(FY 2011) PIA: System Identification

Program or System Name:	VACO > VA Enterprise Wide Area Network (VA EWAN)		
OMB Unique System / Application / Program Identifier	(AKA: UPID #):		029-00-02-00-01-1120-00
Description of System/ Application/ Program:	The Enterprise Wide Area Network (EWAN) infrastructure extends delivery of IP based services to a geographic matrix of 7 regional network administrative domains; it provides a national telecommunications resource that supports all Department business lines. The EWAN supports VA's strategic & enabling goals to create a One-VA Information Technology Framework to carry out the Department's mission. It integrates all VA business units under a single enterprise network topology. The EWAN essentially consists of three separate functional layers that are codependent & interrelated; the core, distribution & access layers. The EWAN is based on a hierarchical network.		
Facility Name:	VA Central Office		
Title:	Name:	Phone:	Email:
Privacy Officer:	Garnett Best	202-461-7474	garnett.best@va.gov
Information Security Officer:	Cassandra Wait	202-461-6385	cassandra.wait@va.gov
System Owner/ Delegation of Authority	Horace Blackman	202-461-7457	horace.blackman@va.gov
Other Titles: System Owner	Steven Pirzchalski	202-461-5910	steven.pirzchalski@va.gov
Other Titles:			
Person Completing Document:	Jose Rincon	202-461-5900	jose.rincon@va.gov
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)			08/2010
Date Approval To Operate Expires:			04/2011
What specific legal authorities authorize this program or system:			Title 38, U.S. Code, Section 7301(a) - VA Directive
What is the expected number of individuals that will have their PII stored in this system:			None
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.			01/1980
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):			06/2011

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

☐ Have any changes been made to the system since the last PIA?

☐ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?

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

If there is no Personally Identifiable Information on your system , please complete TAB 2 & TAB 12. (See Comment for Definition of PII)

(FY 2011) PIA: System of Records

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

(FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	N/A			
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	N/A			
Medical Information	N/A			
Criminal Record Information				
Guardian Information	N/A			
Education Information	N/A			
Benefit Information	N/A			
Other (Explain)	N/A			

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	No			N/A
Family Relation (spouse, children, parents, grandparents, etc)	No			N/A
Service Information	No			N/A

Medical Information	No	N/A
Criminal Record Information	No	N/A
Guardian Information	No	N/A
Education Information	No	N/A
Benefit Information	No	N/A
Other (Explain)	No	N/A
Other (Explain)	No	N/A
Other (Explain)	No	N/A

(FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization		No		N/A	
Other Veteran Organization		No		N/A	
Other Federal Government Agency		No		N/A	
State Government Agency		No		N/A	
Local Government Agency		No		N/A	
Research Entity		No		N/A	
Other Project / System		No		N/A	
Other Project / System		No		N/A	
Other Project / System		No		N/A	

(FY 2011) 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?

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 2011) 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 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public? No

If Yes, Please Specify: Not applicable. No PIA

Explain how collected data are limited to required elements:

Answer: Not applicable. No PIA

How is data checked for completeness?

Answer: Not applicable. No PIA

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

Answer: Not applicable. No PIA

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

Answer: Not applicable. No PIA

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

Answer:

(FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: Not applicable. No PIA

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

Answer: Not applicable. No PIA

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

Answer: Not applicable. No PIA

Where are these procedures documented?

Answer: Not applicable. No PIA

How are data retention procedures enforced?

Answer: Not applicable. No PIA

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:

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

Will information be collected through the internet from children under age 13? No

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

Answer:

(FY 2011) PIA: Security

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

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

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

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

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

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

Answer:

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

If 'No' please describe why:

Answer:

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

Answer:

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

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

Answer: (Other Risks)

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

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

Answer: (Other Controls)

PIA: PIA Assessment

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

Answer:

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. ☐ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. ☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☐ The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. ☐ The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. ☐ The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**	☐ The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. ☐ The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals. ☐ The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

(FY 2011) PIA: Final Signatures

Facility Name: VACO > VA Enterprise Wide Area Network (VA EWAN)

Title:	Name:	Phone:	Email:
Privacy Officer:	Garnett Best	202-461-7474	garnett.best@va.gov
John Buck for 6/30/2011			
Information Security Officer:	Cassandra Wait	202-461-6385	cassandra.wait@va.gov
Cassandra Wait 6/30/11			
System Owner/ Delegation of Authority	Horace Blackman	202-461-7457	horace.blackman@va.gov
for Celeste L. Matthews 6/30/11			
Other Titles: System Owner	Steven Pirzchalski	202-461-5910	steven.pirzchalski@va.gov
Steven C Pirzchalski 6/29/11			
Other Titles:	Jose Rincon	202-461-5900	jose.rincon@va.gov
José Luis Rincón 6/29/11			

Date of Report:	6/29/11
OMB Unique Project Identifier	029-00-02-00-01-1120-00
Project Name	VACO > VA Enterprise Wide Area Network (VA EWAN)