

(FY 2012) PIA: System Information		*Green Highlight = Must Answer Question		*Yellow Highlight = Required to Sign PIA	
Program or System Name (as shown in SMART):		CDCO > AITC > VA > Identity Access Management - Enterprise (IAM-E)			
OMB Unique System / Application / Program Identifier (AKA: UPID #):		029-00-01-25-01-5103-00			
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)"		Identity and Access Management (IAM) is a set of processes and technologies to manage identities across multiple systems, encompassing identity (based on an identifier and a set of attributes) and access (interactions with information and other assets). These processes may be based on individual users, roles, or organizations.			
Facility or Program Office Name:					
Title:		Name:	Phone:	Email:	
Privacy Officer:		Amy Howe	512-326-6217	amy.howe1@va.gov	
Information Security Officer:		Casey Longacre	206-341-8551	casey.longacre@va.gov	
System Owner/Delegate:		David Kubacki	512-326-6408	david.kubacki@va.gov	
Chief Information Officer:		David Kubacki	512-326-6408	david.kubacki@va.gov	
Information Owner:					
Other Titles:					
Person Completing Document:		Oswaldo Melendez	512-326-6248	oswald.melendez@va.gov	
Other Titles:					
Date of Last Full Approved PIA by VACO Privacy Services:		N/A			
What specific legal authorities authorize this program or system:		Title 38, United States Code, 7332			
What is the expected number of individuals that will have their PII stored in this system:		over 1,000,000			
Identify what stage the System / Application / Program is at:		Implementation			
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.		01/2012			
Is there an authorized change control process which documents any changes to existing applications or systems?		<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> N/A : First PIA			
If No, (Explain on Tab 8)					
Is there a contingency plan in place to process information when the system is down?		<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> N/A : First PIA			
Has a PIA been completed within the last three years?		<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> N/A : First PIA			
FISMA QUESTIONS					
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 type="radio"/> Yes <input checked="" type="radio"/> No			
4. Is there a Privacy Impact Assessment (PIA) that covers this system?		<input type="radio"/> Yes <input checked="" 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 identifier?		<input checked="" type="radio"/> Yes <input type="radio"/> No			
6. What is the System of Records Notice (SORN) for this system?		150VA19			
7. Has this SORN been reviewed or updated within the last three years?		Yes last year			
Date of Report (MM/YYYY):		11/4/2011			
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 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?					

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) :

150VA19

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

- 4. Based on Question 3, is a SORN required?
***If Yes, has the process begun to obtain/acquire a SORN

Yes No
 Yes No

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)	Paper & Electronic	Benefits	All	All
Family Relation (spouse, children, parents, grandparents, etc)	N/A	N/A	N/A	N/A
Service Information	Paper & Electronic	Eligibility	All	All
Medical Information	Paper & Electronic	Benefits	All	All
Criminal Record Information	N/A	N/A	N/A	N/A
Guardian Information	N/A	N/A	N/A	N/A
Education Information	Paper & Electronic	Eligibility	All	All
Benefit Information	Paper & Electronic	Benefits	All	All
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	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Family Relation (spouse, children, parents, grandparents, etc)	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Service Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Medical Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Criminal Record Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Guardian Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Education Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Benefit Information	<input type="radio"/> Yes <input checked="" type="radio"/> No	Veteran	<input type="radio"/> Mandatory <input checked="" type="radio"/> Voluntary
Other (Explain on Tab 8)	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Mandatory <input checked="" 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	Veterans Administration	<input checked="" type="radio"/> Yes <input type="radio"/> No	Healthcare	<input type="radio"/> Yes <input checked="" type="radio"/> No	VA Release of Information Form
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 B)					
(FY 2012) PIA: Access to Records					
Does the system gather information from another system?	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Please enter the name of the system:					
(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 B)	<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 B) <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 B)			
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: Per the National Archives and Records Administration General Records Schedule 14, item 6, and published in the Veterans Health Administration Records Control Schedule 10-1, Item XLV.		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: Department of Veterans Affairs Record Control Schedule 10-1, Revised June 28, 2006, specifies how long patient data will be maintained.			
What are the procedures for eliminating data at the end of the retention period?			
Answer: Department of Veterans Affairs Record Control Schedule 10-1, Revised June 28, 2006, specifies how long patient data will be maintained.			
Where are these procedures documented?			
Answer: National Archives and Records Administration General Records Schedule 14, item 6, and published in the Veterans Health Administration Records Control Schedule 10-1, Item XLV.			
How are data retention procedures enforced?			
<p>Answer: The VA Handbook 6300.1 contains mandatory Department of Veterans Affairs (VA) procedures for managing records effectively and efficiently throughout their life cycle. These procedures will facilitate accomplishment of VA's programmatic and administrative missions, preserve official records in accordance with applicable statutory and regulatory requirements, and promote access to information by VA staff and the public as appropriate. In addition specific procedures concerning records disposition, use, maintenance and filing standards for VA Central Office records are contained within this handbook.</p> <p>Under Secretaries, Administration Heads, Assistant Secretaries, Other Key Officials, and Deputy Assistant Secretaries will designate one or more Records Officers (ROs) to serve as staff office Record Officers (ROs). They will manage and coordinate the records management program for their organizations. The ROs will systematically review records, control schedules, file plans and procedures to ensure that they are current and update them as necessary. The ROs will develop and disseminate procedures as needed, to supplement VA-wide procedures to meet the records management needs of their program offices and to support a records management program within their respective organizations.</p> <p>All VA records and information must be identified by records series and be listed in a records control schedule. Proper and timely records disposition is the key to management of records and other documentary materials.</p> <p>A. All records maintained by VA will be reviewed annually by the office holding them, and action will be taken to:</p> <ol style="list-style-type: none"> (1) Remove less-active records to local storage; (2) Transfer inactive records to an approved records offsite storage facility; (3) Transfer permanent records to the National Archives; and; (4) Destroy and document the destruction of records which have reached the term of their authorized retention period. <p>B. Administrations and staff office Records Officers will review their records control schedules annually to ensure that they are kept current, accurately reflect program office needs, and meet all statutory requirements. As a result of each review, administration and staff office Records Officers will submit changes through the records appraisal process procedures contained in Chapter 8, or new records.</p>			
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 B)			
(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 B) <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.	<input checked="" type="radio"/> Yes	<input type="radio"/> 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..	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is security monitoring conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is security assessment conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is adequate physical security in place to protect against unauthorized access?	<input checked="" type="radio"/> Yes	<input type="radio"/> 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 type="checkbox"/> Lightning Strike	<input type="checkbox"/> Terrorism
<input type="checkbox"/> Blizzard	<input checked="" type="checkbox"/> Flood	<input checked="" type="checkbox"/> Malicious Code	<input checked="" type="checkbox"/> Thunderstorm
<input type="checkbox"/> Burglary/Break In	<input checked="" type="checkbox"/> Hacker, Cracker	<input checked="" type="checkbox"/> Password Privacy Negligence	<input checked="" type="checkbox"/> Tornado
<input type="checkbox"/> Civil Unrest	<input checked="" type="checkbox"/> Hail	<input checked="" type="checkbox"/> Personnel Unavailable	<input 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 type="checkbox"/> Sabotage	<input checked="" type="checkbox"/> User Sabotage
<input type="checkbox"/> Dust/Debris	<input type="checkbox"/> Hurricane	<input checked="" type="checkbox"/> System Intrusion, Break-Ins	<input type="checkbox"/> Vibration
<input type="checkbox"/> Earthquake	<input checked="" type="checkbox"/> HVAC Failure	<input checked="" type="checkbox"/> System Misconfiguration	<input type="checkbox"/> Volcano
<input type="checkbox"/> Extreme Cold	<input type="checkbox"/> Indoor Humidity	<input checked="" type="checkbox"/> System Penetration	<input 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: **C.2.8.9 Personal Identity and Authentication Information Information Type**

<p>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)</p>	<input checked="" 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 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>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)</p>	<input checked="" 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 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>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)</p>	<input checked="" 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 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 minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

(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.

The following applications compromise a part of the IAM-E environment:

Credentialing Service Provider CSP is an integral component of the IAM solution construct and provides external end user credentials for a VA Person of Interest (POI) that is not eligible and/or does not have another VA approved credential. CSP enhances external user experience via the integrated self-service functions providing user the ability to request VA credentials, manage password changes and resets, administer security questions, and revise user profile information. For Release 3, the VA CSP service is designed to provide the following:

A comprehensive, in-house, VA CSP Service that provides the ability to issue VA Directive 6500 and NIST SP 800-63 compliant authentication assurance level credentials at Level 1 and Level 2. The production implementation will support issuance of Level 1 and Level 2 credentials requested via the CSP registration interface. Level 1 credential will be a self-asserted credential and Level 2 will require in person proofing before the credential is enabled for usage. The credentials issued by the CSP will be in the form of User ID and password. The full production release will include pilot functionality to provide Level 1 credential as well as support for Level 2 credential issuance via the CSP interface and proofed via Identity Proofing (IP) Service. A migration path to allow the upgrade of a Level 1 to Level 2 credential so that once a user's identity has been validated, the same credential (User ID and password) may be elevated to Level 2. Secure self-service capabilities to accomplish registration, retrieve lost or forgotten User IDs and/or passwords, password changes, administration of security questions, and user profile information. Integration with IP Service to proof an applicant requesting a level 2 credential directly or upgrading to level 2 via CSP. The IP Service will provide the necessary proofing data/results to the CSP to enable the credential request. Integration with VAAFI Solution to provide federated authentication of both Level 1 and Level 2 credentials to VA application using Security Assertion Markup Language (SAML) mechanisms. VAAFI Solution is responsible for integrating VA applications to utilize the CSP credential. Application integration is out of scope for CSP Service. This design will leverage the CA Report Manager, as detailed in the VA IAM System Design, to provide a capability for privileged users to schedule and run standard management reports supporting the storage and output of reports in portable document format (PDF). In the production release of the CSP Service "Standard Management Reports" will be limited to the "basic" reporting functionality readily available and inherent to the CSP Service toolset. Enhanced, robust report and audit capabilities will be realized through the future iteration's integration with the Compliance and Audit Reporting (CAR) Service.

Identity Proofing (IP) Service

IP is one of the key processes associated with a user providing a level of assurance to VA applications that the person authenticating is in fact who they claim to be. By integrating IP into the IAM CSP Solution, VA users will undergo a single instance of in-person identity proofing from which an accepted assurance level 2 will be recorded and subsequently a Level 2 credential issued by the CSP.

IP will enable the Registrar to verify and validate a user's identity either electronically or in person. For Release 3, the VA IP service has been designed to provide:

Integration with Credential Service Provider (CSP) a capability to proof a pre-registered applicants requesting a level 2 credential directly or upgrading to level 2 via CSP. The interface provides the proofing authority the ability to record the data points of interest from approved identification (ID) artifacts per the VA Directive 6500. The IP interface requires the proofing authority to record the ID type, ID number and expiration dates and verifies address and date of birth from the identification presented by the applicant. The Identity Proofer will be responsible for determining that the ID appears valid and that the photo identification reasonably matches the in-person proofing applicant. (Note that the IP Service is not responsible for providing any level of assurance of the validity (non-fraudulent) of the presented identification nor the assertion of a reasonable match between the photo identification and the applicant). The service will store the data points entered by the proof as well as the proofing authority's ID and date/time stamp of the proofing event as result of in person proofing transaction. The IP Service provides the necessary proofing data/results to the CSP to enable the credential request.

Integration with business applications requiring capability to proof new applicants and create an applicant record in the user directory when the applicant is not pre-registered via the CSP and a current proofing record does not exist. For limited production pilot, IP GUI interfaces will be utilized to enter proofing information for an applicant. The IP Service will store the proofing record for an applicant based on data points entered by the proofing authority. The IP Service will also provide VA ID proofing authorities an interface to search for an applicant and retrieve proofing status of the applicant via the IP interface.

Capability for privileged users to schedule and run standard management reports supporting the storage and output of reports in portable document format (PDF). In the limited production pilot release of the IP Service "Standard Management Reports" will be limited to the "basic" reporting functionality readily available and inherent to the IP Service toolset. Additional reporting and auditing capabilities will be realized through future iterations integration with the Compliance and Audit Reporting (CAR) Service.



(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	BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Agent Orange		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)
Bbraun (CP Hemo)	Courseware Delivery System (CDS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
	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
CONDO PUD Builder	Electronic Payroll Deduction (EPD)	Electronic Performance Support System (EPSS)
	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	Modern Awards Process Development (MAP-D)
INS - BIRLS	Inventory Management System (IMS)	
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	Loan Guaranty Training Website	Purchase Order Management System (POMS)
MES		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 Trancking and Response System (VICTARS)
		Veterans Service Representative (VSR) Advisor
VBA Training Academy	VBA Enterprise Messaging System	Vocational Rehabilitation & Employment (VR&E) CH 31
Veterans Canteen Web		
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 Verified 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?			

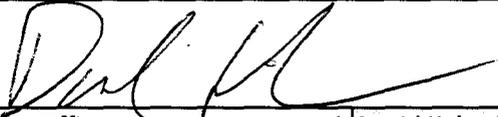
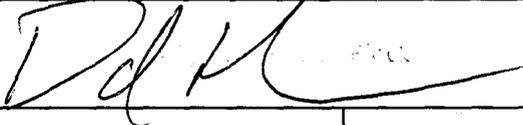
(FY 2012) PIA: VISTA Minor Applications N-Z

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:	0		
Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov
Digital Signature Block			
Information Security Officer:	Casey Longacre	206-341-8551	casey.longacre@va.gov
Digital Signature Block			
System Owner/Delegate:	David Kubacki	512-326-6408	david.kubacki@va.gov
Digital Signature Block			
Chief Information Officer:	David Kubacki	512-326-6408	david.kubacki@va.gov
Digital Signature Block			
Other Titles:	0	0	0
Digital Signature Block			
Date of Report:	11/4/2011		
OMB Unique Project Identifier	029-00-01-25-01-5103-00		
Project Name	CDCO > AITC > VA > Identity Access Management - Enterprise (IAM-E)		

(FY 2012) PIA: Final Signatures

*Green Highlight = Must Answer Question

Facility Name:	0		
Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	Amy.Howe1@va.gov
Digital Signature Block			
Information Security Officer:	0	0	0
Digital Signature Block			
System Owner/Delegate:	David Kubacki	512-326-6408	David.Kubacki@va.gov
			
Chief Information Officer:	David Kubacki	512-326-6408	David.Kubacki@va.gov
			
Other Titles:	0	0	0
Digital Signature Block			
Date of Report:	0-Jan-00		
OMB Unique Project Identifier	0		
Project Name	00000		