

Welcome to the PIA for FY 2012!		
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.		Macros Must Be Enabled To Use Full Functionality For This Form Template!
		Microsoft Office 2003: 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. Or 1) When file opens click on Enable Macros at the prompt.
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.		Microsoft Office 2007: To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable All Macros; 2) Click OK
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.		<u>Final Signatures</u>
		Final signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.
Directions:		Privacy Impact Assessment Uploaded into SMART
VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. 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.		All PIA Validation Letters should be mailed to Christina.Pettit@va.gov to receive full credit for submission.
INTERNAL WEBSITE : http://vaww.privacy.va.gov/PIA.asp		Various Privacy Data Websites:
EXTERNAL WEBSITE : http://www.privacy.va.gov/PRIVACY/Privacy_Impact_Assessment.asp		SORNs : http://www.rms.oit.va.gov/SOR_Records.asp
		Directive Itself (6508): http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=414&FTYPE=2
Roles and Responsibilities:		Schedule FY 2012 : http://www.privacy.va.gov/PRIVACY/Privacy_Impact_Assessment.asp
Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.		
a. Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508		
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 Directive 6508 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. Chief Information Officer (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 reviewing and approving the PIA before submission to the Privacy Service.		
Definition of PII (Personally Identifiable Information)		
Personally Identifiable Information (PII) is —any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.		
Examples of PII include, but are not limited to:		
• Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card		
• Address information, such as street address or email address		
• Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)		
• Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).		
Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.		
A "routine use" is a Privacy Act discretionary authority published in the Federal Register that permits VA to disclose information or records from a Privacy Act-protected record without the patient's prior signed authorization. A "routine use" permits the:		
(1) Release of PHI only when disclosure is also authorized by other applicable legal authorities, including 45 CFR Parts 160 and 164;		
(2) Release of drug or alcohol abuse, HIV, or sickle cell anemia medical information only when the disclosure is also authorized by 38 U.S.C. 7332.		

(FY 2012) PIA: System Information		*Green Highlight = Must Answer Question	*Yellow Highlight = Required to Sign PIA
Program or System Name (as shown in SMART):		Federal Case Management Tool (FCMT)	
OMB Unique System / Application / Program Identifier (UPID #):	(AKA: 029-888888105		
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)" ***Do not type more than allotted space!!!**		The Federal Case management Tool (FCMT) and associated database supports both the Veterans Health Administration (VHA) and the Veterans Benefits Administration (VBA) branches of the Department of Veterans Affairs (VA). FCMT provides the VA tracking information on members of the armed forces who will be transferred from a Department of Defense (DoD) Military Treatment Facility (MTF) to a VA health facility in the future or who already have Veteran status. The FCMT will provide tracking of the Veteran/Service member arrival at the initial VA health facility and provides date and location information for subsequent transfers to other health facilities. In addition, VTA obtains data about patient history from the imported DoD Theater Medical Data Store (TMDS). In addition to the Veteran patient population, FCMT will record benefit tracking information for all severely injured Veterans requesting benefits. This history includes all benefit award details to include application dates, award decisions, dates and amounts. The FCMT will track Service members and Veterans disability claims through the Disability Eligibility System (DES) pilot module. The purpose of the FCMT is to track the initial arrival of a Service member into the VA health system and their subsequent movement among VA health facilities, as well as monitor benefits application and administration details.	
Facility or Program Office Name:		Terremark Worldwide Inc. Culpeper, VA	
Title:	Name:	Phone:	Email:
Privacy Officer:	Garnett Best	(202)-632-7378	Garnett.Best@va.gov
Information Security Officer:	Perry Ungson	(415)-221-4810 Ext 6375, Cell # (650)-444-6444	Perry.Ungson@va.gov
System Owner/Delegate:	Lorraine Landfried	(202)-632-4347 (202)-461-9170	lorraine.landfried@va.gov
Chief Information Officer / Program Manager:	Dick Rickard	(352)-686-3227	Dick.Rickard@va.gov
Information Owner:	Joe Paiva	(202)-461-9035	Joe.Paiva@VA.gov
Other Titles:			
Person Completing Document:	James Dolan	(732)-290-9033	jdolan@caci.com
Other Titles:			
Date of Last Full Approved PIA by VACO Privacy Services: (MM/YYYY)			N/A
What specific legal authorities authorize this program or system:		sections 501(a), 1705, 1710, 1722,	
What is the expected number of individuals that will have their PII stored in this system:		Currently 36,000 records. Annual	
Identify what stage the System / Application / Program is at:		Development/Acquisition	
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.		3/19/2011	
Is there an authorized change control process which documents any changes to existing applications or systems?		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PI	
If No, (Explain on Tab 8)			
Is there a contingency plan in place to process information when the system is down?		<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PI	
Has a PIA been completed within the last three years?		<input type="radio"/> Yes <input checked="" type="radio"/> No <input type="radio"/> N/A : First PI	
FISMA QUESTIONS			
1. System Information			

1. Is this a new system?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
2. Does this system contain Federal information in identifiable form?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
3. Does the system include information on the public?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
4. Is there a Privacy Impact Assessment (PIA) that covers this system?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> National Security System under 40 U.S.C. 11103, a PIA is not required for this system			
5. Is Federal-owned information in this system retrieved by name or unique	<input checked="" type="radio"/> Yes <input type="radio"/> No			
6. What is the System of Records Notice (SORN) for this system?				
7. Has this SORN been reviewed or updated within the last three years?	No, it is a new SORN			
Date of Report (MM/YYYY):			3-Feb-12	
Any check mark in the boxes below will require a full PIA. Please continue to the next TAB and complete the remaining questions.				
If there is no Personally Identifiable Information on your system , please complete TAB 2 & TAB 12. (See Comment for Definition of PII)				
<input checked="" type="checkbox"/>	Have any changes been made to the system since the last PIA?			
<input type="checkbox"/>	Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?			
<input checked="" type="checkbox"/>	Will this system/application/program retrieve information on the basis of name, unique identifier, symbol or other PII data?			
<input checked="" type="checkbox"/>	Does this system/application/program collect, store, or disseminate PII/PHI data?			
<input checked="" type="checkbox"/>	Does this system/application/program collect, store or disseminate the SSN?			
Directions				

(FY 2012) PIA: System of Records

*Green Highlight = Must Answer Question

- 1. Is a SORN (System of Records Notice) Required?
- 2. Is there a SORN already in place?

Yes No Not Sure
 Yes No

***If Yes, select all of the appropriate SORN number(s):
 ***If Not Sure, continue to question 3

***Click to add. Delete SORN by highlighting SORN and comma if included and press the Delete key or place focus on area to delete all SORNs.

LIST OF SORN NUMBER(S) :

163VA005Q3
 SRON # 163VA005Q3 - Is within the VAIQ concurrence process.

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

- 3. If records are retrieved using any of the following entities, A SORN will be required (Please check all that apply)

<input checked="" type="checkbox"/> Full Name
<input checked="" type="checkbox"/> Maiden Name
<input checked="" type="checkbox"/> Mother's Maiden Name
<input checked="" type="checkbox"/> Alias
<input checked="" type="checkbox"/> Social Security Number
<input checked="" type="checkbox"/> Passport Number
<input checked="" type="checkbox"/> Driver's License Number
<input checked="" type="checkbox"/> Taxpayer Identification Number
<input checked="" type="checkbox"/> Financial Account Number
<input checked="" type="checkbox"/> Credit Card Number
<input checked="" type="checkbox"/> Street Address
<input checked="" type="checkbox"/> Email Address
<input checked="" type="checkbox"/> Photographic Image
<input checked="" type="checkbox"/> Fingerprints
<input checked="" type="checkbox"/> Handwriting
<input checked="" type="checkbox"/> Other Biometric Data
<input type="checkbox"/> Other (Explain on Tab 8)

- 4. Based on Question 3, is a SORN required?

Yes No
 Yes No

***If Yes, has the process begun to obtain/acquire a SORN

Location where the specific applicable System of Records Notice may be accessed:

http://www.rms.oit.va.gov/SOR_Records.asp

(FY 2012) PIA: Data Collection And Storage				
*Green Highlight = Must Answer Question				
Please fill in each column for the data types selected.				
Data Type	Collection Method	What are the subjects told about the intended use of their information?	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)	VA File Database	Healthcare	Verbal/Automatic	Written
Family Relation (spouse, children, parents, grandparents, etc)				
Service Information				
Medical Information				
Criminal Record Information				
Guardian Information				
Education Information				
Benefit Information				
Other (Explain on Tab 8)				
Data Type	Storage Method	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Files/Databases (Identify File)	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary	
Family Relation (spouse, children, parents, grandparents, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Other Federal Agency (DEERS)	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Service Information	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Medical Information	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Criminal Record Information	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Guardian Information	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Education Information	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Benefit Information	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Other (Explain on Tab 8)	<input checked="" type="radio"/> Yes <input type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
	(Please Select Yes/No)			
Proximity and Timing: Is the privacy notice provided at the time of data collection?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
	routine use(s)			

(FY 2012) PIA: Data Sharing *Green Highlight = Must Answer Question	** Any connection external to VA requires an ISA/MOU per VA 6500. This section below must be consistent with your System Security Plan Interconnection Security Agreement section.				
Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	Coordinator (FRC)	<input checked="" type="radio"/> Yes <input type="radio"/> No	Healthcare	<input type="radio"/> Yes <input checked="" type="radio"/> No	Internal
Other Veteran Organization		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Other Federal Government Agency		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
State Government Agency		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Local Government Agency		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Research Entity		<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
<input type="checkbox"/> Other Project/ System (Explain on Tab 8)					
(FY 2012) PIA: Access to Records					
Does the system gather information from another system?		<input checked="" type="radio"/> Yes <input type="radio"/> No			
Please enter the name of the system:		DEERS			
(FY 2012) PIA: Secondary Use					
Will PII data be included with any secondary use request?		<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="checkbox"/> Mental Health	<input type="checkbox"/> HIV	<input type="checkbox"/> Drug/Alcohol Counseling
Check all that apply			<input type="checkbox"/> Sickle Cell	<input type="checkbox"/> Other (Explain on Tab 8)	<input type="checkbox"/> Research

(FY 2012) PIA: Records Management		*Green Highlight = Must Answer Question	
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?			
<input type="radio"/> Yes (Explain on Tab 8) <input checked="" type="radio"/> No			
Is the data collected to only what is necessary to provide requested service?			
<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)			
Has the data provided been verified as complete?			
<input checked="" type="checkbox"/> Veteran Verified <input type="checkbox"/> Received From Database <input type="checkbox"/> Verification Unknown			
(FY 2012) PIA: Retention & Disposal			
What is the data retention period?		RCS 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf	
Answer: 75 Years. Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is		RCS VB-1, Part II Revised for VBA: www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/part2.pdf	
		National Archives and Records Administration: www.nara.gov	
Explain why the information is needed for the indicated retention period?			
Answer: Health Care information, needed for life of the Veteran			
What are the procedures for eliminating data at the end of the retention period?			
Answer: Electronic Final Version of Patient Medical Record is destroyed 75 years after the last			
Where are these procedures documented?			
Answer: Veterans Health Administration Records Control Schedule 10-1			
How are data retention procedures enforced?			
Answer: Records Management Responsibilities The Health Information Resources Service (11IRS) is responsible for developing			
Has the retention schedule been approved by the National Archives and Records Administration (NARA)			
<input checked="" type="radio"/> Yes <input type="radio"/> No (Explain on Tab 8)			
(FY 2012) PIA: Children's Online Privacy Protection Act (COPPA)			
Will information be collected through the internet from children under age 13?			
<input type="radio"/> Yes (Explain on Tab 8) <input checked="" type="radio"/> No			

(FY 2012) PIA: Security *Green Highlight = Must Answer Question

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 No (Explain on Tab 8)

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls? Yes No (Explain on Tab 8)

Is security monitoring conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information? Yes No (Explain on Tab 8)

Is security assessment conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information? Yes No (Explain on Tab 8)

Is adequate physical security in place to protect against unauthorized access? Yes No (Explain on Tab 8)

*Ensure PE 2, PE-3, PE-6, PE-7, PE-8 have been addressed appropriately for your categorization

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

<input checked="" type="checkbox"/> Biological Release	<input checked="" type="checkbox"/> Fire	<input checked="" type="checkbox"/> Lightning Strike	<input checked="" type="checkbox"/> Terrorism
<input type="checkbox"/> Blizzard	<input checked="" type="checkbox"/> Flood	<input checked="" type="checkbox"/> Malicious Code	<input checked="" type="checkbox"/> Thunderstorm
<input checked="" type="checkbox"/> Burglary/Break In	<input checked="" type="checkbox"/> Hacker, Cracker	<input checked="" type="checkbox"/> Password Privacy Negligence	<input checked="" type="checkbox"/> Tornado
<input checked="" type="checkbox"/> Civil Unrest	<input checked="" type="checkbox"/> Hail	<input checked="" type="checkbox"/> Personnel Unavailable	<input checked="" type="checkbox"/> Tsunami
<input checked="" type="checkbox"/> Component Failure	<input checked="" type="checkbox"/> HAZMAT Release/Spill	<input checked="" type="checkbox"/> Power Failure	<input checked="" type="checkbox"/> User Negligence
<input type="checkbox"/> Dam Failure	<input checked="" type="checkbox"/> Human Health Emergency	<input checked="" type="checkbox"/> Sabotage	<input checked="" type="checkbox"/> User Sabotage
<input type="checkbox"/> Dust/Debris	<input checked="" type="checkbox"/> Hurricane	<input checked="" type="checkbox"/> System Intrusion, Break-Ins	<input checked="" type="checkbox"/> Vibration
<input checked="" type="checkbox"/> Earthquake	<input checked="" type="checkbox"/> HVAC Failure	<input checked="" type="checkbox"/> System Misconfiguration	<input type="checkbox"/> Volcano
<input checked="" type="checkbox"/> Extreme Cold	<input checked="" type="checkbox"/> Indoor Humidity	<input checked="" type="checkbox"/> System Penetration	<input checked="" type="checkbox"/> Water Damage
<input checked="" type="checkbox"/> Extreme Heat	<input type="checkbox"/> Landslide	<input checked="" type="checkbox"/> System Tampering	<input checked="" type="checkbox"/> Winter Weather Hazards

*If any other risks identified, explain in Tab 8

Based upon the risks identified above, Explain what security controls are being used to mitigate these risks. (Check all that apply)

<input checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Configuration Management	<input checked="" type="checkbox"/> Media Protection	<input checked="" type="checkbox"/> System and Services Acquisition
<input checked="" type="checkbox"/> Audit and Accountability	<input checked="" type="checkbox"/> Contingency Planning	<input checked="" type="checkbox"/> Personnel Security	<input checked="" type="checkbox"/> System and Communication Protection
<input checked="" type="checkbox"/> Awareness and Training	<input checked="" type="checkbox"/> Identification and Authentication	<input checked="" type="checkbox"/> Physical and Environmental Protection	<input checked="" type="checkbox"/> System and Information Integrity
<input checked="" type="checkbox"/> Security Assessment and Authorization	<input checked="" type="checkbox"/> Incident Response	<input checked="" type="checkbox"/> Risk Assessment	<input checked="" type="checkbox"/> Planning
			<input checked="" type="checkbox"/> Maintenance

Answer: (Other Controls) Explain on Tab 8

PIA: PIA Assessment

Based upon NIST 800-60, volume II; List the Information data types chosen as a basis for your FIPS 199 System Categorization.

Answer:

<p><u>Availability Assessment:</u> 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)</p>	<input type="checkbox"/> 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. <input type="checkbox"/> The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. <input checked="" type="checkbox"/> The potential impact is low if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
<p><u>Integrity Assessment:</u> If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? (Choose One)</p>	<input type="checkbox"/> 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. <input checked="" type="checkbox"/> The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
<p><u>Confidentiality Assessment:</u> If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? (Choose One)</p>	<input type="checkbox"/> 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. <input checked="" type="checkbox"/> The potential impact is moderate if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals. <input type="checkbox"/> The potential impact is low if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments? The 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.

(FY 2012) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

Federal Information Processing Standard 199 (FIPS 199) Categorization of the Federal Case Management Tool (FCMT) as a Moderate Risk

1. Per VA Directive 6500 and VA Handbook 6500, each system must have a FIPS 199 risk categorization completed as part of the Certification & Accreditation process. This memo documents and substantiates the rationale for categorizing FCMT as a Moderate versus a High risk.

2. Background: All VA information systems must have a security categorization in accordance with FIPS 199 and must document the results of this categorization in the system security plan. Within the FCMT System Security Plan, this categorization is detailed in Appendix N. Upon completion of the SSP, designated VA IPRM staff review and approve the security categorizations as part of the C&A process in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. For nationally deployed information systems, the FIPS 199 categorization will be made by OI&T system development and will be approved during the C&A process of the system prior to deployment to the field. Further, the VA CISO can recommend to the CIO, as part of the C&A process, to make a particular system medium categorization, rather than high, based on current policy. OCS Policy are revising 6500 to remove the statement that VA sensitive information mandates high categorization and instead will defer to the individual System Security Plan.

3. In performing the FCMT review, the Warrior Support Information Assurance team used National Institute of Standards and Technology (NIST) 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, Appendix D: Impact Determination for Mission-Based-Information and Information Systems, paragraph D.14.4 for Health Care Delivery Services Information Type on pages 171 and 172 as baseline information for the risk categorization of FCMT. The NIST paragraph states:

“Health Care Delivery Services provides and supports the delivery of health care to its beneficiaries. This includes assessing health status; planning health services; ensuring quality of services and continuity of care; and managing clinical information and documentation. The recommended provisional security categorization for health care delivery services information is as follows:

Security Category = {(confidentiality, Low), (integrity, High), (availability, Low)}

Confidentiality: The confidentiality impact level is the effect of unauthorized disclosure of health care delivery services on the ability of responsible agencies to provide and support the delivery of health care to its beneficiaries will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Some information associated with health care involves confidential patient information subject to the Privacy Act and to HIPAA. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Other information (e.g., information proprietary to hospitals, pharmaceutical companies, insurers, and care givers) must be protected under rules governing proprietary information and procurement management. In some cases, unauthorized disclosure of

(FY 2012) PIA: VBA Minor Applications

Which of these are sub-components of your system?		
Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial		Automated Medical Information Exchange II (AIME II)
Agent Orange	BCMA Contingency Machines	Automated Medical Information System (AMIS)290
Appraisal System	Centralized Property Tracking System	Automated Standardized Performance Elements Nationwide (ASPEN)
ASSISTS	Common Security User Manager (CSUM)	Broome Closet
Awards	Compensation and Pension (C&P)	Centralized Accounts Receivable System (CARS)
Baker System	Control of Veterans Records (COVERS)	Committee on Waivers and Compromises (COWC)
	Courseware Delivery System (CDS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Dental Records Manager	
	Education Training Website	Compensation & Pension Training Website
C&P Payment System	Electronic Appraisal System	Distribution of Operational Resources (DOOR)
C&P Training Website	Electronic Card System (ECS)	Educational Assistance for Members of the Selected Reserve Program CH 1606
	Electronic Payroll Deduction (EPD)	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Eligibility Verification Report (EVR)	Enterprise Wireless Messaging System (Blackberry)
	Fiduciary Beneficiary System (FBS)	Financial Management Information System (FMI)
EndoSoft	Fiduciary STAR Case Review	Hearing Officer Letters and Reports System (HOLAR)
FOCAS	Financial and Accounting System (FAS)	Inquiry Routing Information System (IRIS)
Inforce	Insurance Unclaimed Liabilities	
INS - BIRLS	Inventory Management System (IMS)	Modern Awards Process Development (MAP-D)
Insurance Online	Interactive Voce Response (IVR)	Personal Computer Generated Letters (PCGL)
Insurance Self Service	LGY Centralized Fax System	Personnel Information Exchange System (PIES)
LGY Home Loans	Loan Service and Claims	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing		Purchase Order Management System (POMS)
MES	Loan Guaranty Training Website	Reinstatement Entitlement Program for Survivors (REAPS)
Mobilization	Mental Health Assistant	Reserve Educational Assistance Program CH 1607
Montgomery GI Bill	National Silent Monitoring (NSM)	RightFax
MUSE	Powerscribe Dictation System	Service Member Records Tracking System
Omnicell	Rating Board Automation 2000 (RBA2000)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Records Locator System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Remittance Processing System	Training and Performance Support System (TPSS)
Right Now Web	Review of Quality (ROQ)	VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	Search Participant Profile (SPP)	
Script Pro	Spinal Bifida Program Ch 18	VA Reserve Educational Assistance Program
SHARE	State Benefits Reference System	Veterans Assistance Discharge System (VADS)
Sidexis	State of Case/Supplemental (SOC/SSOC)	Veterans Exam Request Info System (VERIS)
Synquest	Telecare Record Manager	Veterans Insurance Claims Tracking and Response System (VICTARS)
VBA Training Academy	VBA Enterprise Messaging System	Veterans Service Representative (VSR) Advisor
Veterans Canteen Web		Vocational Rehabilitation & Employment (VR&E) CH 31
VETSNET Housekeeping	Web Electronic Lender Identification	Web Automated Folder Processing System (WAFPS)
		Web Automated Reference Material System (WARMS)
VR&E Training Website		Web Automated Verification of Enrollment
Web LGY		Web-Enabled Approval Management System (WEAMS)
		Web Service Medical Records (WebSMR)
		Work Study Management System (WSMS)
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		
Is PII collected by this min or application?		
Does this minor application store PII?		
If yes, where?		
Who has access to this data?		
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?		
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?		

(FY 2012) PIA: Minor Applications A-M

Which of these are sub-components of your system?			
1184 Web	Citrix	Electronic Signature	Imaging
A4P	Clinical Case Registries	Embedded Fragment Registry	Incentive Awards
ACCu Care	Clinical Data Repository/Health Data Repository	ENCORE 2	Incident Reporting
ACCU Check	Clinical Info Resource Network	ENDSOFT	Income Verification Match
ACCU Med	Clinical Monitoring System	Engineering	Incomplete Records Tracking
Adobe Acrobat	Clinical Notes Templates	Enrollment Application System	Inpatient Medications
ADP Planning (PlanMan)	Clinical Procedures	Enterprise Terminology Server & VHA Enterprise Terminology Services	Intake/ Output
ADT	Clinical Reminders	ePROMISE	Integrated Billing
Adverse Reaction Tracking	Clippership	Equipment/ Turn-in Request	Integrated Patient Funds
Agent Cashier	Combat Veteran Outreach	Event Capture	Interim Mangement Support
Air Fortress	Committee on Waiver and Compromises	Event Driven Reporting	Inventory Management System
ASISTS	Consult/ Request Tracking	Extensible Editor	Kernal
Authorization/ Subscription	Controlled Correspondence	External Peer Review	Kids
Auto Instrument	Controlled Substances	EYECAP	KOWA
Auto Replenishment/ Ward Stock	CP&E	Fee Based Claims System	Lab Service
AUTOCAD	CPRS	Fee Basis	Laboratory Electronic Data Interchange
Automated Access Request	CPT/ HCPCS Codes	Financial and Accounting System (FAS)	Letterman
Automated Info Collection Sys	Credentials Tracking	Financial Management System (FMS)	Lexicon Utility
Automated Lab Instruments	Credit Card Authentication	Functional Independence	Library
Automated Med Info Exchange	Data Innovations	Gen. Med. Rec. - I/O	List Manager
Automated Sales Reporting	DELIVEREX	Gen. Med. Rec. - Vitals	Lynx Duress Alarm
AutoMed	Dental	Gen. Med.Rec. - Generator	Mailman
Bad Code Med Admin	DICTATION-Power Scribe	GENDEX	MCCR National Database
Barcode Medication Administration Contingency Plan (BCU)	Dietetics	Generic Code Sheet	Meadows (MDWS)
BCMA Contingency Workstations	Discharge Summary	Genesys	Medicine
BDN 301	DRG Grouper	Get Well Networks	Mental Health
Beneficiary Travel	DRM Plus	GMED	MHPT
Big Fix	Drug Accountability	GRECC	MICOM
CA Vertified Components - DSSI	DSIT	Health Data and Informatics	Microsoft Exchange E-mail System
Capacity Management - RUM	DSS Extracts	Health Level Seven	Military/Vet Eye Injury Registry
Capacity Management Tools	DSS Quadramed	Health Summary	Minimal Patient Dataset
CAPRI	EDS Whiteboard (AVJED)	Health Summary Contingency	Missing Patient Reg (Original) A4EL
Cardiff Teleform	Education Tracking	HINQ	Mumps AudioFAX
Cardiology Systems (stand alone servers from the network)	EEO Complaint Tracking	Hospital Based Home Care	MyHealthEVet
Care Management	EKG System	ICB	
CareTracker	Electronic Card System (ECD)	ICR - Immunology Case Registry	
CHECKPOINT	Electronic Payroll Deduction (EPD)	IFCAP	
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			
Is PII collected by this minor application?			
Does this minor application store PII?			
If yes, where?			
Who has access to this data?			
Name			
Description			
Comments			
Is PII collected by this minor application?			
Does this minor application store PII?			
If yes, where?			
Who has access to this data?			
Name			
Description			
Comments			
Is PII collected by this minor application?			
Does this minor application store PII?			
If yes, where?			
Who has access to this data?			

(FY 2012) PIA: VISTA Minor Applications N-Z

Which of these are sub-components of your system?			
National Cemetery Association	Pharmacy Data Management	Scanning Exam and Evaluation System	VBECs
National Drug File	Pharmacy National Database	Scheduling	VDEF
National Laboratory Test	Pharmacy Prescription Practice	Security Suite Utility Pack	Vendor - Document Storage Sys
NDBI	PICIS OR	Sentillion	Veterans Canteen Web
Network Health Exchange	Police & Security	Shift Change Handoff Tool	Veterans Information Solution
NOAHLINK	Problem List	ShoreTel	VHAHUNAPP1
NOIS	Progress Notes	Social Work	VHAHUNFPC1
Nursing Service	Prosthetics	Stellant	VHS & RA Tracking System
Occurrence Screen	Purchase Order Management System	Stentor	Visit Tracking
Omnicell	Pyxis	Surgery	VISTA RAD
Oncology	Q-Matic	Survey Generator	VISTA RO
Onicord (VLOG)	QMSI Prescription Processing	Telecare Record Manager	VistALink
Optifill	Quality Assurance Integration	Temp Trak	VistALink Security
Order Entry/ Results Reporting	Quality Improvement Checklist	Text Integration Utilities	Visual Impairment Service Team ANRV
Outpatient Pharmacy	QUASER	Tickler Database	Vitria BusinessWare
P2000 ROBOT	Radiology/ Nuclear Medicine	Toolkit	VIXS
PACS database	RAFT	TopCon	Voluntary Timekeeping
Patch Module	RALS	TraceMaster	Voluntary Timekeeping National
Patient Data Exchange	Record Tracking	Tracking Continuing Education	WEB HINQ
Patient Feedback	Registration	Traumatic Brain Injury	Whiteboard
Patient Representative	Release of Information - DSSI	Unwinder	Women's Health
PCE Patient Care Encounter	Remote Order/ Entry System	Utility Management Rollup	Workload and Overtime
Personal Computer Generated Letters	RPC Broker	Utilization Review	
Pharmacy Benefits Mangement	Run Time Library	VA Conference Room Registration	
	SAGG	VA Fileman	
	SAN	VAMedSafe	

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	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	
Name	
Description	
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	
Name	
Description	
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

(FY 2012) PIA: Final Signatures		*Green Highlight = Must Answer Question	
Facility Name:	Terremark Worldwide Inc. Culpeper, VA		
Title:	Name:	Phone:	Email:
Privacy Officer:	Garnett Best	(202)-632-7378	Garnett.Best@va.gov
Digital Signature Block			
Information Security Officer:	Perry Ungson	Ext 6375, Cell #	Perry.Ungson@va.gov
Digital Signature Block			
System Owner/Delegate:	Lorraine Landfried	(202)-632-4347 (202)-461-9170	lorraine.landfried@va.gov
Digital Signature Block			
Chief Information Officer:	Dick Rickard	(352)-686-3227	Dick.Rickard@va.gov
Digital Signature Block			
Other Titles:	0	0	0
Digital Signature Block			
Date of Report:	3-Feb-12		
OMB Unique Project Identifier	029-888888105		
Project Name	Federal Case Management Tool (FCMT)		
<p>The Signature Process:</p> <ul style="list-style-type: none"> • Complete the PIA form. • Name the PIA Excel FORM ["FY12-Region # - Facility Name - Facility # -Date(mmddyyyy).xls"] <ul style="list-style-type: none"> • Example: "FY12-Region3-Lexington VAMC-596-10302008.xls" • Submit the completed PIA Excel form to SMART Database. • Fix errors the reviewers sent back, rename the file and submit to SMART Database <ul style="list-style-type: none"> • If no errors, convert form into PDF with Nuance PDF Professional. • Name the PIA PDF form ["FY12-Region #-Facility Name- Facility # -Date(mmddyyyy).xls"] <ul style="list-style-type: none"> • Obtain digital signatures on the "Final Signatures tab" • Submit signed PIA PDF form to the SMART Database. 			