. A separate password is required for access to the application. VA standards are followed for computer login and password establishment and maintenance; access to the network and applications are granted on a need-to-know basis. A FISMA survey was last completed in July 2004. A C&A was completed 10/1/2004. The Authorization to Operate (ATO) was granted July 11, 2005. National cemeteries physically secure all paper records that contain privacy impact informatin and follow directives and guidelines on their destruction, which includes burning and shredding. When appropriate informatin is to be rreleased to the public, requests for such informatin are reviewed and information redacted, as needed, by NCA's Privacy Officer, Social Security numbers and service numbers of the deceased are not released to the public nor is any informatin on the next-of-kin without their expressed permission.

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

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

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: No changes were made to the IT system or collection of information after completing this PIA.

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 VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility' common security controls. These issues are identified and described in the system security plans for the individual information systems.

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.

(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)
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	

(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 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	GEN. MED. REC. - I/O	MEDICINE
CLINICAL CASE REGISTRIES	GEN. MED. REC. - VITALS	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	IFCAP	NOIS
DENTAL	IMAGING	NURSING SERVICE
DIETETICS	INCIDENT REPORTING	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
			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?		

OUTPATIENT PHARMACY

PAID
PATCH MODULE
PATIENT DATA EXCHANGE

PATIENT FEEDBACK

PATIENT REPRESENTATIVE

PCE PATIENT CARE
ENCOUNTER
PCE PATIENT/IHS SUBSET

PHARMACY BENEFITS
MANAGEMENT
PHARMACY DATA
MANAGEMENT
PHARMACY NATIONAL
DATABASE
PHARMACY PRESCRIPTION
PRACTICE
POLICE & SECURITY

PROBLEM LIST

PROGRESS NOTES

PROSTHETICS
QUALITY ASSURANCE
INTEGRATION
QUALITY IMPROVEMENT
CHECKLIST
QUASAR

RADIOLOGY/NUCLEAR
MEDICINE
RECORD TRACKING

REGISTRATION

RELEASE OF INFORMATION - DSSI

REMOTE ORDER/ENTRY
SYSTEM
RPC BROKER

RUN TIME LIBRARY
SAGG
SCHEDULING

SECURITY SUITE UTILITY PACK

SHIFT CHANGE HANDOFF
TOOL

SOCIAL WORK

SPINAL CORD DYSFUNCTION
SURGERY
SURVEY GENERATOR

TEXT INTEGRATION UTILITIES

TOOLKIT

UNWINDER

UTILIZATION MANAGEMENT ROLLUP

UTILIZATION REVIEW

VA CERTIFIED COMPONENTS - DSSI

VA FILEMAN

VBECs

VDEF

VENDOR - DOCUMENT STORAGE SYS

VHS&RA ADP TRACKING SYSTEM

VISIT TRACKING
VISTALINK

VISTALINK SECURITY

VISUAL IMPAIRMENT SERVICE TEAM
ANRV

VOLUNTARY TIMEKEEPING

VOLUNTARY TIMEKEEPING NATIONAL

WOMEN'S HEALTH

CARE TRACKER

(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?		

(HY 2010) PIA: Final Signatures

Locality Name:

0

Title:	Name:	Phone:	Email:
Privacy Officer:	Will Lewis	202-461-6746	willc.lewis@va.gov


Digital Signature: Will Lewis

Information Security Officer:

Bernadette Bowen Welch

202-461-8173

bernadette.bowen-welch1@va.gov

BERNADETTE BOWEN WELCH


Digital Signature: Bernadette Bowen Welch

Chief Information Officer:

William Hyman

703-441-0427

w.l.hyman@va.gov


Digital Signature: William Hyman

Privacy Compiling Department:

Willie Lewis

702-401-6746

willc.lewis@va.gov


Digital Signature: Willie Lewis

System / Application / Program Manager:

Joe Kosari

402-461-9874

joe.kosari@va.gov


Digital Signature: Joe Kosari

Date of Report:

6/1/2010

GMN File Que Project Ident #:

U29-00-02-406-D1 1120 00
Buria Operations Support System
180SS1-2009

Project Name: