Department of Veterans Affairs

Health Eligibility Case Management System (HECMS)

Security Guide

Version 3.12

June 2013
Document Revision Date

August 2013
Software Release Date

Office of Information and Technology (OIT)

Product Development

Revision History

Date	Version	Description	Project Manager	Author
6/10/2013	8.3	Changed cover and footer dates to reflect August release date.	Dan Soraoka	Tom Hamilton
05/10/2013	8.2	Updated Glossary to include VBR and VOA Updated the authentication & identification section to include the authentication details for VBR and VOA Updated VistA patches for 3.12	Dan Soraoka	Sudha Ramani
4/23/2013	8.1	Added VOA & VBR web service	Dan Soraoka	Shaopeng Sun
4/23/2013	8.0	Updated document version and date to correspond with change from 3.11 to 3.12 on cover and footers. Updated any ESR 3.11 references to ESR 3.12.	Dan Soraoka	Tom Hamilton
2/27/2013	7.3	Updated cover/footer dates to revised scheduled release date to June 2013.	Glenda Miller	Tom Hamilton
1/15/2013	7.2	Updated associated patches in *Exported Groups and/or Options and Menus* section.	Glenda Miller	Tom Hamilton
1/10/2013	7.1	Updated document for ESR 3.11.	Glenda Miller	Shaopeng Sun Sudha Ramani
11/26/2012	7.0	Updated document version and date to correspond with change from 3.10 to 3.11 on cover and footers. Updated any ESR 3.10 references to ESR 3.11.	Glenda Miller	Tom Hamilton
10/14/2012	6.0	Reviewed and no updates are needed for 3.10	Glenda Miller	Sudha Ramani
10/1/2012	6.0	Updated document version and cover/footer dates to correspond with change from 3.9 to 3.10 and scheduled release. Also added associated ESR 3.10 VistA patches.	Glenda Miller	Tom Hamilton
8/28/2012	5.0	Updated cover date to revised scheduled release of ESR 3.9 to November 2012.	Glenda Miller	Tom Hamilton
7/30/2012	5.0	Reviewed the document and no updates are needed for ESR 3.9.	Glenda Miller	Sudha Ramani
7/27/2012	5.0	Updated document version to correspond with change from 3.8 to 3.9 on cover. Updated Release dates to January 2013 on cover and footers. Updated ESR 3.8 references to ESR 3.9.	Glenda Miller	Tom Hamilton

Date	Version	Description	Project Manager	Author
4/18/2012	4.0	Updated document version to correspond with change from 3.7 to 3.8 on cover. Updated Release dates to September 2012 on cover and footers. Updated ESR 3.7 references to ESR 3.8.	Glenda Miller	Tom Hamilton
3/14/2012	3.2	Updated Bulletins list, Exported Options, Interfacing tools, and Base System Hardware for ESR 3.7.	Glenda Miller	Laurie Sheppard
3/13/2012	3.1	Updated cover and footer dates to reflect new June 2012 release date.	Glenda Miller	Tom Hamilton
2/23/2012	3.0	Updated document version to correspond with change from 3.6 to 3.7 on cover. Updated Release dates to April 2012 on cover and footers. Updated ESR 3.6 references to ESR 3.7.	Glenda Miller	Tom Hamilton
11/23/2011	2.1	Changed cover and footer dates for scheduled release date of January 2012.	Glenda Miller	Tom Hamilton
10/26/2011	2.0	Updated document version to correspond with change from 3.5 to 3.6 on cover. Updated Release Dates to December 2011 on cover and footers. Updated ESR 3.5 references to ESR 3.6.	Glenda Miller	Tom Hamilton
9/13/2011	1.1	Updated cover and footer dates to correspond with new National Release date for 3.5 to September 2011.	Jennifer Freese	Tom Hamilton
7/18/2011	1.0	Initiated document version to replace application version on cover. Updated dates.	Jennifer Freese	Tom Hamilton
7/7/2011		Basedlined ESR 3.4 by accepting Tracked Changes for 3.5 version. Updated references from 3.4 to 3.5 and changed dates. No other significant changes required for ESR 3.5.	Jennifer Freese	Tom Hamilton
5/17/2011		Updated document in prep. for VDL. Remove *Draft* indicators.	Jennifer Freese	Tom Hamilton
2/15/2011		Reviewed/Edited/Formatted	Jennifer Freese	Tom Hamilton
2/14/2011		Updated for ESR 3.4 release	Jennifer Freese	Sudha Ramani
9/29/2010		Updated for ESR 3.3 release	Jennifer Freese	Sudha Ramani
4/21/2010		Updated 3.0 document with the most current 3.0 information in preparation for uploading to VDL. Changed red fonts to black.	Brian Morgan	Tom Hamilton
03/11/09		Provided link to Trouble Shooting Section	Gerry Lowe	Tavia Leonard

Date	Version	Description	Project Manager	Author
03/10/09		Provided additional toolsets to Interface Section	Gerry Lowe	Tavia Leonard
03/10/09		Provided additional information to Audit Section	Gerry Lowe	Tavia Leonard
03/09/09		Provided Enrollment VistA Changes Patch Information for Release 2 to Export Group Section	Gerry Lowe	Tavia Leonard
03/04/09		Updated Application Dependency Section	Gerry Lowe	Tavia Leonard
02/25/09		Updated hyperlink for Electronic Signature	Gerry Lowe	Tavia Leonard
10/02/08		Initial draft Security document	Gerry Lowe	Tavia Leonard

Table of Contents

Legal Requirements

Applicable Laws or Regulations Affecting the System

This section lists the laws and/or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information within the Health Eligibility Case Management System, a.k.a. (HECMS or HECMS V3.12) application.

Applicable Laws or Regulations

The following are laws and regulations that establish specific operational or protective requirements for confidentiality, integrity, or availability of information that have been tentatively identified and applied to the HECMS application.

- Computer Security Act of 1987, Public Law 100-235
- OMB Circular A-123 - "Internal Control Systems"
- OMB Circular A-130 - "Management of Federal Information Resources, "Appendix III, "Security of Federal Automated Information Resources"
- 5 U.S.C. 552a, Privacy Act of 1974, 5 United States Code 552a, Public Law 99- 08.
- 5 U.S.C. 552, Freedom of Information Act, 5 United States Code 552, Public Law
- 18 U.S.C. 1030 (a) (3), Fraud and related activity in connection with computers.
- 18 U.S.C. 1001, Computer Fraud, and Abuse Act of 1986.
- Electronic Communications Privacy Act of 1986, Public Law 99-08, 100 Stat. 1848.
- Federal Information Processing Standards (FIPS)
- Publication 31 - "Guidelines for Automatic Data Processing Physical Security and Risk Management"
- Publication 39 - "Glossary for Computer Systems Security"
- Publication 41 - "Computer Security Guidelines for Implementing the Privacy Act of 1974"
- Publication 46 - "Data Encryption Standards"
- Publication 73 - "Guideline for Security of Computer Applications"
- Publication 83 - "Guideline on User Authentication Techniques for Computer Network Access Control"
- Publication 87 - "Guidelines for AIS Contingency Planning"

Supporting Policy and Agency Documents

Listed below are specific policies and agencies that support the HECMS:

VA Directives:
- VA Directive 6210, "Automated Information Systems (AIS) Security Procedures"
- VA Directive 6214, "Information Technology Security Certification and Accreditation

Programs:
- IRS Publication 1075
- Title 26, Subtitle F, Subchapter B, Section 6103
- Title 26, Chapter 75, Subchapter A, Part 1, Section 7213
- Title 26, Chapter 75, Subchapter A, Part 1, Section 7213A
- Title 26, Chapter 76, Subchapter B, Section 7431

Auditing

The database team Administrative Database Repository (ADR) is responsible for maintaining an audit trail. The team maintains an audit log at the application level. Changes to user information are tracked through the HECMS, which automatically records additions and deletions. Currently, the HECMS administrators generate and review the audit log for security purposes on a daily basis, and the ISSO generates and reviews the audit log on a weekly basis. HECMS maintains audit trails that are sufficient in assisting in reconstruction of events due to a security compromise or malfunction.

The audit trail of HECMS contains the following requirements:
- Identity of each person and device having access or attempting access the system
- Date and time of the access and logoff
- Activities that modify, bypass, or negate IT security safeguards controlled by the computer system
- Security-relevant actions associated with processing
- User ID and password for unsuccessful logon attempts

Note:
Access to online security audit logs is strictly enforced. Only the DBA and ISSO are authorized to access the security audit logs. In addition, audit trails are reviewed following a known system violation or application software problem that has occurred. If discrepancies are identified, the information in the audit trail provides the means for a thorough investigation.

Authentication Identification and Authorization

HECMS Authentication

HECMS ensures that each user is authenticated before access is permitted. HEC users must request for an HECMS role in order to gain access to the system. All users receive a user ID,

password, and access rights because of their roles and responsibility to the system. A user has up to three attempts to log in to the system. After the third unsuccessful attempt, the application automatically locks out that user ID until the system administrator resets it.

HECMS ensures that any external system consuming the Enrollment & Eligibility Web service is authenticated. External systems must request for a service account in order to gain access to the web services. External systems will receive a user id and password and service requests they can consume based on their business roles.

HECMS provides web services to access and store handbook artifacts in the Veteran Benefits Repository (VBR) and submit health benefits application from Veteran Online Application (VOA). These web services use the mutual TLS authentication with VA-issued certificates to identify and authorize server-to-server communications. HECMS uses the Military Service Data Sharing Web Service provided by VA/DoD Information Repository (VADIR). This interface uses Mutual TLS Authentication with VA-issued certificates to identify and authorize server-to-server communications. TLS also provides the message's confidentiality and integrity between the endpoints.

ⓘ To obtain more information on <u>user privileges and auditing</u> review the <u>system security plan</u> outlined in TSPR website.

Identification and Authorization

HECMS uses the following password control requirements to identify and authorize:

- Passwords consist of a minimum of eight characters in length, and contain three of the following four items: letters (upper case and lower), numbers, and/or   symbols ("#""," @" or "$").
- Passwords must be changed every 90 days and reminders are sent 15 days in advance prior to expiration date
- Procedures for verifying that all system-provided administrative default passwords have been changed
- Procedures for limiting access scripts with embedded passwords (for example, scripts with embedded passwords are prohibited)
- System shall be configured to force the user to select a new password immediately after signing on with an initial password
- Null passwords are not permitted
- Controls are implemented to require strong passwords.
- Accounts that have been inactive for 90 days are disabled.
- To preclude password guessing, an intruder lock out feature shall suspend accounts after five invalid attempts to log on. When "Round-the-Clock", System Administration (SA) service is available; the SA intervention is required to clear a locked account. If the "Round-the-Clock" system administration service is not available, accounts shall remain locked out for at least ten minutes.

• All VA information systems have the ability to audit password activity, specifically when and who last changed a password, and when and who last changed account privileges.

Logical Access Controls

The controls to access the HECMS for the user and user classes are controlled through the ISO located at the HEC. In addition the access of business roles are controlled and monitored through the HEC ISO, however specific roles are defined within the HECMS application. The HEC ISO controls the population of the user groups across the domain but the AITC (Austin Information Technology Center) controls the access groups.

Note:
Details are describe in the AITC Directive 0712 (Parts: 16 General User Security Procedures and 20 System Administrator Security Procedures) and HEC-18.

Application users are restricted from accessing the operating system, applications, or other system resources not required in the performance of their duties. Authorized Web services staff monitors the security log regularly to detect any instances of unauthorized transaction attempts. The system will automatically end the user's session after 20 minutes of inactivity.

Logical Access Security Warning Banner

The National Institute of Standards and Technology (NIST) Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems", recommends that a standardized log-on banner be placed on Government systems. Public Law 99-474 requires that a warning message be displayed notifying unauthorized users that they have accessed a U.S. Government computer system. All unauthorized use is punishable by fines or imprisonment.

Note:
An illustration of the "Sign-on Warning Banner", for HECMS listed below:

WARNING
This system may contain Government information which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject the individual to Criminal and Civil penalties pursuant to Title 26, United States Code, Sections 7213(a), 7213A (the Taxpayer Browsing Protection Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel. **ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.**

Security Controls

Listed below are the minimum-security controls that were put in place prior to authorizing HECMS for processing:

- Technical and/or Security evaluation completed
- RA was conducted
- Rules of behavior established and signed by users
- Contingency plan was developed and tested
- Security plan was developed, updated, and reviewed
- Assurance that the system meets all applicable federal laws, regulations, policies, guidelines, and standards
- In-place adequate and appropriate planned security safeguards

Technical Controls

Technical Controls primary function focuses on security controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Application Dependencies

ℹ️ To learn what all the HECMS Application Dependencies are you can start by reviewing the Supplementary Specification manual.

Mail Groups, Alerts, and Bulletins

HECMS utilizes the following Message, Bulletins, and Mail Groups.

1	**Message= HL7 - Z07 from site** **Bulletin=HEC Notification of POW Discrepancy** **Mail Group= G.DGEN Eligibility Alert @(site).med.va.gov**
2	**Message= HL7 - Z07 from site** **Bulletin=HEC Notification of Need for Site to Verify Veteran** **Mail Group=G.DGEN Eligibility Alert @(site).med.va.gov**
3	**Message= ORU/ORF Z07** **Bulletin=Inconsistent Conflict Data from Site.** **Mail Group=Send to site that sent the inconsistent data.** **The mail-group is- g.DGEN ELIGIBILITY ALERT (SITE).MED.VA.GOV**
4	**Message= ORU/ORF Z07** **Bulletin=Inconsistent Conflict Data from Site** **Mail Group=Send to site that sent the inconsistent data.**

	The mail group is - g.DGEN ELIGIBILITY ALERT (SITE).MED.VA.GOV
5	**Message= ORU/ORF Z07** **Bulletin=HEC Notification of Need for Site to Send Ineligible Information** **Mail Group=G.DGEN Eligibility Alert @(site).med.va.gov**
6	**Message= ORU/ORF Z07 (TBL 235.2)** **Bulletin=HEC Notification of Need for Site to Verify Veteran** **Mail Group=G.DGEN Eligibility Alert @(site).med.va.gov**
7	**Message= ORU Z07** **Bulletin=HEC Notification of Need for Site to Verify DOD Deletion.** **Mail Group=G.DGEN Eligibility Alert @(site).med.va.gov**
8	**Message= ORF~Z11 from VBA** **Bulletin=Solicited Z11 did not match on a Person** **Mail Group=VHA CIO HECAlert Mailgroup - HECAlert@med.va.gov**
9	**Message= Receive Query Z11** **Bulletin=Eligibility Not Verified, Call HEC** **Mail Group=Send to the site that sent the query - G.DGEN Eligibility Alert (site).med.va.gov**
10	**Message= ORF~Z11 from VBA** **Bulletin= HEC Notification of NSC, VA Pension and HB** **Mail Group= G.DGEN Eligibility Alert @(site).med.va.gov**
11	**Message= ORF~Z11 from VBA** **Bulletin= HEC Notification of NSC to NSC, VA Pension** **Mail Group= G.DGEN Eligibility Alert @(site).med.va.gov**
12	**Message= ORF~Z11 from VBA** **Bulletin= HEC Notification of Terminated VA Pension NSC** **Mail Group= G.DGEN Eligibility Alert @(site).med.va.gov**
13	**Message= ORF~Z11 from VBA** **Bulletin= HEC Notification of Terminated VA Pension SC** **Mail Group= G.DGEN Eligibility Alert @(site).med.va.gov**
14	**Message= ORF~Z11 from VBA** **Bulletin= HEC Notification of NSC, VA Pension and A&A** **Mail Group= G.DGEN Eligibility Alert @(site).med.va.gov**
15	**Message= ORF~Z11 from VBA** **Bulletin= HEC Notification of SC and NSC, VA Pension** **Mail Group= G.DGEN Eligibility Alert @(site).med.va.gov**
16	**Message= Bulletin is not triggered by a message; triggered by completion of Add a Person** **Bulletin= HEC Notification of Person Added Preferred Site** **Mail Group= G.DGEN Eligibility Alert @(site).med.va.gov** **Sent only to the Preferred Facility**

ⓘ To learn more about HECMS Messaging Process HL7 transmissions review the Interface Control Document (ICD).

Remote Access/Transmission

HECMS utilizes and protects messages sent remotely through using an encryption service based on Sun JCA (Java Cryptography Architecture) and JCE 2.0 (Java Cryptographic Extension). The ESR system uses minimum-strength 128-bit Triple-DES encryption algorithm to convert data and process encoding and decoding messages.

NOTE: *Note:*

NOTE: (PL 104- HIPAA 191) (http://vista.med.va.gov/hipaa/) and FISMA (http://csrc.nist.gov/policies/FISMA-final.pdf) Web sites address encryption of data exchanged over any facility connection.

Archiving

There are currently no plans for archiving ADR data. ADR production database backup will be conducted using Oracle's Recovery Manager (RMAN). The backup schedule will be determined by the SLA. In conjunction with the archive logging configured on the database server, the backups will allow ADR production to be recovered to any point in time.

Contingency Planning

In the event of physical or man-made disaster that would affect the Austin Information Technology Center (AITC) and deem it non-operational, business processing will be moved to a hot site for temporary processing until AITC re-opens or a long term facility is established. Under the Disaster Recovery Plan (DRP), services will be restored within 72 hours. AITC has hot sites available for instant switchover to alternate from based upon the Continuation of Operations Plan (COOP) and the Consolidated Data Center Integration Plan (CDCI).

To learn more about DRP and COOP services, some information can be found in the ADR Security Guide.

Daily backups

Daily backups are maintained from both the UNIX based database servers and the Windows 2000 based application and web servers. There are incremental backups Monday through Friday and full backup processing on Saturday. Clones or copies of the backups are made and sent offsite on Saturday.

Exported Groups and/or Options and Menus

ESR 3.12 includes a VistA release
Includes installing the following patch(es).

Enrollment Hostfile	Scheduling Hostfile	Radiology Patch	Laboratory Patch
EAS*1.0*111 host file- includes patches EAS*1.0*111, DG*5.3*871 and IVM*2.0*155.	N/A	N/A	N/A

Security Keys and/or Roles

Listed below are the following recommended users:

Roles		
Local Administrator	ISO	**Report Viewer - DQM**
System Administrator	IRM	**Report Viewer - LAS**
EE LAS	Report Manager- Everything	**Report Viewer - PSC**
EE Supervisor	**Report Manager - DQM**	**Report Viewer - SSN**
DQ Supervisor	**Report Manager - LAS**	**Report Viewer - NON-HEC Limited**
Director	**Report Manager - PSC**	**Undeliverable Mail Manager**
EE Program Clerk	**Report Viewer - Everything**	**EGT Manager**
VistA Clerk	**Report Viewer - Non-HEC**	**IV LAS**
Call Center Clerk	**Report Viewer - HEC**	

Note:

Federal policies require that all IT positions are evaluated and that a sensitivity level is assigned to the position description. A background investigation is required for all VHA employees filling sensitive positions. VHA personnel and non-VHA personnel, including contractors, shall have personnel security clearances commensurate with the highest level of information processed by the system.

User access is restricted to the minimum necessary to perform the job. Each HECMS user is assigned privileges that allows or restricts updating, deleting, and/or inserting records in the database. In addition, HECMS uses application-level security controls to limit access to various system functions to only authorized users.

Interfacing

The HECMS architecture complies with all of the recommendations made by Health*e*Vet standards and guidelines. This also includes the use of third party software.

The following table outlines the different set of tools integrated as part of ESR architecture. Essentially as part of the selection process, the technical stakeholders ensured that the tools are not part of the prohibited VHA software list. In addition, a detailed analysis was performed comparing each product with its competitor to ensure that only the best viable solutions were included as part of the architecture.

Product Name	Description	Reason
Toad	A database administration and SQL development software application from Quest Software. It is widely used by Oracle developers and DBAs	Toad can view the Oracle Dictionary, tables, indexes, stored procedures, and more-- all through a multi-tabbed browser.
BMC/Patrol	Software application that concentrates on the IT structure. Ensures that appropriate levels of service, responsiveness, and throughput are delivered across changes to both the business and the IT environment.	Improves the ability of IT structure's mainframe. Solves problems and prioritize them within the context of the business functionality.
Introscope	Provides the capability to monitor as many servers and applications as a given enterprise needs.	Performs automatic baselining of applications, so that boundary conditions can be detected and alerts issued without interference from a production support staff.
Apache Ant	A pure Java based Application tool used for software build process.	• To support the following: • Platform Independent • Syntax

Product Name	Description	Reason
		• Functionality and flexibility • Development team awareness
Spring Framework	Spring framework is a light container with AOP based module support.	• Well integration with other selected products such as Struts, Hibernate, and Quartz • Removal of Dependency from the application container • Ease of Testing
Hibernate	An Object Relational Mapping tool that removes the low-level system maintenance away from the application components.	• Ease of Testability • Better Integration with the business Tier and Data object transfer • Remove complexity
ILOG JRule	A business management execution engine responsible for application logic management.	ILOG encapsulates the business logic into one central repository. The solution creates a more flexible solution to ESR architecture.
Apache Struts	A MVC framework used for the development of web based applications.	Struts offered the following set of advantages: • Stable Solution • Seamless integration with other selected tools • Industry standard • Validation Framework (allows constraints on data entry to prevent suspicious characters)
CruiseControl	An automated build tool used for scheduled build processes.	CruiseControl is build on top ANT architecture and it offers the following set of features: • Automation of the build process • Reporting • Promotion of continuous Integration
JUnit	Unit testing framework used for testing the different components of an application.	A proven testing framework in the software industry. There is a tremendous amount of support in the industry.

Product Name	Description	Reason
Log4j	A lightweight logging utility framework used for tracing and monitoring an application.	Log4J integrates extremely well with Spring, and Hibernate. In addition, compared to other logging utilities it has a much smaller footprint.
Apache ValueList	A pagination web framework, allows for a list of data to be presented in page mode format.	Offers the following flexibility: • Load all data at once • Allows for pagination • Retrieves objects from the database during each page load up
Quartz	Schedule component that allows batch jobs to trigger on a "temporal" or "on demand" basis.	The capabilities required by the users for schedule batch jobs go beyond what currently J2EE timer component currently supports. Quartz supports both the on demand and schedule jobs.
JasperReports	An open source component for J2EE based application. The solution provides out of the box capabilities for pdf and other template type reports.	Was selected based on its functional capabilities and seamless integration with Spring framework.
JAX-WS	A Java programming language API for creating web services. It is part of the Java EE platform from Oracle (Sun Microsystems)	Selected for the development and deployment of web service clients and endpoints. It can be used in Java SE starting with version 6.

Electronic Signatures

The Electronic Signature is in accordance with the Health_e_Vet rules and guidelines. To learn about the Electronic Signatures standards you can view the Health Information Management and Health Records that applies to all Health_e_Vet standards, VHA Handbook 1907.1 April 15, 2004.

 http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1469

File Security

VA FileMan is not applicable to this Health_e_Vet system but only to the VistA side.

Troubleshooting

Base System Hardware

⚠ All hardware is located at the Austin Information Technology Center (AITC) Austin, Texas.

ℹ To learn more on troubleshooting information, click here. This is a living document and will be updated periodically.

Listed below is the following minimum standard equipment required before troubleshooting the system.   For a more current specific equipment listing, contact the AITC.

System Resources		
Resource	**Quantity (Minimum)**	**Name and Type**
Application Server with Weblogic 10.3	1	Dell Power Edge 2850 Base Unit: PowerEdge 2850, 3.6 GHZ/2M Cache Xeon, 800MKz Front side Bus Processor: Dual Processor for 800FSB, PowerEdge 2850 Memory: 8GB DDR2, 400MHz Operating System: Windows 2003 Enterprise Edition, 25 Client Access Licenses English (420-3895); Linux RedHat Advanced Server 5.0 Update 2
Web Server	1 (clustered)	Dell Power Edge 2850 Base Unit: PowerEdge 2850, 3.6 GHZ/2M Cache Xeon, 800MKz Front side Bus Processor: Dual Processor for 800FSB, PowerEdge 2850 Memory: 8GB DDR2, 400MHz Operating System: Windows 2003 Enterprise Edition, 25 Client Access Licenses English (420-3895); Linux RedHat Advanced Server 5.0 Update 2
Database/Data Server	1	HP 9000 Superdome 32-way server Base Unit: HP Superdome EDB has a hard partition on each server consisting of 8 CPUs Processor: PA8700+ 875MHz CPU Memory(16GB): 512Mb DIMM Hard Drive: 36GB

System Resources		
Resource	**Quantity (Minimum)**	**Name and Type**
		<u>DVD Drive:</u> DVD ROM Device for HP Server Superdome systems
		<u>NIC:</u> PCI 1000Base-T Fibre Channel Adapter; PCI 10/100Base-T LAN Adapter
		<u>Operating System:</u> HP-UX Enterprise OE Server Media - HP-UX 11i Version 1

Glossary

Name	Definition
AITC	The Austin Information Technology Center, formerly known as the AAC.
Adjudicate	To hear and settle a case through judicial procedure and/or study and settle a dispute or conflict.
Architecture	The organizational structure of a system or component.
Beneficiary	A beneficiary is one that receives a benefit as in VA health care benefits.
Capabilities	Capabilities are pre-defined and are essentially the known HECMS system functions.
Configuration Control Board (CCB)	Represents a group of people who are responsible for evaluating and approving or disapproving proposed changes to a product and or project.
Dependent	Individual relying on or requiring the aid of another for support.
Enrollment	The process for providing beneficiaries access to VA health care benefits covered by the medical benefits package.
Enrollment Group Threshold (EGT)	EGT is the enrollment priority limit set per the Secretary of the VA for enrollment inclusion. These settings are used to determine which priority groups (and/or subgroups) are eligible for enrollment into the VA healthcare system.
Enrollment System Redesign (ESR)	Designed for the completion development of the Enrollment Database (EDB) Version 3.0. EDB Version 3.0 replaces the HEC Legacy system and provides additional enhancements in support of the Health Eligibility Center.
Health Eligibility Case Management System (HECMS)	ESR, a.k.a. Enrollment System Redesign. HECMS V3.12 is the Health*e*Vet replacement system for the product known as HEC Legacy.
HealtheVet	My Health*e*Vet is a centralized web based on the J2EE platform. It allows seamless data sharing between all parts of VA.
HEC	The Health Eligibility Center is located in Atlanta, Georgia.
HL7	Health Level Seven is one of several American National Standards Institute (ANSI) -accredited Standards Developing Organizations

Name	Definition
	(SDOs) operating in the healthcare arena.
ILOG Rule	An execution engine that is responsible for application business management processes.
IV	Income Verification
IVM	Income Verification Matching
Means Test Threshold	Means Test (MT) Threshold is the income threshold level set within the VA for establishing benefit levels for veterans. The Veteran's income must fall below this dollar amount to be considered exempt from co pays. These MT Thresholds are supplied each year in a VA Means Test Threshold directive that contains the attributes, start and end dates.
P&T	Permanent & Total
PH	Purple Heart (PH) is a medal awarded to a member of the military who has been wounded or killed in combat or hostile forces.
Priority Groups	The number of veterans who can be enrolled in the health care program is determined by the amount of money Congress gives VA each year. Since funds are limited, VA sets up priority groups to make sure that certain groups of Veterans are enrolled before others.
PSIM	Person Service Identity Management
Service-Connected	Generally, a service-connected disability is a disability that VA determines was incurred or aggravated while on active duty in the military and in the line of duty.
Spring Framework	A light container framework with an AOP base module support.
TLS	Transport Level Security
VA	Department of Veterans Affairs
VAMC	Department of Veterans Affairs Medical Center
VBA	Veterans Benefit Administration
VADIR	VA/DoD Information Repository
VAMC	Department of Veterans Affairs Medical Center
VBR	Veterans Benefits Repository

Name	Definition
Veteran	A person who has served in the armed forces.
VistA	Veterans Health Information Systems and Technology Architecture - the system that manages clinical and business information for VA.
VOA	Veteran Online Application
VPID	Veterans Affairs Person Identifier
WebHelp	An Adobe (RoboHelp) output type that is designed for authors who want to be sure that end users can view their Web-based or desktop application Help on virtually any browser and platform.

References and Official Policies

The following were used in the certification and accreditation of this system:

• NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995

• NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996

• NIST Special Pub 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001

• NIST Special Pub 800-30, Risk Management for Information Technology Systems, January 2002

• NIST Special Pub 800-34, Contingency Planning Guide for Information Technology Systems, June 2002

• Public Law 104-106, Clinger-Cohen Act of 1996, formerly Information Technology Management Reform Act, August 8, 1996

• Electronic Government Act of 2002, Title III, Federal Information Security