Privacy Impact Assessment for the VA IT System called:

REMOTE ACCESS PORTAL (RAP)
SOLUTIONS DELIVERY
VA CENTRAL OFFICE (VACO)

Date PIA submitted for review:
7/5/2022

System Contacts:

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Julie Drake</td>
<td><a href="mailto:Julie.drake@va.gov">Julie.drake@va.gov</a></td>
<td>202-632-8431</td>
</tr>
<tr>
<td>Information System</td>
<td>Derek Sterns</td>
<td><a href="mailto:Derek.sterns@va.gov">Derek.sterns@va.gov</a></td>
<td>804-585-6015</td>
</tr>
<tr>
<td>Security Officer (ISSO)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information System</td>
<td>John Gardner</td>
<td><a href="mailto:John.gardner@va.gov">John.gardner@va.gov</a></td>
<td>304-262-5076</td>
</tr>
<tr>
<td>Owner</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Abstract**

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

The Remote Access Portal (RAP) supports all aspects of client (user) remote access. There are seven portals (modules) within RAP:

1) ISO Portal / Application Module - where ISOs audit the remote access process for users assigned to facilities within their management purview.

2) DAC Portal / Application Module - allows RAP users with the DAC role to manage RAP approving officials for facilities within their management purview (user information visible includes names and email addresses of VA supervisors and CORs)

3) Approving Official Portal / Application Module - where remote access requests are approved or denied and user settings are managed for users who fall within the management purview of the approving officials (user information visible includes all data elements identified in 3.5)

4) RAP Portal / Application Module – this is the RAP home page which provides general information about the overall RAP application

5) OBLO Portal / Application Module – where onboarding/offboarding liaisons assist RAP approving officials with remote access administrative tasks for users within their administrative purview.

6) Self Service Portal / Application Module - where users request remote access, view remote access settings currently enabled, facilitate facility and/or supervisor/COR changes, ability to (optionally) upload training certificate documents (if requested by their supervisor/COR), etc. - all remote access users have access to the RAP Self Service Portal.

7) Portal Support / Application Module - where Enterprise Service Desk and IT Support personnel have access to remote access user information and features to assist users. Additionally, there is an Online Help / Application Module where users can access FAQs detailing how to perform various RAP functions. The Online Help module does not include any user information.

**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:

- **The IT system name and the name of the program office that owns the IT system.**
- **The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.**
- **Indicate the ownership or control of the IT system or project.**
- **The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.**
- **A general description of the information in the IT system and the purpose for collecting this information.**
- **Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.**
• 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.
• A citation of the legal authority to operate the IT system.
• Whether the completion of this PIA will result in circumstances that require changes to business processes
• Whether the completion of this PIA could potentially result in technology changes
• 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?

Formerly, ISO VPN Portal, the Remote Access Portal (RAP) is owned and managed by Solution Delivery, Security Engineering.

RAP encompasses all aspects of client (user) remote access for the VA Enterprise, supporting VA business processes and enforcing security controls as dictated by VA and federal policies (primarily NIST SP 800-53).

The RAP database includes information on approximately 290,000 individuals. These individuals include remote access users, approving officials (supervisors, CORs and area managers) and ISSOs. The information collection began in April 2018, when RAP was first released. Information for users who held the above roles at the time of release was obtained from the legacy ISO VPN Portal, which RAP replaced.

Most of the information collected in RAP comes from either the Identify and Access Management (IAM) team or Active Directory. The only required information provided by users is a justification for their remote access request; users may optionally provide a personal phone number and/or a personal email address. The justification is used by RAP approving officials to assist them in making the decision whether to approve the request or not. The optional personal phone number and email may be used by Enterprise Service Desk and IT Support personnel when assisting users. Additionally, if a secondary email address is identified, the RAP email notifications are sent to that email address in addition to the user’s VA email address. A secondary email is especially important for 100% remote users who, when onboarded, do not yet have access to VA email. The RAP system sends them information when their access is approved, provides details on how to connect, and how to obtain additional assistance, if needed.

There are currently seven portals: 1) ISO Portal / Application Module -where ISOs audit the remote access process for users assigned to facilities within their purview, 2) DAC Portal / Application Module - allows management of RAP approving officials for facilities within the DAC’s management purview (User information visible includes requester name, source of request (which RAP Portal), names and email addresses of VA supervisors and CORs, as well as their affiliated VA facility and company (if contractor)); 3) Approving Official Portal / Application Module - where remote access requests are approved or denied and user settings are managed for users who fall within the management purview of the approving officials (user information visible includes all data elements
identified in PTA 3.5); 4) RAP Portal/Application Module – this is the RAP home page which provides general information about the overall RAP application (no user information is on this Portal); 5) OBLO Portal / Application Module – where onboarding/offboarding liaisons assist RAP approving officials with remote access administrative tasks for users within their administrative purview (user information visible includes all data elements identified in PTA 3.5); 6) Self Service Portal / Application Module - where users request remote access, view remote access settings currently enabled, facilitate facility and/or supervisor/COR changes, ability to (optionally) upload training certificate documents (if requested by their supervisor/COR), etc. (user information visible includes data elements identified as ‘from Active Directory’ and ‘from the User’ identified in PTA 3.5 - all remote access users have access to the RAP Self Service Portal; and 7)Portal Support / Application Module - where Enterprise Service Desk and IT Support personnel have access to remote access user information and features to assist users (user information visible includes all data elements identified in PTA 3.5); Additionally, there is an Online Help / Application Module where users can access FAQs detailing how to perform various RAP functions. The Online Help module does not include any user information.

The legal authorities to operate the system include: Homeland Security Presidential Directive 12; Federal Information Processing Standard 201-3; National Institute of Standards and Technology (NIS) Special Publication 800-53; M-19-26 Update to the Trusted Internet Connection (TIC) Initiative

The completion of this PIA will not require business process changes, nor will it result in technology changes.

There are no system modifications in process that would affect the existing SORN.

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 Account Information

- Health Insurance Beneficiary Numbers
- Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Gender

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>

User’s VA Active Directory Domain
User’s VA Email
User’s Primary VA Phone
User’s VA Active Directory NTUserID
User’s VA Active Directory Distinguished Name
User’s VA Active Directory User Principal Name (UPN)
User’s VA Active Directory Office Code (optional)
User’s VA Active Directory Globally Unique Identifier (GUID) (not visible within application)
User’s VA Active Directory User Identifier (UID) (not visible within application)
User’s VA Active Directory SECID (not visible within application)
User’s Remote Access Justification
Date User’s Remote Access Profile was Created
User’s Remote Access Types Enabled
User’s Remote Access Settings
User’s 2FA Exemption Information
User’s VA Facility Affiliation
User’s Company Affiliation (if contractor)
User’s Supervisor/COR
User’s Account Expiration Date (if applicable)
VAVO User Name
VAVO Class
VAVO Provisioning Email
VAVO IP Phone
PII Mapping of Components

Remote Access Portal (RAP) consists of two key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Remote Access Portal (RAP) and the reasons for the collection of the PII are in the table below.

### PII Mapped to Components

*PII Mapped to Components*

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAMP database</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Phone number, VA Email, Secondary Email, Secondary phone number, and Active</td>
<td>To enable initiation, authorization, auditing, and support of client remote access.</td>
<td>Database is compliant with SQL19 Baseline, including TDE encryption. Connections use TLS and application</td>
</tr>
<tr>
<td>ADAM database</td>
<td>Yes</td>
<td>Yes</td>
<td>Active Directory Domain, NTUserID, UPN and VA email address</td>
<td>Information collected to accurately identify the correct user to apply the PIV exemption</td>
<td>Database is compliant with SQL19 Baseline, including TDE encryption. Database connection uses TLS</td>
</tr>
<tr>
<td>----------------</td>
<td>-----</td>
<td>-----</td>
<td>------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>

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

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?

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 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Active Directory – Authoritative source for user information and account information which is required to authorize, manage, audit, and support remote access

Identity and Access Management (IAM) – VA’s authoritative onboard solution. Required to meet the VA requirement to utilize IAM for onboarding.

Active Directory Access Management (ADAM) – This is a tool used by the Enterprise Service Desk to facilitate actions in Active Directory. ADAM includes a RAP integration that allows the ESD to send PIV exemption information to RAP when network PIV exemptions are granted.

SPLUNK – SPLUNK is used to retrieve user connection data via reporting in RAP. Data is transferred via Hypertext Transfer Protocol Secure (HTTPS), utilizing a single domain SSL certificate that cryptographically establishes an encrypted link the web server and a browser. This link ensures that all data passed between the web server and the browser remain private and encrypted. The RAP Server safeguards against unencrypted sessions by forcing clients to send
requests over https by sending a HTTPS response header "Strict-Transport-Security" in the event attempts are made to establish a connection over HTTPS.

Individual – Individuals identify their VA facility, supervisor/COR, and justification for authorization. Optionally, users may provide a personal email and/or phone number, which are used for communications and support.

1.3 How is the information collected?

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?

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.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is collected from the below sources

Active Directory - For AD communication, RAP utilizes “Principal Context” with Secure Socket Layer as part of the constructor’s Context Option. Each “User Principal” and “Group Principal” context is then established within the construct of the “Principal Context”, thus ensuring all the communication between the client and AD is private and encrypted.

Identify and Access Management – RAP API transfers data via Hypertext Transfer Protocol (HTTP), utilizing a single domain SSL certificate that cryptographically establishes an encrypted link the web server and a browser. This link ensures that all data passed between the web server and the browser remain private and encrypted. The RAP Server safeguards against unencrypted sessions by forcing clients to send requests over https by sending a HTTP response header "Strict-Transport-Security" in the event attempts are made to establish a connection over HTTP.

Active Directory Account Management (ADAM) – The ADAM application communicates with an ADAM database, which is a separate database within the same SQL instances as the RAMP database. ADAM transfers data via Hypertext Transfer Protocol (HTTP), utilizing a single domain SSL certificate that cryptographically establishes an encrypted link the web server and a browser. This link ensures that all data passed between the web server and the browser remain private and encrypted. The RAP Server safeguards against unencrypted sessions by forcing clients to send requests over https by sending a HTTP response header "Strict-Transport-Security" in the event attempts are made to establish a connection over HTTP. The ADAM database updates the RAMP database within the same SQL instance – no data is transmitted outside of the database.

SPLUNK – Data is transferred via Hypertext Transfer Protocol (HTTP), utilizing a single domain SSL certificate that cryptographically establishes an encrypted link the web server and a browser. This link ensures that all data passed between the web server and the browser remain private and encrypted. The RAP Server safeguards against unencrypted sessions by forcing clients to send
requests over https by sending a HTTP response header "Strict-Transport-Security" in the event attempts are made to establish a connection over HTTP.

Individuals - RAP is accessed via a web browser and utilizes a single domain SSL certificate that cryptographically establishes an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and the browser remain private and encrypted. The RAP Server safeguards against unencrypted sessions by forcing clients to send requests over https by sending a HTTP response header "Strict-Transport-Security" in the event attempts are made to establish a connection over HTTP. Data passed between the RAP web frontend servers and the RAP database are encrypted via TLS.

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

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.

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.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Each time a user visits the RAP Self Service Portal, RAP utilizes the Active Directory GUID to validate the user’s domain and NTUserID; if incorrect, it is automatically updated. Users have the ability to update their own information in RAP via the Self Service Portal. Additionally, ISSOs and supervisors/CORs can update user information, as needed. IAM updates user information based on their sources (IE HR Smart, ECMS and MPI).

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.

Homeland Security Presidential Directive 12; Federal Information Processing Standard 201-3; National Institute of Standards and Technology (NIST) Special Publication 800-53; M-19-26 Update to the Trusted Internet Connection (TIC) Initiative, The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the
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.

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:** Ability to view other user’s name, active directory account information, secondary phone number and secondary email address. RAP enforces role-based access. General users can only see their own information.

**Mitigation:** RAP roles enforce separation of duties and least privilege. Users may choose not to provide their secondary email address and/or phone number.

### 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.*

<table>
<thead>
<tr>
<th>Information</th>
<th>Internal VA Use</th>
<th>External Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identify VA user</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Field</td>
<td>Authentication Method</td>
<td>Used/Shared</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Active Directory Domain</td>
<td>Logical authentication</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VA Email</td>
<td>Send system emails to user</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Secondary Email</td>
<td>Send system emails to user</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Primary VA Phone</td>
<td>Contact user</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Secondary Phone</td>
<td>Contact user</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Active Directory NTUserID</td>
<td>Logical authentication</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Active Directory Distinguished Name</td>
<td>Allows mapping of user to VA facility</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Active Directory User Principal Name (UPN)</td>
<td>Logical authentication</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Active Directory Office Code (optional)</td>
<td>Identify user's work unit</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Active Directory Globally Unique Identifier (GUID) (not visible within application)</td>
<td>Uniquely identify user’s Active Directory record</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Active Directory User Identifier (UID) (not visible within application)</td>
<td>Uniquely identify user’s Active Directory record</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Active Directory SECID (not visible within application)</td>
<td>Uniquely identify user’s Active Directory record</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Remote Access Justification</td>
<td>Justify approval of remote access</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Date Remote Access Profile was Created</td>
<td>Audit requirement</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Remote Access Types Enabled</td>
<td>Logical authentication</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Remote Access Settings</td>
<td>Logical authentication</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>2FA Exemption Information</td>
<td>Logical authentication</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VA Facility Affiliation</td>
<td>Identify user’s physical location</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>Company Affiliation (if contractor)</td>
<td>Identify contractor’s company</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>User’s Supervisor/COR</td>
<td>Required to create approval workflow</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>User’s Account Expiration Date (if applicable)</td>
<td>Disables access on identified date</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VAVO User Name</td>
<td>Identity assigned to VAVO router</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VAVO Class</td>
<td>Combination of VAVO router model and preferred gateway</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VAVO Provisioning Email</td>
<td>Email address identified to push configuration information to</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VAVO IP Phone</td>
<td>Identifies if user has an IP Phone</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VAVO UC Primary IP</td>
<td>Identifies IP phone IP addresses to allow VAVO device to communicate with</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VAVO UC Secondary IP</td>
<td>Identifies IP phone IP addresses to allow VAVO device to communicate with</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VAVO Video DX80</td>
<td>Identifies if user has a video device</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VAVO Display Name</td>
<td>Unique username assigned to VAVO device</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VAVO Status</td>
<td>Identifies if VAVO is enabled or disabled</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VAVO ISP Speed</td>
<td>VAVO user’s ISP speed</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VAVO Request Justification</td>
<td>User’s justification to supervisor to approve VAVO</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>VAVO DV Primary IP</td>
<td>Identifies video IP addresses to allow VAVO device to communicate with</td>
<td>Not used/shared</td>
</tr>
<tr>
<td><strong>VAVO DV Secondary IP</strong></td>
<td>Identifies video IP addresses to allow VAVO device to communicate with</td>
<td>Not used/shared</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>VAVO Serial Number</strong></td>
<td>Serial number of user’s VAVO router</td>
<td>Not used/shared</td>
</tr>
<tr>
<td><strong>Approval Workflow initiations/status changes</strong></td>
<td>Status of remote access request workflow</td>
<td>Not used/shared</td>
</tr>
<tr>
<td><strong>Request Approvals/Denials</strong></td>
<td>Audit of approval or denial of remote access request</td>
<td>Not used/shared</td>
</tr>
<tr>
<td><strong>User Review Flows and Approvals/Denials</strong></td>
<td>Audit of User Review initiations, actions and completion</td>
<td>Not used/shared</td>
</tr>
<tr>
<td><strong>Transfers to Other Companies/Facilities/Supervisors/CORs (if applicable)</strong></td>
<td>Audit to show changes in companies, facilities, and supervisors/CORs</td>
<td>Not used/shared</td>
</tr>
<tr>
<td><strong>Conversion to Employee/Contractor (if applicable)</strong></td>
<td>Audit to show change in user type from employee to contractor and vice versa</td>
<td>Not used/shared</td>
</tr>
<tr>
<td><strong>Remote Access Types Enabled/Disabled</strong></td>
<td>Status of each remote access method</td>
<td>Not used/shared</td>
</tr>
<tr>
<td><strong>Account Deletion (if applicable)</strong></td>
<td>Audit of account deletion</td>
<td>Not used/shared</td>
</tr>
<tr>
<td><strong>ESD Actions Related to User (if applicable)</strong></td>
<td>Audit of ESD actions (IE PIV exemption, re-enable account, delete account)</td>
<td>Not used/shared</td>
</tr>
</tbody>
</table>

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

RAP updates information in the existing record. Most updates are reflected in the user’s audit trail, showing the old value and new value.

Example: Existing remote access user transfers from supervisor to another. Updates in RAP include:
• Old supervisor is replaced with new supervisor; user’s RAP audit trail annotates old supervisor/new supervisor. This action can be initiated by the user or their old/new supervisor and requires approval before the record is updated.

2.3 How is the information in the system secured?

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

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

N/A SSNs are not collected

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

Data at Rest: The RAP database is SQL19 and adheres to the VA SQL 19 Baseline. Transparent Data Encryption (TDE) encrypts the database files and database backups (data at rest).

Data in Transit: For data transmissions between the RAP application and the database, the ‘Force Encryption’ setting, which encrypts data in transit, is set to 'Yes'. In addition, FIPS is enabled on the SQL VMs and TLS 1.2 is enabled.

Data in Transit: Data transfers between the RAP application and user are sent via Hypertext Transfer Protocol (HTTP), utilizing a single domain SSL certificate that cryptographically establishes an encrypted link the web server and a browser. This link ensures that all data passed between the web server and the browser remain private and encrypted. The RAP Server safeguards against unencrypted sessions by forcing clients to send requests over https by sending a HTTP response header "Strict-Transport-Security" in the event attempts are made to establish a connection over HTTP.

The RAP database is SQL19 and adheres to the VA baseline. Transparent Data Encryption (TDE) encrypts the database files and database backups (data at rest). Force Encryption, which encrypts data in transit, is set to 'Yes'. In addition, FIPS is enabled on the SQL VMs and TLS 1.2 is enabled.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

There is a RAP Access Control Policy, which was created/maintained as part of the prior minor application eMASS process.

ISO Portal – The ISSO role is managed by the ISSO hierarchical chain of command. DISDs manage ISSMs and ISSMs manage ISSOs. DISDs (there are only six individuals in this role) are managed by RAP personnel via ServiceNow tickets. All ISSO roles are restricted to specific facilities which are also managed by DISDs and ISSMs.

DAC Portal – DAC is short for Designated Approver Capability. DACs are generally ISSOs, however, ISSOs may assign the role to other individuals, as appropriate for their facilities. The DAC role manages RAP supervisors, CORs and Area Managers for facilities under the DAC’s purview (as dictated by the ISSO role).

Approving Official Portal – Supervisors, CORs and Area managers have the role of Approving Official in RAP. DACs manage the Approving Official role.

Portal Support – Portal Support access is governed by membership in AD security groups for ESD personnel and IT support personnel. Access is granted via ServiceNow request tickets.

Self Service Portal – any user with a valid VA AD credential has access to the RAP Self Service Portal. This is where they can request remote access, see the type(s) of access they have enabled, update their information, etc.

OBLO Portal – OBLO stands for Onboarding/Offboarding Liaison Official. OBLOs are usually contract staff who assist CORs with the administrative side of remote access; however, OBLOs can also be VA employees. The OBLO role is managed by Approving Officials (supervisors and CORs) and is restricted based on the user’s company.

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

Name
User’s VA Active Directory Domain
User’s VA Email
User’s Secondary Email
User’s Primary VA Phone
User’s Secondary Phone
User’s VA Active Directory NTUserID
User’s VA Active Directory Distinguished Name
User’s VA Active Directory User Principal Name (UPN)
User’s VA Active Directory Office Code (optional)
User’s VA Active Directory Globally Unique Identifier (GUID) (not visible within application)
User’s VA Active Directory User Identifier (UID) (not visible within application)
User’s VA Active Directory SECID (not visible within application)
User’s Remote Access Justification
Date User’s Remote Access Profile was Created
User’s Remote Access Types Enabled
User’s Remote Access Settings
User’s 2FA Exemption Information
User’s VA Facility Affiliation
User’s Company Affiliation (if contractor)
User’s Supervisor/COR
User’s Account Expiration Date (if applicable)
VAVO User Name
VAVO Class
VAVO Provisioning Email
VAVO IP Phone
VAVO UC Primary IP
VAVO UC Secondary IP
VAVO Video DX80
VAVO Display Name
VAVO Status
VAVO ISP Speed
VAVO Request Justification
VAVO DV Primary IP
VAVO DV Secondary IP
VAVO Serial Number
User’s Approval Workflow initiations/status changes
User’s Request Approvals/Denials
User’s User Review Flows and Approvals/Denials
User’s Transfers to Other Companies/Facilities/Supervisors/CORs (if applicable)
User’s Conversion to Employee/Contractor (if applicable)
User’s Remote Access Types Enabled/Disabled
User’s Account Deletion (if applicable)
ESD Actions Related to User (if applicable)
### 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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

This question is related to privacy control DM-2, Data Retention and Disposal.

Records are retained until the business use ceases.

### 3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

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.


### 3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

All records are electronic. To date, none have been destroyed or eliminated. There are no paper records. Electronic records would be eliminated by deleting the data from the databases.

### 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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

Data is used in test environments - test environments have the same security controls as production. The RAP test database is SQL19 and adheres to the VA SQL19 Baseline. Transparent Data Encryption (TDE) encrypts the database files and database backups (data at rest). The 'Force Encryption' setting, which encrypts data in transit, is set to 'Yes'. In addition, FIPS is enabled on the SQL VMs and TLS 1.2 is enabled.

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.

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:** Ability to view user’s name, active directory account information, personal phone number and personal email address after account becomes inactive.

**Mitigation:** Accounts become inactive in RAP a variety of ways: 1) via an offboard request from the Identify and Access Management API - IAM integration with HRSmart provides data feed for offboard of VA employees and eCMS data feeds information for offboard of contractors; 2) Supervisors and/or CORs can deactivate accounts directly in RAP; 3) ISSOs can deactivate accounts directly in RAP; 4) Users can deactivate their own accounts; and 5) YourIT ticket can initiate an offboard request to IAM and/or directly to the RAP team. All deactivations are tracked in the system and displayed in an audit trail which shows the date, time, and source of the deactivation. Inactive records are stored in the same database as active records and have the same security and privacy controls in place. Per the RCS, electronic records will be eliminated when no longer needed.
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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Purpose 1) User information and account information are received from AD; Purpose 2) User NTUserIDs are written to AD security group(s) from RAP which are used for authorization/access control (only applies)</td>
<td>Purpose 1 data elements: Primary Phone, First Name, Middle Initial, Last Name, Mail Code, VA Domain, NTUserID, UPN, Distinguished Name, VA Email, GUID, VA UID, SECID</td>
<td>Purpose 1 and Purpose 2: For AD communication, RAP utilizes “Principal Context” with Secure Socket Layer as part of the constructor’s Context Option. Each “User Principal” and “Group Principal”</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>to CAG Print, CAG Copy/Past and AVD access).</td>
<td>Primary Phone, First Name Middle Initial, Last Name Mail Code, VA Domain, NTUserID, UPN, Distinguished Name, VA Email, Secondary Email, GUID, VA UID, SECID, Computer Type, Distinguished name, Company Affiliation, Order Number, Supervisor/COR Affiliation, Account Expiration Date</td>
<td>RAP API transfers data via Hypertext Transfer Protocol (HTTP), utilizing a single domain SSL certificate that cryptographically establishes an encrypted link the web server and a browser. This link ensures that all data passed between the web server and the browser remain private and encrypted. The RAP Server safeguards against unencrypted sessions by forcing clients to send requests over https by sending a HTTP response header &quot;Strict-Transport-Security&quot; in the event attempts are made to establish a context is then established within the construct of the “Principal Context”, thus ensuring all the communication between the client and AD is private and encrypted.</td>
<td></td>
</tr>
<tr>
<td><strong>List the Program Office or IT System information is shared/received with</strong></td>
<td><strong>List the purpose of the information being shared/received with the specified program office or IT system</strong></td>
<td><strong>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</strong></td>
<td><strong>Describe the method of transmittal</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>ADAM</td>
<td>Purpose 1) User PIV exemption information received from ADAM; Purpose 2) ADAM database sends user PIV exemption information to RAMP database (databases within same SQL instance)</td>
<td>Purpose 1 and 2: Domain, NTUserID, UPN, VA Email, Exemption Justification</td>
<td>Purpose 1: ADAM transfers data via Hypertext Transfer Protocol (HTTP), utilizing a single domain SSL certificate that cryptographically establishes an encrypted link the web server and a browser. This link ensures that all data passed between the web server and the browser remain private and encrypted. The RAP Server safeguards against unencrypted sessions by forcing clients to send requests over https by sending a HTTP response header &quot;Strict-Transport-Security&quot; in the event attempts are made to establish a connection over HTTP. Purpose 2: The ADAM database updates the RAMP database within the same SQL instance – no data is transmitted outside</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>LDAP</td>
<td>User remote access account attributes sent to LDAP for authorization/access control</td>
<td>Domain, NTUserID, UPN, Access types enabled, Access settings, 2FA Exemptions</td>
<td>For LDAP communication, RAP utilizes port 636 as part of the LDAP Directory Identifier Constructor when establishing a connection through Directory Services context. LDAP port 636 is TLS Encrypted, thus ensuring all the communication between the RAP and LDAP is encrypted.</td>
</tr>
<tr>
<td>SPLUNK</td>
<td>User historical connection information received from SPLUNK presented to user via reporting (audit requirement – data is not stored in RAMP)</td>
<td>Domain, NTUserID, UPN, Date connected, Access method, VA IP address, User IP address, Bytes Sent/Received</td>
<td>SPLUNK transfers data via Hypertext Transfer Protocol (HTTP) over port 8089, utilizing a single domain SSL certificate that cryptographically establishes an encrypted link the web server and a browser. This link ensures that all data passed between the web server and the browser remain private and encrypted. The RAP Server safeguards against unencrypted</td>
</tr>
<tr>
<td><strong>List the Program Office or IT System information is shared/received with</strong></td>
<td><strong>List the purpose of the information being shared/received with the specified program office or IT system</strong></td>
<td><strong>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</strong></td>
<td><strong>Describe the method of transmittal</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>MEVO</td>
<td>User remote access account attributes sent to MEVO for authorization/access control/device configuration</td>
<td>VAVO User Name, VAVO Class, VAVO Provisioning Email, VAVO IP Phone, VAVO UC Primary IP, VAVO UC Secondary IP, VAVO Video DX80, VAVO Display Name, VAVO Status, VAVO ISP Speed, VAVO Request Justification, VAVO DV Primary IP, VAVO DV Secondary IP, VAVO Serial Number</td>
<td>RAP transfers data to MEVO API via Hypertext Transfer Protocol (HTTP), utilizing a single domain SSL certificate that cryptographically establishes an encrypted link the web server and a browser. This link ensures that all data passed between the web server and the browser remain private and encrypted. The RAP Server safeguards against unencrypted sessions by forcing clients to send requests over https by sending a HTTP response header &quot;Strict-Transport-Security&quot; in the event attempts are made to establish a connection over HTTP.</td>
</tr>
</tbody>
</table>
**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. This question is related to privacy control UL-1, Internal Use.

Follow the format below:

**Privacy Risk:** Information disclosed to unauthorized individuals/systems.

**Mitigation:** RAP roles ensure information is viewed only by those with a need to know. Information shared with other systems is based on business need and includes security and privacy controls.

**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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared/received/transmitted with the specified program office or IT system</th>
<th>List the specific PHI/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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:

**Privacy Risk:** N/A

**Mitigation:** N/A
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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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.

This question is 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.

Users and/or their supervisors/COR initiate remote access requests, which starts the data collection process. No privacy notice is given. Users (users and/or their supervisors/CORs) do see a summary of information collected from the user when visiting the RAP web site. SORN: Department of Veterans Affairs Identity Management System (VAIDMS)-VA. 146VA005Q3 https://www.oprm.va.gov/docs/Current_SORN_List_2_25_2022.pdf

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.

Users have the option to decline providing a personal email and/or personal phone number without incurring a penalty. Other information, with exception of justification for remote access, is received from other sources (IE Active Directory, Identity and Access Management).

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.
No consent is provided.

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.

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:** System users don’t know there is a PIA or SORN.

**Mitigation:** A statement is provided upon logon to the system (reference Appendix A). Add link to SORN to the existing notice.

**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?

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.

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).

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.

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.
SORN NOTIFICATION PROCEDURES: An individual can determine if this system contains a record pertaining to him/her by sending a signed written request to the Systems Manager. When requesting notification of or access to records covered by this Notice, an individual should provide his/her full name, date of birth, agency name, and work location. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to access, such as a government-issued photo ID. Individuals requesting notification via mail or telephone must furnish, at minimum, name, date of birth, social security number, and home address in order to establish identity. RECORD ACCESS PROCEDURE: Same as notification procedures.

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.

CONTESTING RECORD PROCEDURE: Same as Notification procedures above. Requesters should also reasonably identify the record, specify the information they are contesting, state the corrective action sought and the reasons for the correction along with supporting justification showing why the record is not accurate, timely, relevant, or complete.

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.

SORN CONTESTING RECORD PROCEDURE: Same as notification procedures. Requesters should also reasonably identify the record, specify the information they are contesting, state the corrective action sought and the reasons for the correction along with supporting justification showing why the record is not accurate, timely, relevant, or complete.

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. 
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. 
This helps ensure data accuracy.

RAP allows users to update information directly. If a user is unable to update information, a ServiceNOW ticket can be opened for the RAP team to update the information on their behalf.

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.

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: Incorrect information in the system would prevent the user from being able to access the VA network remotely.

Mitigation: Users have the ability to update: Name, VA email, secondary email, Primary VA Phone, Secondary Phone, Active Directory Office Code. Users contact their supervisor/COR to update information they do not have access to. The RAP Self Service Portal is accessible to all VA network users via the internal VA network at https://vaww.ramp.vansoc.va.gov.
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?

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

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Information System Security Officer (ISSO): RAP includes three ISSO roles: District Information Security Directors (DISDs), which includes management of all ISSM roles and ISSO roles within a District and audit capability of all remote access users within a district; Information System Security Managers (ISSMs) which includes management of all ISSO roles within a Territory and audit capability of all remote access users within a territory; and Information System Security Officers (ISSOs) which includes audit capability of all remote access users within a facility. The RAP ISO role allows ISOs to audit the remote access process and remote access users.

Remote Access Approving Officials: There are two remote access approving official roles: 1) supervisor/COR and 2) area manager. The RAP DAC role manages the Approving Official roles. Supervisors approve remote access requests for employees and CORs approve for contractors. Area Managers were second level approvers until March 13, 2020, at which time they were removed at the request of VA leadership. Approving Officials perform general remote access management via the RAP Approving Official Portal.

Designated Approver Capability (DAC): The DAC role is responsible for maintaining the remote access approving officials list. DACs are responsible for ensuring only authorized individuals are in the approving official role. ISSOs manage the DAC role.

Portal Support: The Portal Support portal within RAP is granted to users who perform IT Support functions. There are three roles, which provide different levels of functionality. Membership in various Active Directory (AD) security groups dictate access. The three roles include:

- Enterprise Service Desk
- IT Support Personnel
- VA NSOC
On-boarding/Off-boarding Liaison Official (OBLO): The OBLO role is an administrative role created to support CORs who manage large contracts. OBLOs can initiate new remote access requests on behalf of CORs and perform other administrative duties. They cannot perform remote access management functions such as approve access, disable access, etc. The OBLO role is managed by the COR and access is restricted based on users assigned to that COR, along with the user’s contract company.

Self Service Portal (SSP): The SSP is available to all VA enterprise (authenticated) users. The SSP is where users request remote access, complete a user review, update information, see access methods enabled, etc.

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.

Yes, contract staff have access to the system and PII due to their development role. Contract staff are tasked under the Network Engineering, Design, Implementation and Infrastructure Support (NEDIIS) contract which includes a Non-Disclosure Agreement (Appendix A of the contract)

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.

Contract and VA staff have taken the requisite TMS training: VA Security and Privacy Awareness Training (includes Rules of Behavior), Information Security and Privacy Role-Based Training for IT Specialist, Information Security Role-Based Training for System Administrators, and Training for Elevated Privileges for System Access. All staff are aware of the need to meet SP 800-53 controls. Additionally, the RAP application adheres to routine WASA and Fortify scans.
8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If yes, provide:

1. The Security Plan Status,
2. The Security Plan Status Date,
3. The Authorization Status,
4. The Authorization Date,
5. The Authorization Termination Date,
6. The Risk Review Completion Date,
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

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

RAP is a minor application within the NOC LAN Assessing. ATO was granted on 11/4/2020 and expires on 11/4/2023. The system impact categorization is 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).

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.

Cloud technology is not used – RAP is on-prem.

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.
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.

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.

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).

N/A – RPA is not utilized
Summary of Privacy Controls by Family

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

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

**JULIE C. DRAKE** Digitally signed by JULIE C. DRAKE 969177
Date: 2022.09.09 10:33:13 -06'00'

Privacy Officer, Julie Drake

**DEREK STERNS** Digitally signed by DEREK STERNS
Date: 2022.09.09 12:53:57 -04'00'

Information Systems Security Officer, Derek Sterns

**John I Gardner** Digitally signed by John I Gardner 105346
Date: 2022.09.12 11:23:24 -04'00'

Information Systems Owner, John Gardner
APPENDIX A-6.1

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).

Department of Veterans Affairs Identity Management System (VAIDMS) - VA. 146VA005Q3

Current System Notice

![Warning Message]

This site and all subdirectories and files within are restricted to authorized Department of Veterans Affairs Network Security Operations Center (NSOC) staff and/or authorized VA NSOC customers only. All use is monitored for authorized purposes, and any use constitutes consent to monitoring, storage and retrieval, disclosure, analysis, access restriction, investigation, or any other authorized actions. Any unauthorized access (or denial of access) to this system, all files, and all data therein is prohibited and is subject to criminal, civil, and administrative penalties under Federal Laws including, but not limited to, 18 U.S.C. §1030 (fraud and related activity in connection with computers) and 18 U.S.C. §2701 (unlawful access to stored communications). In addition, Federal Laws (18 USC 287 and 1001) provide for criminal penalties for knowingly submitting or making false, fictitious, or fraudulent statements or claims.