

(FY 2010) PIA: System Identification

Program or System Name: Regional 5>VBA>St. Paul
 Region>VARO Cleveland RO
 LAN(LAN)

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1028-00-404-139

The Regional Office (RO) Local Area Network (LAN) serves as the default repository for incidental data used and processed by various VBA Major Applications. This data is used in granting compensation, pension, education, vocational rehabilitation and employment, insurance and loan guaranty benefits to veterans. Information stored also includes data used for various administrative functions. The system provides RO employees local access to file and print sharing services on the LAN. It also provides client access to various

Description of System / Application / Program: applications, including email.

Facility Name: VARO Cleveland (325)

Title:	Name:	Phone:	Email:
Privacy Officer:	Larry Zietlow	(216) 522-3530 x3421	laurance.zietlow@va.gov
Information Security Officer:	Don Kennett & Ray Burns	(216) 522-3530 x3710 / x 3202	donald.kennett@va.gov / ray.burns2@va.gov
Chief Information Officer:	Christine Wilson	(216) 522-3530 x 3729	christine.wilson2@va.gov

Person Completing Document:	Don Kennett & Larry Zietlow	(216) 522-3530	donald.kennett@va.gov
		X3710 / x3421	laurance.zietlow@va.gov
Record Management Officer	Ron Whitcomb	(216) 522-3530	
System Owener	Kevin C. Causley	x3402	ron.whitcomb@va.gov
C&A Coordinator	Mary D. Barley	(202) 461-9170	kevin.causley@va.gov
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	06/2009	(202) 461-9175	mary.barley@va.gov
Date Approval To Operate Expires:	08/2011		

What specific legal authorities authorize this program or system: Title 38 of the United States Code

What is the expected number of individuals that will have their PII stored in this system:
1,000,000 - 1,500,000

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. 06/1997

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): 06/2010

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?

- 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):

58VA21/22

2. Name of the System of Records:

Compensation, Pension, Education, and
Rehabilitation Records-VA

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

<http://vaww.va.gov/privacy/systemsofrecords>

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

No

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)	ALL	Benefits	All	All
Family Relation (spouse, children, parents, grandparents, etc)	ALL	Benefits	All	All
Service Information	ALL	Benefits	All	All
Medical Information	ALL	Benefits	All	All
Criminal Record Information	ALL	Benefits	All	All
Guardian Information	ALL	Benefits	All	All
Education Information	ALL	Benefits	All	All
Benefit Information	ALL	Benefits	All	All
Other (Explain)	N/A	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)	Voluntary	none
Family Relation (spouse, children, parents, grandparents, etc)	Yes	VA Files / Databases (Identify file)	Voluntary	none
Service Information	Yes	VA Files / Databases (Identify file)	Voluntary	none

Medical Information	Yes	VA Files / Databases (Identify file)	Voluntary	none
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Voluntary	none
Guardian Information	Yes	VA Files / Databases (Identify file)	Voluntary	none
Education Information	Yes	VA Files / Databases (Identify file)	Voluntary	none
Benefit Information	Yes	VA Files / Databases (Identify file)	Voluntary	none
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	VARO Cleveland	Yes	Determination of VA Benefits	Both PII & PHI	VA Directive 6500
Other Veteran Organization	Various - Service Organizations	Yes	Claims Filing	Both PII & PHI	Service agreement at VACO
Other Federal Government Agency	Defense Finance and Accounting	Yes	Veterans Pay Information	PII	Service Agreement at VACO
State Government Agency	State Offices	Yes	Claims Filing	Both PII & PHI	Service Agreement at VACO
Local Government Agency	County Veterans Service Organization	Yes	Claims Filing	Both PII & PHI	Service Agreement at VACO
Research Entity	N/A				
Other Project / System	N/A				
Other Project / System	N/A				
Other Project / System	N/A				

(FY 2010) PIA: Access to Records

Does the system gather information from another system? No
 Please enter the name of the system:

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?

No

if yes, please check all that apply:

- Drug/Alcohol Counseling Mental Health HIV
 Research Sickle Cell 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?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Information is collected primarily on defined forms and entered to specific fields of database records. The required veteran's data is stored within the database(s) which support the individual claim or claims the veteran has been granted.

Answer:

How is data checked for completeness?

Answer:

Data is checked for completeness by system audits, manual verifications and annual questionnaires through automated veteran letters. These letters ask specific questions for verification based on the existing entitlement or benefit the veteran is receiving. Also, data is updated with each veteran correspondence.

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

Answer:

Data is updated as a result of returned mail, or returned direct deposits, or through contact with the veteran, beneficiary, or power of attorney. Additionally, verifications and system audits are performed.

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

Answer:

All data is matched against supporting claims documentation submitted by the veteran, widow, or dependent. Certain data such as SSN is verified with the social Security Administration. Prior to any award or entitlement authorization(s) by the VBA, the veteran record is manually reviewed and data validated to ensure correct entitlement has been approved.

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 retained on all VBA systems indefinitely.

Answer:

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

For veterans benefits.

Answer:

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

Data is not eliminated but stored on removable media.

Answer:

Where are these procedures documented?

Procedures are documented in the Disaster Recover and Continuity of Operations (COOP) plans for the respective data centers where the data is housed.

Answer:

How are data retention procedures enforced?

Answer:

Enforcement procedures are documented in the Disaster Recover and Continuity of Operations (COOP) plans for the respective data centers where the data is housed.

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

Yes

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

Answer:

(FY 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:

A PIA is required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of Personally Identifiable Information (PII) of the public or that make substantial changes to existing technology for managing information of the public in identifiable form. The assessment of risk and the development of system security plans are two important activities in an Information Security program that directly support security accreditation and are required by FISMA and OMB Circular A-120, Appendix III.

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

- | | |
|---------------------------------------------------------------|----------------------------------------------------------------|
| <input checked="" type="checkbox"/> Air Conditioning Failure | <input checked="" type="checkbox"/> Hardware Failure |
| <input type="checkbox"/> Chemical/Biological Contamination | <input type="checkbox"/> Malicious Code |
| <input type="checkbox"/> Blackmail | <input checked="" type="checkbox"/> Computer Misuse |
| <input type="checkbox"/> Bomb Threats | <input checked="" type="checkbox"/> Power Loss |
| <input type="checkbox"/> Cold/Frost/Snow | <input type="checkbox"/> Sabotage/Terrorism |
| <input type="checkbox"/> Communications Loss | <input checked="" 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)*

- | | |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <input type="checkbox"/> Risk Management | <input type="checkbox"/> Audit and Accountability |
| <input checked="" type="checkbox"/> Access Control | <input checked="" type="checkbox"/> Configuration Management |
| <input checked="" type="checkbox"/> Awareness and Training | <input checked="" type="checkbox"/> Identification and Authentication |
| <input checked="" type="checkbox"/> Contingency Planning | <input type="checkbox"/> Incident Response |
| <input checked="" type="checkbox"/> Physical and Environmental Protection | <input type="checkbox"/> Media Protection |
| <input type="checkbox"/> Personnel Security | |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments | |

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:

The PIA analysis seeks to identify and mitigate the privacy and security risks associated with the use of PII by a program, system, or practice. It provides a framework for examining whether privacy, security and other vital data stewardship issues have been identified, addressed, and incorporated into the plan, design, operation, maintenance, and disposal of electronic information systems.

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
X			VA Reserve Educational Assistance Program	CONDO PUD Builder
X	LGY Processing		Web Automated Verification of Enrollment	Centralized Property Tracking System
X	Loan Service and Claims		Right Now Web	Electronic Appraisal System
	LGY Home Loans		VA Online Certification of Enrollment (VA-ONCE)	Web LGY
X	Search Participant Profile (SPP)		Automated Folder Processing System (AFPS)	Access Manager
X	Control of Veterans Records (COVERS)		Personal Computer Generated Letters (PCGL)	SAHSHA
X	SHARE	X	Personnel Information Exchange System (PIES)	VBA Data Warehouse
X	Modern Awards Process Development (MAP-D)	X	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)
X	Rating Board Automation 2000 (RBA2000)	X		
X				Enterprise Wireless Messaging System (Blackberry)
	State of Case/Supplemental (SOC/SSOC)		SHARE	VBA Enterprise Messaging System
X			State Benefits Reference System	
X	Awards		Training and Performance Support System (TPSS)	LGY Centralized Fax System
	Financial and Accounting System (FAS)		Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)
X	Eligibility Verification Report (EVR)		Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)
X	Automated Medical Information System (AMIS)290			
X			Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
	Web Automated Reference Material System (WARMS)			

X	Automated Standardized Performance Elements Nationwide (ASPEN)		Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
	Inquiry Routing Information System (IRIS)	X	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
X	National Silent Monitoring (NSM)	X	Compensation and Pension (C&P) Record Interchange (CAPRI)	Purchase Order Management System (POMS)
	Web Service Medical Records (WebSMR)	X	Control of Veterans Records (COVERS)	Veterans Canteen Web
X	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
X	Veterans Exam Request Info System (VERIS)		Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS
X	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
		<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?		



Baker System		Veterans Assistance Discharge System (VADS)
Dental Records Manager		VBA Training Academy
Sidexis	X	Veterans Service Network (VETSNET) Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Priv Plus Mental Health Asisstant	X	BIRLS Centralized Accounts Receivable System (CARS)
Telecare Record Manager		
Omnicell	X	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 Post Vietnam Era educational Program (VEAP) CH 32		INS - BIRLS Mobilization 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	MYHEALTHEVET
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.

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

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?		
<input type="checkbox"/> 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?		
<input type="checkbox"/> If yes, where?		
<input type="checkbox"/> Who has access to this data?		

Minor app #3



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	UNWINDER
ENCOUNTER	UTILIZATION MANAGEMENT ROLLUP
PCE PATIENT/IHS SUBSET	
PHARMACY BENEFITS	UTILIZATION REVIEW
MANAGEMENT	
PHARMACY DATA	VA CERTIFIED COMPONENTS - DSSI
MANAGEMENT	
PHARMACY NATIONAL	VA FILEMAN
DATABASE	
PHARMACY PRESCRIPTION	VBECs
PRACTICE	
POLICE & SECURITY	VDEF
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	VISIT TRACKING
QUALITY ASSURANCE	VISTALINK
INTEGRATION	
QUALITY IMPROVEMENT	VISTALINK SECURITY
CHECKLIST	
QUASAR	VISUAL IMPAIRMENT SERVICE TEAM
	ANRV

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

VOLUNTARY TIMEKEEPING

VOLUNTARY TIMEKEEPING NATIONAL

WOMEN'S HEALTH

CARE TRACKER

(FY 2010) PIA: Minor Applications

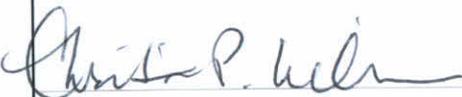
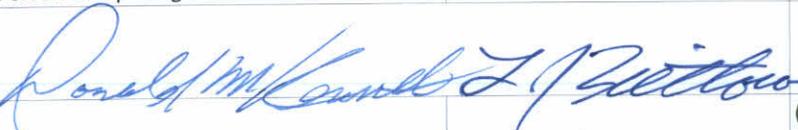
Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

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?			

(FY 2010) PIA: Final Signatures

Facility Name:	VARO Cleveland (325)		
Title:	Name:	Phone:	Email:
Privacy Officer:	Larry Zietlow	(216) 522-3530 x3421	laurance.zietlow@va.gov
			
Information Security Officer:	Don Kennett & Ray Burns	(216) 522-3530 x3710 / x 3202	donald.kennett@va.gov / ray.burns2@va.gov
			
Chief Information Officer:	Christine Wilson	(216) 522-3530 x 3729	christine.wilson2@va.gov
			
Person Completing Document:	Don Kennett & Larry Zietlow	(216) 522-3530 X3710 / x3421	donald.kennett@va.gov laurance.zietlow@va.gov
			
Record Management Officer	Ron Whitcomb	(216) 522-3530 x3402	ron.whitcomb@va.gov
			
System Owner	Kevin C Causley	(202) 461-9170	kevin.causley@va.gov
Date of Report:	01/00/1900		
OMB Unique Project Identifier	029-00-02-00-01-1028-00-404-139		
Project Name	Regional 5>VBA>St. Paul Region>VARO Cleveland RO LAN(LAN)		