**SPLASH PAGE LANGUAGE**
**(Remove Splash Page Language before submitting to PIA Support)**

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

*The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements*
*under the Federal Information Security Management Act (FISMA).*

VA HANDBOOK 6508.1: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," July 2015, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=810&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

# WebVRAM VistA Remote Access Management (WebVRAM) Assessing

# Office of Information and Technology (OIT)

# Software Product Management (SPM)

# Patient Care Services (PCS) Product Line

Date PIA submitted for review:

May 17, 2023

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Lynn A Olkowski | Lynn.Olkowski@va.gov | 202-632-8405 |
| Information System Security Officer (ISSO) | Brian Orange | Brian.orange@va.gov | 512-762-2482 |
| Information System Owner | Laura Young | Laura.young3@va.gov | *847-420-7401* |

## Abstract

*The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.*

Web VistA Remote Access Management (WebVRAM) is a web-based, cloud-hosted application utilizing VA Enterprise Architecture and Design principles which facilitates provider, clinician, Consolidated Patient Accounting Center (CPAC), Office of Community Care (OCC) staff and Enterprise Service Desk (ESD) access to multiple remote Veterans Health Information Systems and Technology Architecture (VistA) applications without requiring users to establish login authentication and credentials at each VistA. WebVRAM provides authorized users access to remote systems to perform VA-directed job duties corresponding to their local VistA credentials and makes a remote connection for the user to VistA sites the user is authorized to access. Once the connection is established and the VistA application of the user's choosing is launched at the remote site, WebVRAM becomes dormant and all user interaction with Veteran data is controlled by the remote application (VistA, Computerized Patient Record System (CPRS), etc.) the user launches at the remote site. All the remote VistA systems accessed contain Veteran clinical and claim data required to provide clinical care, benefit status or claims activation. Clinical data will be viewed by an authorized VHA provider or clinical team providing healthcare to a specific Veteran at any location. Veteran claims data will be viewed by CPAC and OCC evaluating the Veteran benefits status. The need for multiple VistA sessions, with separate user profile login to each VistA instance, is eliminated. WebVRAM is available for internal VA use only, with no public facing portal.

## Overview

*The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:*

1 *General Description*

A. *The IT system name and the name of the program office that owns the IT system.*

Web VistA Remote Access Management (WebVRAM) Assessing Office of Information and Technology (OIT) Software Product Management (SPM) Patient Care Services (PCS) Product Line.

B. *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*

In April 2011, the Executive Director of Office of Information Technology (OIT) Field Operations challenged the Director, Region Field Program Office (FPO), with finding a technology solution to solve access control complexities for the Consolidated Patient Account Center (CPAC). As a result, a Single Sign On (SSO) project was chartered to develop a local application, utilizing existing capabilities of the VistA System and Remote Procedure Call (RPC) Broker that would potentially be migrated to the VA enterprise to allow remote access (read and write), using a single set of credentials, for organizations requiring access to information resources provided by Veterans Health Information Systems and Technology Architecture (VistA). The VistA Remote Access Management application (VRAM) was developed to address these access control complexities. VRAM has been deployed to CPAC users to allow remote terminal emulation and certain GUI application connectivity to perform consolidated Medical Care Cost Fund/Recovery and other activities as part of the CPAC mission. VRAM uses a graphical user interface (GUI) written in DELPHI that requires individual distribution and installation on the desktop of individual users, which in turn requires knowledge of and support from local IT staff. This thick-client, distributed application sustainment model is less than ideal as compared to modern, thin client web-based applications. Additionally, the version of DELPHI that VRAM was programmed in is outdated and no longer supported on the VA TRM. Rather than continuing to follow that outdated and costly sustainment model, in 2014 VHA engineers developed a web-based version of VRAM which provided the traditional VRAM functionality while also enhancing upon its capabilities. Being web based, the application can now be centrally maintained requiring no client-side installation and no local IT support. The new WebVRAM application provides the capability to access authorized VistA accounts nationwide, allowing users to remotely execute VistA, and Computerized Patient Record System (CPRS) menu options in support of their business model and mission, with a single URL login. WebVRAM is a web-based, cloud-hosted application utilizing VA Enterprise Architecture and Design principles which facilitates provider and clinician access to multiple remote VistA systems and CPRS systems, and related business applications without requiring physician users to establish login authentication and credentials at each VistA where Veteran clinical data is related to the Veteran and includes all data associated with that Veteran that would be required to provide any clinical care. Clinical data will be viewed by an authorized VHA provider or clinical team providing healthcare to a specific Veteran at any location. The need for multiple VistA sessions, with separate user profile login to each VistA instance, is eliminated. WebVRAM will be available for internal VA use only. There are currently 15,000+ users who will be connecting to/using the application. Typical users and client types are listed here: Primary Care Physician, Consulting Physician, Telehealth Services Clinicians, Telestroke Clinicians, Community Care Office Staff, CPAC (Consolidated Patient Account Center) Staff, OIT

Enterprise Service Desk (ESD) Staff This will be an Enterprise system, providing Class 1 software to all VA regions. The WebVRAM application authenticates the user by obtaining their VA Network ID from their Windows VA Login information and passing that Network ID to their local VistA system. Once the local VistA system recognizes the user as "authorized", the application receives user VistA keys, menus as part of the user login transaction. The VA Network ID and VistA profile data are stored it in the application SQL database for Audit logging purposes only. All data, including VA Network ID for auditing purposes, is maintained internally on the application's SQL database and is not available nor shared with any VA users. User Profile information containing menus and keys the users are authorized to use by their line management, along with a single-use token received from the VistA system, is passed to each remote VistA system the user accesses, and written into the New Person file of the target VistA system. This profile/token allows login to the remote VistA system for the user requiring access to that system to perform their job (Telehealth or Telestroke patient care, clinical care, etc.), The following modules within the application control or store application information/data: Login module – Uses VistA system to validate users logging into the WebVRAM application. RPC broker module - creates a bridge to connect client applications on workstations to the Mbased data and business rules on M servers through TCP connections. No shared data in this transaction is stored by WebVRAM or the M servers. • Caching module - Captures the user profile information and creates an audit record in the WebVRAM SQL data base for Audit logging. • Exception Handler module – Captures any system or data errors in the WebVRAM exception log table WebVRAM is an enterprise, cloud-hosted web-based application accessible from any VA enterprise location via login URL. PII is maintained as part of the user login transaction for WebVRAM Audit purposes and is shared with the user's local VA VistA system for purposes of user authentication. A three-year Authority to Operate was granted on 12/10/2020 with an expiration date of 12/10/2023.The Business Owner and Stakeholders have approved funding for development and deployment of the system for production use. No business process will be changed with the completion of this PIA. Completion of this PIA will not result in technology changes. All WebVRAM software, hardware and networking components are TRM approved, built using VA Enterprise Cloud (VAEC) guidelines, and operate within the VA Intranet hosted by the VAEC Microsoft Azure Government (MAG) Cloud services as part of the VA FedRAMP certified cloud network topology. WebVRAM utilizes the 79VA10/85FR84114, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. SORN.

C. *Indicate the ownership or control of the IT system or project.*

Office of Information and Technology (OIT) Software Product Management (SPM)Patient Care Services (PCS) Product LineDepartment of Veterans Affairs.

*2. Information Collection and Sharing*

D. *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*

The current number of users is 15,000+ and could reach up to 25,000 users. The users are VA employees/contractors. No patient data is persisted or stored by WebVRAM.

E. *A general description of the information in the IT system and the purpose for collecting this information.*

The users are VA employees/contractors and their VA network ID, their VA email, and full name are stored within WebVRAM. These users utilize WebVRAM in order to have access to multiple, remote VistA sites throughout the VA to perform their job (Telehealth or Telestroke patient care, clinical care, etc.). The VA User's Profile information contains the menus and keys the users are authorized to use by their service line management, along with a single-use token received from the VistA system, is passed to each remote VistA system the user accesses and written into the New Person file of the target VistA system. No patient data is persisted or stored by WebVRAM.

F. *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*

WebVRAM shares information with various VistA systems throughout the VA. The following modules within the application control or store application information/data: Login module – Uses VistA system to validate users logging into the WebVRAM application. RPC broker module - creates a bridge to connect client applications on workstations to the M-based data and business rules on M servers through TCP connections. No shared data in this transaction is stored by WebVRAM or the M servers. Caching module - Captures the user profile information and creates an audit record in the WebVRAM SQL data base for Audit logging. Exception Handler module – Captures any system or data errors in the WebVRAM exception log table. PII is maintained as part of the user login transaction for WebVRAM audit purposes and is shared with the user's local VA VistA system for purposes of user authentication.

G. *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*

WebVRAM cache at the termination of each user session. PII login transaction data, as received from the Windows AD Service and STIC Module, are stored in an encrypted JavaScript Object Notation Web Token (JWT), which is not persisted when the user browser closes. PII data is NOT created, received, used, or maintained internally, nor is it shared with external applications. WebVRAM uses SSN during the duplicate account check on the remote VistA site during account synchronization. The SSN is read from the home VistA account into memory and passed to the remote VistA, then remove from WebVRAM memory once the synchronization is completed. Controls applicable to the application are recorded in eMASS.

*3. Legal Authority and SORN*

H. *A citation of the legal authority to operate the IT system.*

WebVRAM utilizes the 79VA10/85FR84114, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. SOR

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The SORN will not require revision. The SORN covers cloud usage

*D. System Changes*

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*

*The application uses, but does not collect, SSN for authenticating and synchronizing the user profile to remote VistA systems (not the user's local VistA system), and the PIA will need to be updated to reflect this information. And the PII/PHI data elements have been updated to reflect both the VA Network ID and VA unique Windows Active Directory Identification (ID) along with the local and remote VistA hostnames are being used. NOTE: The WebVRAM Development team will collaborate with vendors who rely on Windows Server 2012 operating systems to document a migration plan from the operating system to the Windows Server 2019 platform. Please note extended support for Windows Server 2016 ends January 2027; with an expected VA divest date of January 2024. WebVRAM will have all current/new Production Virtual machines. (Please see below). Current: VAC21PRDWVR200 [10.245.195.228] VAC21PRDWVR201 [10.245.195.229] VAC21PRDWVR202 [10.245.195.230] New: VAC21PRDWVR210 [10.245.195.231] VAC21PRDWVR211 [10.245.195.233] VAC21PRDWVR212 [10.245.195.234]*

K. *Whether the completion of this PIA could potentially result in technology changes*

*The WebVRAM Development team will collaborate with vendors who rely on Windows Server 2012 operating systems to document a migration plan from the operating system to the Windows Server 2019 platform. Please note extended support for Windows Server 2016 ends January 2027; with an expected VA divest date of January 2024. WebVRAM will have all current/new Production Virtual machines. (Please see below). Current: VAC21PRDWVR200 [10.245.195.228] VAC21PRDWVR201 [10.245.195.229] VAC21PRDWVR202 [10.245.195.230] New: VAC21PRDWVR210 [10.245.195.231] VAC21PRDWVR211 [10.245.195.233] VAC21PRDWVR212 [10.245.195.234]*

## Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

### 1.1 What information is collected, used, disseminated, created, or maintained in the system?

*Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.*

*If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.*
*This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.*

*The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1*.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

☒ Name

☒ Social Security Number

☐ Date of Birth

☐ Mother's Maiden Name

☐ Personal Mailing Address

☐ Personal Phone Number(s)

☐ Personal Fax Number

☐ Personal Email Address

☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)

☐ Financial Information

☐ Health Insurance Beneficiary Numbers Account numbers

☐ Certificate/License numbers*

☐ Vehicle License Plate Number

☐ Internet Protocol (IP) Address Numbers

☐ Medications

☐ Medical Records

☐ Race/Ethnicity

☐ Tax Identification Number

☐ Medical Record Number

☐ Gender

☐ Integrated Control Number (ICN)

☐ Military History/Service Connection

☐ Next of Kin

☒ Other Data Elements (list below)

Other Data Elements - VA Network ID (vhaxxxLnameF) and VA unique windows active directory ID (usually VA email).

**PII Mapping of Components (Servers/Database)**

Windows Servers 2019:
Web: 1 Dev, 2 PreProd, 3 Prod [6 Total],
SQL: 1 Dev, 1 PreProd, 2 Prod [3 Total]

Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Web VistA Remote Access Management (WebVRAM) and the reasons for the collection of the PII are in the table below.
**Note**: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

*Internal Database Connections*

| **Database Name of the information system collecting/storing PII** | **Does this system collect PII? (Yes/No)** | **Does this system store PII? (Yes/No)** | **Type of PII (SSN, DOB, etc.)** | **Reason for Collection/ Storage of PII** | **Safeguards** |
|---|---|---|---|---|---|
| WebVRAM Caching Module – | Yes – collected | Yes - stored) | Other - VA Network ID | Login transaction | Encrypted SQL Database access |

| | | | | | |
|---|---|---|---|---|---|
| Global Address List (GAL) | | | (vhaxxxLnameF); Other - VA Unique Windows Active Directory (AD) identification (usually VA email)<br>• Other - VA Unique Windows Active Directory (AD) identification (usually VA email)<br>• Name – First and Last Name. | capture for audit and user authentication; Finalize user authentication against their local VistA account. | is locked down to WebVRAM Developers and System Administrators, auditors/scanners with elevated privileges; Maintained in an encrypted JSON Web Token during user authentication and stored in SQL database which is only accessible to system administrator with elevated privileges. |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**1.2 What are the sources of the information in the system?**

*These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

*1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?*

VA Active Directory
VistA systems

*1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.*

WebVRAM does not create data or information. WebVRAM utilizes the VA Active Directory and VistA systems as an identification and authentication with the user having to have an active home VistA site and a valid, current VA Network ID. WebVRAM utilizes the user's Active Directory name, pulled from their Windows session initially to allow access to WebVRAM login page. Once we validate a match with our database, the user must enter a valid Access/Verify code for their home VistA account. This information is passed to the VistA system via RPC, verified, and then the user is granted access to the WebVRAM GUI.

*1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.*

WebVRAM does not create data or information

**1.3 How is the information collected?**

*These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

*1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?*

*1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.*

Information is collected and processed through the RPC broker and stored in an encrypted, WebVRAM Cloud SQL database and will be safeguarded in accordance with VA Handbook 6500 and FIPS-140-2 encryption and data processing standards. No paper forms are involved with the collection of PII.

**1.4 How will the information be checked for accuracy? How often will it be checked?**

*These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.*

*1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.*

User PII is collected and received from the VistA and Network Windows Active Directory Login System at each user login.

*1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.*

Not Applicable - WebVRAM does not access a commercial aggregator.

**1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?**

*List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect*

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397

**1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information**

*Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.* (*Work with your System ISSO to complete this section)*

*Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:*

*Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

*Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?*

*Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?*

*Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?*
*This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.*

Follow the format below when entering your risk assessment:

**Privacy Risk:** Intentional/Unintentional disclosure of PII

**Mitigation:** The WebVRAM System Owner identifies and authorizes team members as System Administrators, Developers, and Testers and provides VA user profile information directly to the Microsoft Azure Cloud administrators using the *VA Azure Resource Request Form*. Those resources are then added to the Azure Active Directory for access only to those servers and databases necessary to support development, testing and deployment of the application. ePAS elevated privileges approval is required to gain final access to the servers/databases in question based on validation of the Azure Active Directory entry for each resource. Enterprise Security External Change Council (ESECC) tickets are submitted to obtain approval to open specific IP addresses and Ports and allow connectivity between the VistA test and production systems (Data Source Systems) and the WebVRAM application test, pre-production, and production systems (Data Target Systems). All other connection traffic is blocked by the VA Enterprise Cloud (VAEC) Microsoft Azure Government (MAG).

## Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

**2.1 Describe how the information in the system will be used in support of the program's business purpose.**

*Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.*

Internal Only - VA Network ID, VA Unique Windows Active Directory (AD) identification, SSN, and full name: Used to identify the User. No external use.

**2.2 What types of tools are used to analyze data and what type of data may be produced?**
*These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.*

*2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.*

WebVRAM does not perform complex analysis of data stored in its SQL database. Business management requests for queries against the WebVRAM User Table, sorted by user group, will be provided for auditing of the user profile records only. Data derived from such queries will NOT be placed in any individual existing record, no new records will be created, and no action against or for individuals identified in the query, and no Government employees will make determinations about the individual based on the query records.

*2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the* *individual? If so, explain fully under which circumstances and by whom that information will be used.*

WebVRAM does not create or make available new or previously unutilized information about an individual.

## 2.3 How is the information in the system secured?

*These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.*

*2.3a What measures are in place to protect data in transit and at rest?*

The VA protects the confidentiality and integrity of sensitive and confidential data while at rest, and in transit. All sensitive and confidential data is encrypted using FIPS 140-2 compliant algorithms. The SQL databases are encrypted, and encryption is used in transit. The WebVRAM system only utilizes products from the TRM that has the capability to ensure protection of information at rest. WebVRAM transmits the SSN securely in an encrypted JSON, and then once authentication occurs, the JSON is discarded and not saved.

*2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?*

WebVRAM does not collect, process, or retain Social Security Numbers.

*2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?*

The VA protects the confidentiality and integrity of sensitive and confidential data while at rest, and in transit. All sensitive and confidential data is encrypted using FIPS 140-2 compliant algorithms. The SQL databases are encrypted, and encryption is used in transit. The WebVRAM system only utilizes products from the TRM that has the capability to ensure protection of information at rest. WebVRAM transmits the SSN securely in an encrypted JSON, and then once authentication occurs, the JSON is discarded and not saved. Information is collected and processed which is relevant to the mission of the project through the VA RPC Broker and stored in an encrypted, WebVRAM Cloud SQL database and is safeguarded in accordance with VA Handbook 6500 and FIPS-140-2 encryption and data processing standards. All Azure SQL databases employ FIPS-140-2 encryption of data at rest. WebVRAM is a Moderate Security Impact system hosted in the VAEC Microsoft AZURE Government (MAG) FedRAMP High classified environment. Security controls are in place to ensure data is used and protected in accordance with legal requirements, VA cyber security policies, and VA’s stated purpose for using the data. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. The following training courses are provided to assist in implementation of the Privacy Controls that are in accordance with NIST SP 800-53-rev-4: VA

Privacy and Information Security Awareness Training and Rules of Behavior, TMS #10176 Privacy and HIPAA Training TMS #10203 OIT Role Based training Incident Response testing and training

**2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.**

*Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.* ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

*Consider the following FIPPs below to assist in providing a response:*

*Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?*

*Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?*
*This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.*

*2.4a How is access to the PII determined?*

*2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?*

WebVRAM facilitates multiple SSH VistA sessions for viewing data. As such, the application applies all inherited Azure Cloud hosting VA network and firewall security requirements for displaying Personally Identifiable Information (PII) and Personal Health Information (PHI), as viewed within the framework of VistA sessions. No PII or PHI data is persisted in the WebVRAM cache at the termination of each user session. PII login transaction data, as received from the Windows AD Service and STIC Module, are stored in an encrypted JavaScript Object Notation Web Token (JWT), which is not persisted when the user browser closes. PII data is NOT created, received, used, or maintained internally, nor is it shared with external applications

*2.4c Does access require manager approval?*

Yes

*2.4d Is access to the PII being monitored, tracked, or recorded?*

No

*2.4e Who is responsible for assuring safeguards for the PII?*

WebVRAM Information System Security Officer (ISSO)

## Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

### 3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is* ***retained*** *by the system.*
*This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

Information is only processed by the system through the API's. User VA Network IDs, VA Unique Windows Active Directory (AD) identification, and full name (PII) are stored in the application databases as previously description.

### 3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types.* ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

WebVRAM policy is to retain user login information for no longer than 6 years, 1 month, and 1 day in accordance with RCS 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1.pdfUser profile data will be retained for the useful life of the application, aligned with VA policy for retention of VistA user profile data. A synchronization log is created each time a user connects to a remote VistA site. It includes the log-start/log-end date/times and debugging information. These synchronization logs will be retained for one year.

### 3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

*An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA Records Officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.*
*This question is related to privacy control DM-2, Data Retention and Disposal.*

*3.3a Are all records stored within the system of record indicated on an approved disposition authority?*

User login and user profile data is retained as described in section 3.2 above. Approval for retention of these records is inherited from the NARA approval for VistA login and user profile retention.

*3.3b Please indicate each records retention schedule, series, and disposition authority.*

User Login Information, User Profiles: Records Control Schedule 10-1, January 2021, Item Number 2100.3 entitled “System Access Records”, “Systems requiring special accountability for access”, Disposition Instructions: “Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.” Disposition Authority: AA-GRS 2013-0006-0004, item 31

Synchronization Logs: Records Control Schedule 10-1, January 2021, Item Number 2201.2 entitled “Intermediary Records”, Disposition Instructions: “Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.” Disposition Authority: GRS 5.2, item 020 DAA-GRS2017-0003- 0001

**3.4 What are the procedures for the elimination or transfer of SPI?**

*Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.*

Any residual electronic data or media is sanitized in accordance with VA Handbook 6500.1 for the sanitization of electronic storage media and information technology (IT) equipment that stores or processes VA information by, or on behalf, of the Department of Veterans Affairs (VA). WebVRAM Version follows the Standard Operating Procedure (SOP) for Electronic Media Sanitization stored at the location provided by this URL link:https://dvagov.sharepoint.com/sites/OITDevSecOps/comms/SOP_Library/Forms/AllItems.aspx

**3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?**

*Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.*

WebVRAM utilizes pre-production environments for application development, testing and deployment. During pre-production development and testing, WebVRAM collects user login PII only, and stores/protects that information using the same procedures and controls as those applied to the production system as previously described. When the tester logs into WebVRAM, their login PII (User VA Network IDs and full name) is stored in the pre-production application database. This is the only PII used during testing.
No PII is used for research or training purpose.

### 3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

*Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

*While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.*

*Consider the following FIPPs below to assist in providing a response:*

*Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?*

*Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?*
*This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.*

Follow the format below:

**Privacy Risk:** If information maintained by WebVRAM is retained longer than the minimum time as specified in the *Federal Records Act*, then that information is at increased risk of disclosed or breach.

**Mitigation:** WebVRAM adheres to the NARA General Records Schedule. As designated in the WebVRAM Sustainment Plan, when the retention date is reached for a record, the information is carefully disposed of by the determined method as described in GRS 3.1, item 050 DAA-GRS-2013-0005-00

## Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

**4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?**

**NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.**

*Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.*

*State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.*

*For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.*

*Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?*
*This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.*

*Data Shared with Internal Organizations*

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| VistA (Veterans Health Information Systems and Technology Architecture | VistA – purpose is to identify and validate user at each facility | Network user ID (Identification) also known as VA unique Windows Active Directory Identification (ID), VA Network ID, full name, and SS | VistA RPC Broker |

## 4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

*Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

*This question is related to privacy control UL-1, Internal Use.*

Follow the format below:

**Privacy Risk:** Data sharing is necessary for identification and authentication, and for verification of the user. The WebVRAM application provides the capability to access authorized VistA sites nationwide, allowing users to remotely execute VistA and Computerized Patient Record System (CPRS) menu options in support of their business model and mission, with a single URL login. There is risk data could be shared with inappropriate organizations or institutions which has the potential for a catastrophic impact on privacy.

**Mitigation:** WebVRAM relies on the integrity of the information from the VistA System to be accurate. In order for a user to log into WebVRAM, their user information must come from the VistA System, and the termination dates are lowered from 90 days inactivity to 30 days inactivity at the remote VistA sites, and thus terminated.

## Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

**5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?**

**Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.**

**NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.**

*Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.*

*For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.*

*What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?*

*Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.*
*This question is related to privacy control UL-2, Information Sharing with Third Parties*

*Data Shared with External Organizations*

| *List External Program Office or IT System information is shared/received with* | *List the purpose of information being shared / received / transmitted* | *List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system* | *List the legal authority, binding agreement, SORN routine* | *List the method of transmission and the measures in place to secure data* |
|---|---|---|---|---|

|  | ***with the specified program office or IT system*** |  | ***use, etc. that permit external sharing (can be more than one)*** |  |
|---|---|---|---|---|
| N/A | N/A | N/A | N/A | N/A |

**5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>**

*Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.*

*Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.*

*Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

*This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing*

Follow the format below:

**<u>Privacy Risk:</u>** Not Applicable – no external sharing and disclosure.

**<u>Mitigation:</u>** Not Applicable.

## Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

**6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?**

*These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.*

*6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.*

This Privacy Impact Assessment (PIA) also serves as notice as required by the eGovernment Act of 2002, Pub. L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the PIA under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.".

*6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.*

WebVRAM does not collect information from individuals. For this reason, no notice was provided. The U.S. Department of Veterans Affairs, Veterans Health Administration, Notice of Privacy Practices can be found at this link: Notice_of_Privacy_Practices_VA_Poster_10-163.pdf

*6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.*

WebVRAM does not collect information from individuals. For this reason, no notice was provided.

**6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?**

*This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.*

Employees and VA contractors are required to permit collection of the requested information (VA Network ID) to access the WebVRAM application. If they decline to permit collection of said information, application use is denied.

**6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?**

*This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent* *is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.*

VA permits individuals to agree to the collection of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VA Notice of Privacy Practices and conversations with VA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required. Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing, or sharing PII and PHI. Individuals have a right to restrict the disclosure and use of their health information. WebVRAM does not use PHI, protected health information

### 6.4 PRIVACY IMPACT ASSESSMENT: Notice

*Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

*Consider the following FIPPs below to assist in providing a response:*

*Principle of Transparency: Has sufficient notice been provided to the individual?*

*Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*
*This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.*

Follow the format below:

**Privacy Risk:** There is a risk that an individual may not understand what their information is being collected or maintained about them.

**Mitigation:** Employees and contractors are required to review, sign, and abide by the National Rules of Behavior (ROB) on an annual basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. The VA National ROB and the Contractor ROB address notice and consent issues identified by the Department of Justice and other sources. It also serves to clarify the roles of management and system administrators, as well as to provide notice of what is considered acceptable use of all VA information and information systems, VA sensitive information, and behavior of VA users. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

## Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

### 7.1 What are the procedures that allow individuals to gain access to their information?

*These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.*

*7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions.* ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

WebVRAM users have free and open access to their VA Network ID, and full name, the only PII collected/used by the application, as stored, and publicized in the VA Global Address List (GAL).

*7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).*

WebVRAM is not exempt from the access provisions of the Privacy Act, thus; this question does not apply.

*7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.*

WebVRAM is a Privacy Act system; thus, this question does not apply.

### 7.2 What are the procedures for correcting inaccurate or erroneous information?

*Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

User's VA Network ID is obtained electronically from the Windows Active Directory, based on a current, authorized connection to the VA network. WebVRAM does not control changes to a user's Network ID based on new work assignments or new contract awards. A user could enter an IT Service NOW ticket for any corrections to their Windows Active Directory account with approval by their supervisor.

### 7.3 How are individuals notified of the procedures for correcting their information?

*How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

WebVRAM does not control changes to a user's Network ID (PII) based on new work assignments or new contract awards. Employee and contractors can enter an OIT Service NOW ticket for any corrections to their Windows Active Directory account with approval by their supervisor.

### 7.4 If no formal redress is provided, what alternatives are available to the individual?

*Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.* ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
*This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

Not Applicable – WebVRAM does not control changes to a user's Network ID (PII). Employee and contractors can enter an OIT Service NOW ticket for any corrections to their Windows Active Directory account with approval by their supervisor. Please provide response here

### 7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

*Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks.* ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

*Consider the following FIPPs below to assist in providing a response:*
*Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?*

*Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?*

*Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?*
*This question is related to privacy control IP-3, Redress.*

Follow the format below:

**Privacy Risk:** There is a risk that individuals whose records contain incorrect information may not obtain access to WebVRAM.

**Mitigation:** WebVRAM project staff would work with the affected individual and assist with opening an OIT Snow ticket for the individual. The WebVRAM application web site has a help section and has published a user guide for assistance. In addition, WebVRAM would work with the Business Unit Administrators who would assist their sponsored users.

## Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

**8.1 What procedures are in place to determine which users may access the system, and are they documented?**

*These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

*8.1a Describe the process by which an individual receives access to the system.*

User access to the WebVRAM system will be provisioned and processed in accordance with VA Handbook 6510 (VA Identity and Access Management), which defines the policy and responsibilities to manage identity and access management for the Department of Veterans Affairs (VA) enterprise, and VA Handbook 6500 (Risk Management Framework for VA Information System: VA Information Security Program), which provides the risk-based process for selecting system security controls, including the operational requirements for Department of Veterans Affairs (VA) information technology systems. These policies also define the mandatory requirements for annual information security and privacy training for VA employees and contractors, acknowledging VA Rules of Behavior and Non-Disclosure Agreement (NDA) for contractors who work on the system. In accordance with this process, the users follow their business line management policies/processes to apply for user credentials to access WebVRAM. Those requests for access, once approved by their management, are forwarded to the System Administrators of the VA Network and VistA system and a user profile is created in the VA Network Windows Active Directory and VistA system which contains the VA applications and security keys necessary to use those VistA applications. When a user logs in to the WebVRAM application, a request is sent via RPC Broker to the Windows Active Directory to obtain an authorized VA Network ID. The ID is passed via a second RPC Broker call to the user's local VistA system to validate the user has access and application use privileges on the local VistA system. If the user is an authorized VistA user, the VistA user profile information is returned to the WebVRAM application. Upon user authentication through this electronic exchange, the user is permitted to login to the WebVRAM application and use the application features. If a user does not have an active, authorized VistA profile (has been disusered), they are denied access to the WebVRAM application.

*8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?*

Users from other agencies do not have access to WebVRAM.

*8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.*

1. WebVRAM Administrator: The WebVRAM Administrator is responsible for creating new Business Units and creating accounts for Business Unit Administrators.

2. WebVRAM Business Unit Administrator: The WebVRAM Business Unit Administrator is responsible for creating new accounts for users within their respective Business Unit and for disabling accounts when a user leaves their Business Unit.

3. Regular User: Regular Users utilize WebVRAM to connect to remote VistA sites.

**8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?**

*If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

Contractors will have access to the WebVRAM system. Contractors act in the roles of application system maintenance and testing of the application prior to deployment of the software to the VA enterprise for use. Contracts are reviewed annually to validate permission to continue working on the project, according to the contract periods of performance, by the WebVRAM Contracting Officer at a minimum. Each contractor working on the system and WebVRAM project is required to also to submit a Non-Disclosure Agreement (NDA) to the VA Contracting Officer Representative (COR) before being allowed to work on the project and its associated systems. Only the WebVRAM developers and senior analysts will have access to PII stored in the WebVRAM User table (VA Network ID) and may access employee/contractor PII if required to troubleshoot production defects or issues in order to affect repairs to the production system. WebVRAM developers and senior analysts will obtain an elevated privilege account thru the MyVA ePAS (electronic Permission Access System) to have access to the SQL database. Once the system is in the sustainment phase of its lifecycle, only approved, designated staff of system administrators will have access to employee PII for the same need to troubleshoot and repair production defects/issues.

**8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?**

*VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.*

Employees and contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA's Talent Management System (TMS). All contractors are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI) clearance before application access is granted. Initial and annual VA Privacy and Information Security and Rules of Behavior training includes security best practices, threat recognition, privacy, compliance and policy requirements, and reporting obligations. Upon completion of training, personnel must complete a security and privacy quiz with a passing score. All required VA privacy training must be completed in TMS prior to the user being provided VA Network access, including access to work on the application for administration and testing purposes. Contractors providing System Administration services (maintaining the cloud environments, virtual machines, and databases) must complete the TMS VA IT System Administrator training module with a passing score.

**8.4 Has Authorization and Accreditation (A&A) been completed for the system?**

*8.4a If Yes, provide:*

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 4/27/2023
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 12/10/2020
5. *The Authorization Termination Date:* 12/10/2023
6. *The Risk Review Completion Date:* 1/12/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

*Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.*

*8.4b If No or In Process, provide your* ***Initial Operating Capability (IOC) date.***

Web VistA Remote Access Management (WebVRAM) system obtained a three-year Authority To Operate (ATO) on 12/10/2020 with an expiration of 12/10/2023. The latest, current SSP (System Security Plan) was signed on 6/2/2022. The latest Risk Review completion date was on 1/12/2022 during the Annual Assessment. The FIPS 199 Classification is Moderate/Moderate/Moderate with an overall security impact of Moderate.

## Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

**9.1 Does the system use cloud technology? If so, what cloud model is being utilized?**

*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.*

***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1****. (Refer to question 3.3.1 of the PTA)*

The Web VistA Remote Access Management (WebVRAM) system is hosted in the VA Enterprise Cloud (VAEC) Microsoft AZURE Government (MAG) High environment as an IaaS (Infrastructure as a Service).

**9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract).** (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

WebVRAM is within VAEC, and no further information required per question 9.1

**9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?**

*Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.*

*This question is related to privacy control DI-1, Data Quality.*

WebVRAM is within VAEC, and no further information required per question 9.1

**9.4 NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?**

*What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

WebVRAM is within VAEC, and no further information required per question 9.1

**9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.**

*Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as “Bots” or Artificial Intelligence (AI).*

One Business Unit Administration, CPAC utilizes RPA for updating service-connected (SC) reports and changes within the remote VistA sites. A 50-100 SC Recon Report is a high volume of claims needing to be cancelled due to patient's level of Service Connection changing, thereby requiring the charge to change. The volume is split between Priority 1 and Priority 2 charges. A bot will be designed to run through the Priority 1 charges then the Priority 2 charges needing to be cancelled at each site. The Priority 1 charges will be the new incoming claims coming in on a monthly basis with a status of ‘Open’, ‘Active’, or ‘On Hold’ and the rest will be considered Priority 2 charges. The future state solution will perform the process for all 129 VistA sites one after the other. The initial Priority 2 reports will be accessed and manually downloaded for each site. The bot will then refer to those reports to identify the charges that need to be cancelled. The Priority 1 solution will include automated steps for downloading and formatting the report for each site. Each site will be considered as one instance of the process, but since there exist discrepancies among sites, the solution will have dynamic steps and behave accordingly based on the current instance (site name).

## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

| ID | Privacy Controls |
|---|---|
| **AP** | **Authority and Purpose** |
| AP-1 | Authority to Collect |
| AP-2 | Purpose Specification |
| **AR** | **Accountability, Audit, and Risk Management** |
| AR-1 | Governance and Privacy Program |
| AR-2 | Privacy Impact and Risk Assessment |
| AR-3 | Privacy Requirements for Contractors and Service Providers |
| AR-4 | Privacy Monitoring and Auditing |
| AR-5 | Privacy Awareness and Training |
| AR-7 | Privacy-Enhanced System Design and Development |
| AR-8 | Accounting of Disclosures |
| **DI** | **Data Quality and Integrity** |
| DI-1 | Data Quality |
| DI-2 | Data Integrity and Data Integrity Board |
| **DM** | **Data Minimization and Retention** |
| DM-1 | Minimization of Personally Identifiable Information |
| DM-2 | Data Retention and Disposal |
| DM-3 | Minimization of PII Used in Testing, Training, and Research |
| **IP** | **Individual Participation and Redress** |
| IP-1 | Consent |
| IP-2 | Individual Access |
| IP-3 | Redress |
| IP-4 | Complaint Management |
| **SE** | **Security** |
| SE-1 | Inventory of Personally Identifiable Information |
| SE-2 | Privacy Incident Response |
| **TR** | **Transparency** |
| TR-1 | Privacy Notice |
| TR-2 | System of Records Notices and Privacy Act Statements |
| TR-3 | Dissemination of Privacy Program Information |
| **UL** | **Use Limitation** |
| UL-1 | Internal Use |
| UL-2 | Information Sharing with Third Parties |

**Signature of Responsible Officials**

**The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.**

Lynn A Olkowski Digitally signed by Lynn A Olkowski
Date: 2023.07.12 09:00:07 -05'00'

**Privacy Officer, Lynn A Olkowski**

Brian D. Orange 452379 Digitally signed by Brian D. Orange 452379
Date: 2023.07.12 09:25:37 -05'00'

**Information Systems Security Officer, Brian Orange**

LAURA YOUNG Digitally signed by LAURA YOUNG
Date: 2023.07.12 10:34:44 -05'00'

**Information System Owner, Laura Young**

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

WebVRAM utilizes the SORN of 79VA10/85FR84114, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.
VHA Handbook 1605.4 Notice of Privacy Practices, October 7, 2015
(https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147 )

## HELPFUL LINKS:

**Record Control Schedules:**

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

**General Records Schedule 1.1: Financial Management and Reporting Records (FSC):**

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

**National Archives (Federal Records Management):**

https://www.archives.gov/records-mgmt/grs

**VHA Publications:**

https://www.va.gov/vhapublications/publications.cfm?Pub=2

**VA Privacy Service Privacy Hub:**

https://dvagov.sharepoint.com/sites/OITPrivacyHub

**Notice of Privacy Practice (NOPP):**

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices