Web VistA Remote Access Management

Release 1.2

Deployment, Installation, Back-Out, and Rollback Guide

May 2020

Department of Veterans Affairs

Office of Information and Technology

Revision History

Date	Document Version	Description	Author
5/5/2020	1.0	Initial document publication for WebVRAM Release 1.2 *(associated with information-only patch WEBG*1.0*1)*.	WebVRAM Project Team, VA Office of Information and Technology (OIT) Enterprise Program Management Office (EPMO)

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Plan (DIBR) for new products going into the VA Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software, and should be structured appropriately, to reflect particulars of these procedures at a single or at multiple locations.

Per the Veteran-focused Integrated Process (VIP) Guide, the Deployment, Installation, Back-out, and Rollback Plan is required to be completed prior to Critical Decision 2 (CD2), with the expectation that it will be updated throughout the lifecycle of the project for each increment, as needed.

Table of Contents

List of Figures

List of Tables

1.   Introduction

This document describes how to deploy and install the Web VistA Remote Access Management (WebVRAM) product, as well as how to back-out the product and rollback to a previous version or data set. This document is a companion to the project charter and management plan for this effort.

1.1.   Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the WebVRAM solution, will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

1.2.   Dependencies

Dependencies include:

- Secure Shell (SSH) communications protocol is required at regional VistA systems or individual VistA instances where the application is intended to be used.

- VistA sites must support use of RPC Broker v1.1 component.

- Successful use of WebVRAM to access remote VistA systems requires:

  o Remote VistA system must be accessible via VA Wide Area Network (WAN) resources.

  o Implementation of Local Security Keys must be communicated and incorporated into the WebVRAM user profile where impact to assigned menus or options exist.

  o Remote VistA system configuration changes impacting connectivity (i.e. port, protocol, initial logon prompt) must be communicated and incorporated into the WebVRAM system USER TABLE.

  o Remote application entry must be configured in the remote VistA system.

  o Specific WebVRAM VistA Security Keys must be stored in the remote VistA system.

- Synchronization of the User Account Profile is required for WebVRAM to function.

- Synchronization of User Account credentials is required for VistA Graphical User Interface (GUI) Application usage by WebVRAM users.

1.3.   Constraints

There are no additional constraints to this project.

2. Roles and Responsibilities

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
1	Project Team and Development Team	Deployment	Plan and schedule deployment (including orchestration with vendors).	Increment 7
2	Development Team	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.	Increment 7
3	Enterprise Operations (EO)	Deployment	Test for operational readiness.	Increment 7
4	Development Team	Deployment	Execute deployment.	Increment 7
5	Development Team	Installation	Plan and schedule installation.	Increment 7
6	Project Team/Hosting Team	Installation	Ensure Authority to Operate and that certificate authority security documentation is in place.	Increment 7
7	Development Team	Back-out	Confirm availability of back-out instructions and back-out strategy (the criteria that trigger a back-out).	Increment 7
8	Enterprise Support Desk (ESD)/Development Team	Post Deployment	Provide hardware, software and system support.	Increment 7

This section describes the teams who perform the steps described in this plan. Representatives from the teams listed in the following table perform deployment and installation activities. This phase begins after the solution design (including deployment topology) is complete. Design activities are not included in this phase.

Table 2: General Roles and Responsibilities

Team	Tasks / Responsibilities
ESD Team	- Receive and process incoming incidents via Service Now Ticket. - Determine incident types and capture all relevant incident data. - Create developer user accounts. - Troubleshoot and resolve basic issues.

Team	Tasks / Responsibilities
VA Project Team	• Liaison between the Development Team and the ESD Team. • Facilitate deployment and issue resolution. • Identify and submit issues to the VA Project Manager.
WebVRAM Development Team	• Develop and deploy the application between environments. • Provide Tier 3 support for application issues. • Identify and submit issues to the VA Project Manager.

Table 3: Code Deployment Responsibilities

Team	Phase	Role
WebVRAM Development Team	Planning	• Finalize development increment and code compilation instructions. • Provide listing of developer accounts.
WebVRAM Project Team	Planning	• Schedule Software Quality Assurance (SQA) and Initial Operating Capability (IOC) testers and support all aspects of IOC Testing preparation.
WebVRAM Development Team	Prepare for Deployment	• Freeze all development activities. • Request secure and technical code reviews. • Resolve internal QA testing defects/issues and IOC testing defects/issues.
WebVRAM Project Team	Execute Deployment	• Coordinate deployment support by maintaining the bridge and managing all involved stakeholders. • Conduct IOC Testing activities.
Microsoft Development Team	Execute Deployment	• Work with Project Team to resolve issues. • Deploy final increment version from DEVTEST to PREPROD. • Deploy final version of code from PREPROD to PROD.
WebVRAM Project Team	Validation & Go-Live	• Validate that the PROD environment functions as expected.
Development Team	Validation & Go-Live	• Execute rollback, if necessary. • Provide Tier 3 support as required.

3.   Deployment

The deployment is planned as a single rollout.

This section provides the schedule and milestones for the deployment.

This Installation Guide identifies processes and procedures to promote the Web VistA Remote Access Management (WebVRAM) system into the Production environment. The WebVRAM system is web-based and is deployed using files containing configuration information rather than code package objects moved directly from one environment to another.

3.1.   Timeline

The deployment and installation will run for approximately one day, as depicted in the master deployment schedule WebVRAM.

The high-level schedule is included below:

Table 4: High-level Milestones

Milestones	Target Date
WebVRAM Project Initiation	10/26/2018
Increment 1 – VA Enterprise Cloud Setup/System Integration Testing	1/22/2019[1]
Increment 2 – WebVRAM Single Sign-on to FBCS/VistA	4/4/2019
Increment 3 – Redesign of WebVRAM	6/28/2019[1]
Increment 4 – IOC and Production Release (Redesign)	9/27/2019
Increment 5 – Two Factor Authentication (2FA) Development	12/18/2019
Increment 6 – Production Hot Fix	3/18/2020
Increment 7 – 2FA Production Release Part 2	6/17/2020
Sustainment – Defect Repair/System Enhancements	6/16/2020-9/14/2020
Project Closeout	9/15/2020-10/13/2020

3.2.   Site Readiness Assessment

This section discusses the locations that will receive the WebVRAM deployment. Topology determinations are made by the project architect and lead developer and vetted with the Strategic Technology Alignment Team (STAT) and Project Manager during the design phase as appropriate. IOC testing arranged through a Memorandum of Understanding (MOU) with each testing site will be coordinated with the Area Manager and designated VistA Applications Division Supervisor. Site readiness will be assessed prior to and during IOC testing in the site Pre-production and Production environments.

---

[1] As reported on the VIP Dashboard.

3.2.1. Deployment Topology (Targeted Architecture)

Deployment will be conducted through web client in a DEVTEST, Pre-production (PREPROD), and Production (PROD) environment administered by the Development Team.

The WebVRAM system is web-based and is deployed using files containing configuration information rather than code package objects moved directly from one environment to another.

Figure 1 outlines the physical architecture for deployment of the application from development through national release.

Figure 1: WebVRAM Physical Architecture and Environments
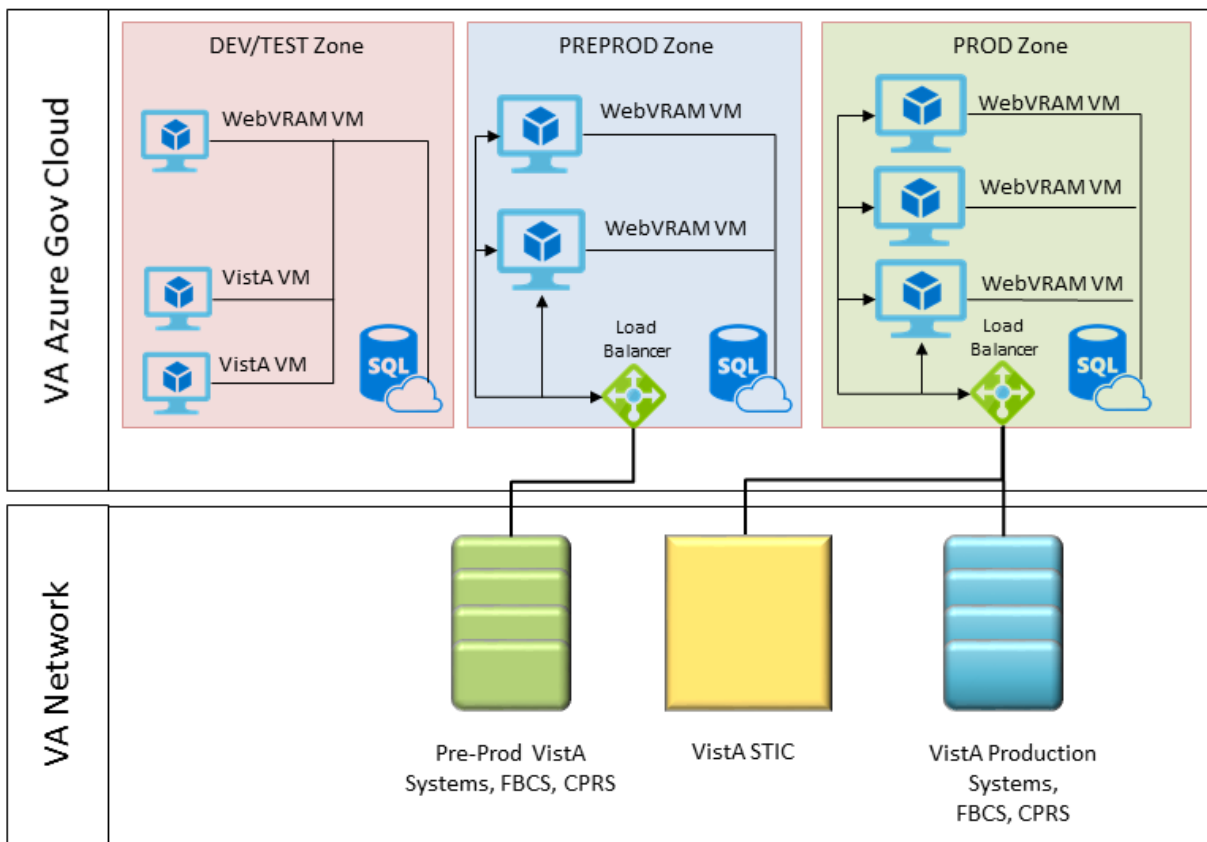
The WebVRAM Administrative Module (WAM) with a GUI front-end will provide an automated method of obtaining business user profile information to populate the WebVRAM USER TABLE to create the WebVRAM user profile. The business stakeholders will provide the user's basic information, which will be used by the WAM to query the user's local VistA instance(s) to gather their VistA user profile.

NOTE: Provisioned users who routinely perform work at more than one VA location will have a WebVRAM user profile consisting of a superset of all authorized VistA menus and keys from all locations.

WebVRAM communicates within its internal DEVTEST, PREPROD, and PRODUCTION environments through Transmission Control Protocol (TCP) connections defined by specifically authorized Internet Protocol (IP) addresses and ports.

In the DEVTEST environment, Application Windows Operating System (OS) Virtual Machines (VMs) communicate with two Linux OS VMs which host the four VistA database instances used for development and testing of the application. The application also communicates through a TCP/IP connection with its DEVTEST SQL database. Connections to testers' VA workstations for application testing are initiated through instantiation of the WebVRAM DEVTEST URL. The tester's VistA user profile is fabricated to replicate the necessary VistA menus, keys, user/person class and electronic signature code to fully test WebVRAM functionality. This "testing" user profile is stored in the WebVRAM USER TABLE on the DEVTEST SQL database. All tester Personally Identifiable Information (PII) data is fabricated and has no relation to the tester's actual demographic data.

In the PREPROD environment, WebVRAM Windows OS application VMs communicate with IOC site Pre-production (Test) VistAs, Pre-production Fee Basis Claim System (FBCS) servers, and Computerized Patient Record System (CPRS) Pre-production instances to accommodate required Pre-production testing. All TCP connections use authorized IPs and ports and are considered on-premise connections as all applications and databases reside within the VA network. The application also communicates through a TCP/IP connection with its PREPROD SQL database. Connections to testers' VA workstations for application testing are initiated through instantiation of the WebVRAM PREPROD URL. The IOC tester's user profile is retrieved by the WebVRAM Pre-production application version, and the local tester's VistA profile data is pulled from the tester's IOC Pre-production VistA NEW PERSON FILE to create the WebVRAM user profile stored in the Pre-production WebVRAM USER TABLE.

The VistA Station ID Callback (STIC) Remote Procedure Call (RPC) verifies that the user has current, active VistA credentials and permissions. The WebVRAM application then retrieves the following data from the local VistA files listed for the user:

- 200 – NEW PERSON
- 19 – OPTION
- 19.1 – SECURITY KEY
- 201 – PRIMARY MENU OPTION
- 203 – SECONDARY MENU OPTIONS
- 51 – KEYS
- 101.13 – CPRS TAB
- 9.2 – TERMINATION DATE
- 2 – ACCESS CODE
- 11 – VERIFY CODE
- 200.04 – MULTIPLE SIGN-ON
- 200.18 – AUTO SIGN-ON
- 7 – DISUSER
- 20.4 – ELECTRONIC SIGNATURE CODE

- 20.3 – SIGNATURE BLOCK TITLE

- 20.2 – SIGNATURE BLOCK PRINTED NAME

- PERSON CLASS

- USER CLASS

- 8 – TITLE

- 41 – ALLOWED TO USE SPOOLER

- SERVICE/SECTION

- NAME

- DEGREE

- NATIONAL PROVIDER IDENTIFIER (NPI)

- NPI STATUS

- 200.1 – TIMED READ

  - If the existing visited site value < 900, the value is set to 900; otherwise, no action is taken.

The connections established between the WebVRAM PROD environment and VA Network Production VistA, FBCS, and CPRS instances also utilize authorized TCP/IP connections through specified ports. The application communicates through a TCP/IP connection with its PROD SQL database. User login is facilitated through the WebVRAM PROD URL. At user login, the user's VistA profile data is pulled from the user's local IOC Production VistA NEW PERSON FILE to create the WebVRAM user profile stored in the production WebVRAM USER TABLE. If the user is directed by line management and authorized to perform work at more than one VistA on a daily or routine basis, each VistA instance is queried to create a superset of that user's VistA profile containing all menus, keys, user/person class and electronic signature code data. The user's "home" VistA Access/Verify codes are kept in the WebVRAM user profile and passed to remote VistA systems the user is authorized to access.

All application-to-VistA communications will be facilitated through RPC Broker protocol. User-to-application connections will utilize web protocol in keeping with VA Enterprise Design Patterns.

3.2.2. Site Information (Locations, Deployment Recipients)

The WebVRAM system is web-based and is deployed using files containing configuration information rather than code package objects moved directly from one environment to another.

3.2.3. Site Preparation

VistA Production instances installed patch WEGB*1.0*0 with the first release of the product (WebVRAM Release 1.0). For WebVRAM Release 1.2, an Information Only patch will be distributed since there are no VistA updates associated with this release. This Information Patch will be WEGB*1.0*1. The web application will sustain software changes and be deployed into the production instances in the Azure Cloud.

3.3.   Resources

This section describes hardware, software, and facilities required for the WebVRAM deployment and installation.

3.3.1.   Facility Specifics

WebVRAM will deploy on a cloud-hosted environment. There are no facility-specific features required for deployment.

Table 5: Facility-specific Features

Site	Space/Room	Features Needed	Other
IOC	None	N/A	N/A
Enterprise VistA Sites	None	N/A	N/A

3.3.2.   Hardware

WebVRAM will be supported by the existing Azure cloud-hosted environments. See Section 3.2.1 Deployment Topology (Targeted Architecture) for hardware topology.

Table 6: Hardware Specifications

Required Hardware	Model	Version	Configuration	Manufacturer	Other
Windows Virtual Machine (VM) – 3 each	DS3	Version 2	4 cores (14GB RAM) w/ 1 P10 (128GB) managed premium OS Volume	Microsoft Azure	N/A
SQL Database	Gen4	vCore	2 cores (14GB RAM) Business Critical Tier w/ 100GB Data Storage	Microsoft Azure	N/A
Load Balancer	Basic	IPv4	Private with back-end connections to 3 application VMs	Microsoft Azure	N/A

Please see Section 2 Roles and Responsibilities for details about who is responsible for preparing the site to meet these hardware specifications.

3.3.3. Software

WebVRAM will be utilizing approved existing software listed on the [VA Technical Reference Model (TRM)](#).

Table 7: Software Specifications

Required Software	Make	Version	Configuration	Manufacturer	Other
RPC-BSE	N/A	1.1	TCP M-based server connection enabler	VA Infrastructure and Security Services	N/A
ASP.NET Core	N/A	2.2	Application run-time support	Microsoft	N/A
.NET Framework	N/A	4.7	Framework which runs ASP.NET	Microsoft	N/A

3.3.4. Communications

A VA Skype meeting will occur for all members involved and/or invested in WebVRAM deployment. All members involved and/or invested in WebVRAM deployment will receive status emails throughout the deployment activities.

Table 8: Team Support Information/Role

Team Support Information	Role
Communication Lead *Scheduled*	Serves as the main communication and coordination point of contact on behalf of the application to provide regular status updates and issue escalation.
SQA Tester(s) *Scheduled*	Performs testing to verify that application is functioning as expected.
Development *On Call*	Development resources are typically on-call for production deployments, unless they are required to serve as advisory resources during the release activities.
VA VIP Triad *On Call*	Perform a VIP Critical Decision 2 (CD2) review of the application to approve national release if all VIP requirements are met.
VA Business / TDD *On Call*	Engage Business Contacts if decisions need to be made regarding production issues.
Development Team *Scheduled*	Application Support contacts are scheduled to perform Production code releases and infrastructure changes.
Product Support *On Call*	Product Support contacts are scheduled to assist with VistA patch distribution or are otherwise scheduled to be on call.

Team Support Information	Role
VA Enterprise Cloud (VAEC) Cloud Operations Management (COMS) Team *Scheduled*	Typically, on-call support for infrastructure issue troubleshooting and resolution.

3.3.4.1. Deployment/Installation/Back-Out Checklist

This section will be completed once each task is complete.

Table 9: Deployment/Installation/Back-out Checklist

Activity	Day	Time	Individual who completed task
Deploy	May 13, 2020	TBD	Development Team Member
Install	May 13, 2020	TBD	Development Team Member
Back-Out	May 13, 2020	TBD	Development Team Member

4. Installation

4.1. Pre-installation and System Requirements

Beginning with WebVRAM Release 1.2, system requirements are tracked in the Backlog in the Jira WebVRAM repository. WebVRAM Release 1.0 customer-approved user stories/system requirements are archived in the WebVRAM Rational Tools repository.

4.1.1. VistA Patch Installation

An Information Only patch, WEBG*1.0*1, will be forwarded to all VistA sites. There are no VistA updates/changes associated with this release.

4.2. Platform Installation and Preparation

Deployment occurs during off hours, after 6:00 PM EST.

Software installs within 60-120 minutes.

4.3. Download and Extract Files

The WebVRAM system is web-based and is deployed using files containing configuration information rather than code package objects moved directly from one environment to another.

For the identified extract files, refer to the "webvram_files_list.txt" text file located in the env_depl_impl folder in the GitHub WebVRAM product repository.

The WebVRAM Source Code can be found in the GitHub WebVRAM code repository.

4.4. Database Creation

This section is not applicable.

4.5. Installation Scripts

This section is not applicable.

4.6. Cron Scripts

There are no Cron[2] scripts for this installation.

4.7. Access Requirements and Skills Needed for the Installation

To complete the installation:

- Basic system administration skills are needed.

- Access to the web server is required.

- Permission is needed to:

    o Start/Stop the web server.

---

[2] A Cron script is a term for a routine or script that runs chronologically (i.e., runs on a regular timetable).

        o   Update WebVRAM web application files.

4.8.   Installation Procedure

The Installation Procedure is as follows:

1. Stop the web server.
2. Copy the WebVRAM files to the configured web application folder.
3. Configure the WebVRAM application to use the appropriate database.
4. Start the web server.

4.9.   Installation Verification Procedure

Visit the web application at its [WebVRAM Homepage](#):

1. Login using credentials.
2. Test drive the application.
3. Check the application logs for any errors.

4.10. System Configuration

Figure 2: WebVRAM Single Production String shows the configuration of a single production string to the extent that it is known. A full production aspect of the application will involve multiple users and VistA sessions through several cloud subnets.

The user logs in to the WebVRAM web application located in the cloud. The application utilizes the VistA Station ID Callback module and communicates with remote VistA systems via RPC Broker. The user is connected to the remote VistA systems via Secure Shell (SSH).

Figure 2: WebVRAM Single Production String
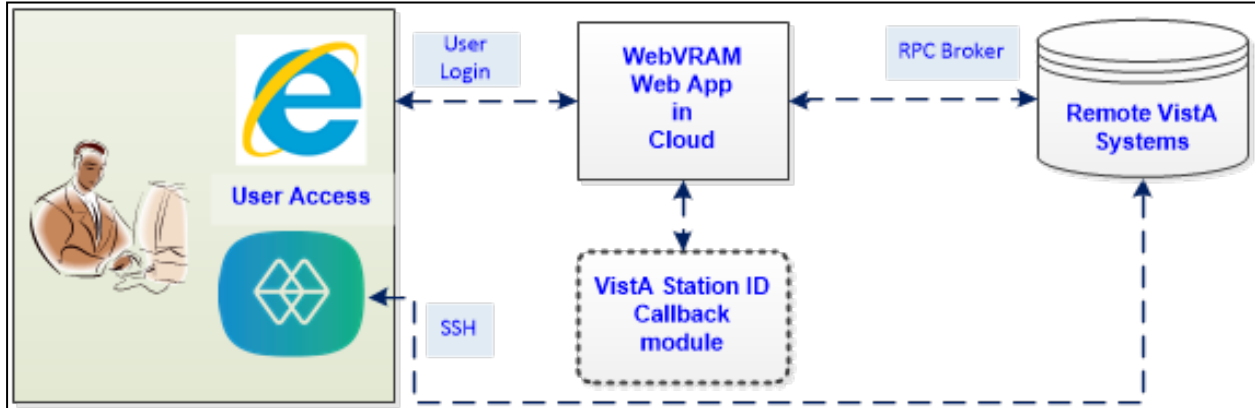
4.11. Database Tuning

This section is not applicable.

5.   Back-Out Procedure

Back-out pertains to a return to the last known good operational state of the software and appropriate platform settings. Should a rollback of this deployment occur, the software will be removed from the appropriate platform.

5.1.   Back-Out Strategy

Back-out and rollback are highly intertwined. The same high-level procedure is in place for both back-out and rollback. The back-out and rollback strategy for a project begins at the time of application deployment. Back-out and rollback procedure will bring the system back to the functionality of the previous release. The steps below describe, at a general level, what should be included in the procedure for back-out/rollback:

1.   At the time of system deployment, create a complete backup of the system and store it on a separate machine.

2.   Proceed with application-specific system deployment steps. If the system fails during deployment, perform a system rollback using the system backup created in step 1.

3.   Perform thorough and comprehensive testing to ensure the integrity and functionality of the system.

4.   Perform a system backup once the system is deemed stable and ready for users and store it on a separate machine. Once users begin working on the system, regularly create system backups and store them on another machine.

5.   If system failure occurs after users are on the system, perform a system rollback using the system backup created in step 4.

6.   Any client machines may need to clear their web browser cache before they will see the effects of the system rollback.

The strategy above provides assurance against fault and a guaranteed rollback position in the event of an undiagnosed fault. At times, however, there may be a reason to not rollback the complete solution migration and instead only rollback a portion of it. Some potential reasons for this include:

- The fault is easily identified and localized in a single software component which is deemed non-essential.

- The fault is not identified during initial release testing, but only after the solution is in use in Production and a complete database restore is no longer an option.

- The backup file is corrupted or lost.

In such cases, alternate approaches may be taken to restore the system to its previous state, although each approach will be dependent on the situational specifics.

5.2. Back-Out Considerations

5.2.1. Load Testing

Load testing is a performance test that subjects the system to varying workloads to measure and evaluate the performance behaviors and abilities of the system to continue to function properly under these different workloads. Load testing determines and ensures that the system functions properly beyond the expected maximum workload. Additionally, load testing evaluates the performance characteristics (e.g. response times, transaction rates, and other time-sensitive issues).

5.2.2. User Acceptance Testing

Pre-production IOC testing was conducted Apr. 13-17, 2020. The software is tested from both a user perspective and Business Unit Administrator perspective to ensure all screens are tested. Functional defects are reported and resolved.

Business Owner approval for national release was obtained on May 5, 2020.

5.3. Back-Out Criteria

The criteria for a back-out are:

- The fault is easily identified and localized in a single software component that has been deemed non-essential.

- The fault is not identified during initial release testing, but only after the solution is in use in production, and a complete database restore is no longer an option.

- The backup file is corrupted or lost.

5.4. Back-Out Risks

There are no risks to removing the WebVRAM product as this is the inaugural release for the product.

5.5. Authority for Back-Out

Authority for back-out should be provided by the VA Project Manager, Laura Young.

5.6.   Back-Out Procedure

The Back-Out Procedure is as follows:

1. Stop the web server.

2. Remove the WebVRAM files to the configured web application folder.

3. Remove the configuration of the WebVRAM application from the appropriate database.

4. Start the web server.

5.7.   Back-Out Verification Procedure

To verify back-out:

1. Visit the web application at its WebVRAM Homepage.

2. Locate the version information at the bottom of the page.

3. Check the application logs for any errors.

Figure 3: WebVRAM Homepage
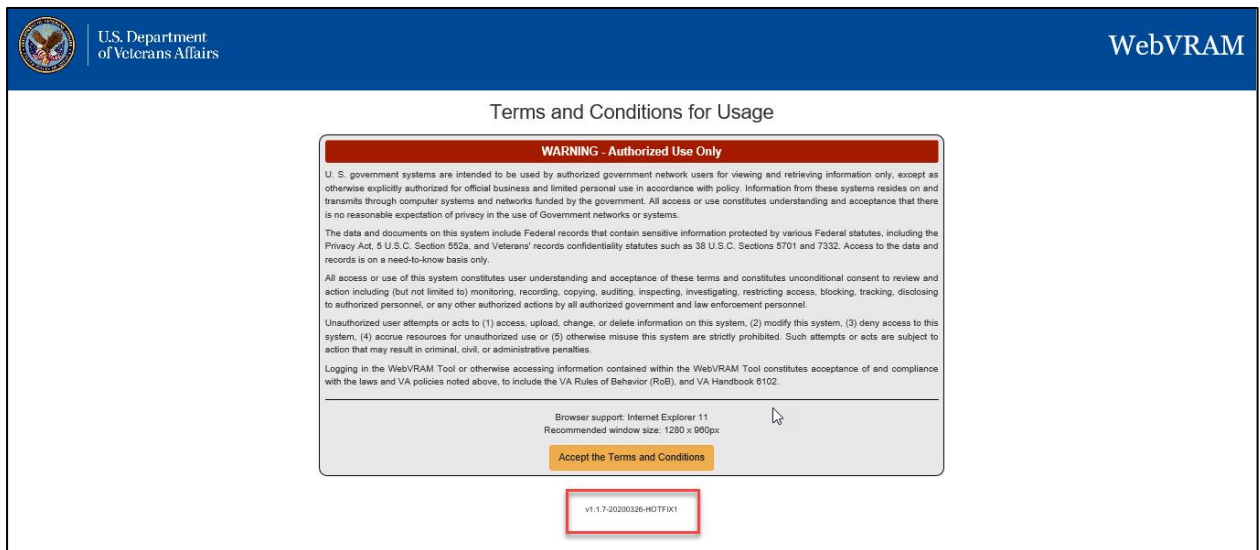
6. Rollback Procedure

This section describes the processes necessary to perform the Rollback Procedure.

6.1. Rollback Considerations

Business Owner approval will decide viability to proceed.

6.2. Rollback Criteria

Restore backup of Production environment taken prior to deployment.

6.3. Rollback Risks

No risks have been identified.

6.4. Authority for Rollback

Authority for rollback should be provided by the VA PM, Laura Young.

6.5. Rollback Procedure

A member of the Development Team will be assigned to this deployment. Rollback procedure is outlined above in Section 5.6.

6.6. Rollback Verification Procedure

After a rollback procedure has been performed, the WebVRAM product will be rolled back to the previous version in the production environment. Verification procedure is outlined above in Section 5.7.