Privacy Impact Assessment for the VA IT System called:

REMOTE ACCESS PORTAL (RAP)

CONNECTIVITY AND COLLABORATION SERVICES

VA CENTRAL OFFICE (VACO)

eMASS ID # 2281

Date PIA submitted for review:

12/20/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.Drake@va.gov	202-632-8431
Information System Security Officer (ISSO)	Derek Sterns	Derek.Sterns@va.gov	727-201-7364
Information System Owner	Daniel Mesimer	Daniel.Mesimer@va.gov	816-701-3079

Abstract

The abstract provides the simplest explanation for "what does the system do?".

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

1) ISSO Portal / Application Module - where Information System Security Officers (ISSOs) audit the remote access process for users assigned to facilities within their management purview.

2) DAC Portal / Application Module - allows RAP users with the Designated Approver Capability (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 Contracting Officer Representatives (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) OBLO Portal / Application Module – the On Boarding / Off Boarding Liaison Official (OBLO) portal is where on boarding/off boarding liaisons assist RAP approving officials with remote access administrative tasks for users within their administrative purview.

5) Self Service Portal / Application Module - where users request remote access, view remote access settings currently enabled, facilitate RAP 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.

6) Portal Support / Application Module - where Enterprise ServiceDesk (ESD) and Information Technology (IT) Support personnel have access to remote access user information and features to assist users.

7) Online Help / Application Module - where users can access Frequently Asked Questions (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:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

The Remote Access Portal (RAP) is aligned within the Office of Information and Technology (OIT) Connectivity and Collaboration Services (CCS) Core Network Services (CNS) program office.

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

RAP includes modules to sustain all aspects of client (user) remote access including initiation of requests; approvals and denials; auditing; reporting; and IT support. The CCS mission is 'Connecting Everyone to Everything'; RAP supports this mission by providing the means for VA employees and contractors to be authorized to work remotely.

C. Who is the owner or control of the IT system or project?

RAP is owned and maintained by CCS CNS.

2. Information Collection and Sharing

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

The RAP database currently has information on approximately 327,000 active remote access users. The typical user is a VA employee or contractor who has a business need to connect remotely to the VA network. RAP also supports user roles for ISSOs who audit the remote access process; Approving Officials who approve/deny remote access requests; OBLOs who assist approving officials with access requests; and IT Support personnel who provide IT support to remote access users.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

Most of the information collected in RAP is Global Address List (GAL) data and VA account data and is received from either the Identify and Access Management (IAM) onboarding system or Active Directory (AD). The only required information provided by users (or supervisors/CORs who enter requests on behalf of users) is a justification for their remote access request; users may optionally provide a secondary phone number and/or a secondary email address. The justification provided is used by RAP approving officials to assist them in making the decision whether to approve the request or not. The optional secondary phone number and email may be used by ESD 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 users information when their access is approved, provides details on how to connect, and how to obtain additional assistance, if needed. The secondary emails and phone numbers (if populated) are removed completely from the database when a user's account status becomes 'deleted'.

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

RAP shares information with two systems: 1) The ESD Active Directory Account Management (ADAM) tool and 2) the Manage Express Virtual Office (MEVO) management system. The ADAM tool is used by ESD to, among other things, grant smart card exemptions. The integration with RAP allows ESD to grant the remote access smart card exemption at the same time the AD exemption is granted, which results in improved efficiency and improved customer service. The information shared with MEVO is information needed to appropriately provision VA Virtual Office (VAVO) routers.

G. *Is 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?*

RAP has application and database redundancy between the Capital Region Readiness Center (CRRC) located in Martinsburg, WV (primary) and the Hines Information Technology Center (ITC) located in Hines, IL (secondary). Replication between primary and secondary RAP Structured Query Language (SQL) instances is performed via Arcserve replication which replicates at the block level, keeping SQL data and transaction log files synchronized. SQL services on the secondary SQL instance are stopped during the replication process, and a comprehensive web front end allows administrators to monitor the replication process, and therefore, ensure both primary and secondary sites are synchronized at all times. Additionally, routine integrity checks are performed daily.

3. Legal Authority and SORN

H. *What is the citation of the legal authority to operate the IT system?*

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 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 Version Date: October 1, 2021Page 10 of 35system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317. The existing Privacy Act system of records notice that covers this system is: Department of Veterans Affairs Identity Management System (VAIDMS)-VA. 146VA005Q3.

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?*

N/A

4. System Changes

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

No

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

No

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. It must also match the information provided in question 3.4 of the PTA.

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[1]
- ☐ 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)

User's VA Email
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 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 Security Identifier (SECID) (not visible within application)

PII Mapping of Components (Servers/Database)

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

RAP consists of twenty-two (22) key components: Ten (10) web servers and one (1) database at each of the two (2) sites (Martinsburg, WV and Hines).
(servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by RAP 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 server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**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**
RAMP Database	Yes	Yes	Name, Phone number, VA Email, Secondary Email, Secondary phone number, and Active Directory account information	Data is needed to authorize remote access; to send remote access information to the user via email; to audit connectivity and produce reports; and to allow identification for troubleshooting purposes	Transparent Data Encryption (TDE) encrypts the database files and database backups (data at rest). Force Encryption is set to 'Yes'. In addition, FIPS is enabled on the SQL VMs and TLS 1.2 is enabled. Data transfers between the RAP application and user are sent via Transport Layer Security (TLS). 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.
ADAM Database	Yes	Yes	Active Directory NTUserID, User Principal Name (UPN), and VA email address	Information collected to accurately identify the correct user to apply the smart card exemption.	Transparent Data Encryption (TDE) encrypts the database files and database backups (data at rest). Force Encryption is set to 'Yes'. In addition, FIPS is enabled on the SQL VMs and TLS 1.2 is enabled. ADAM transfers data via TLS. The RAP Server safeguards against unencrypted sessions by forcing the client to send requests over TLS by sending a HTTP response header "Strict-Transport-Security" in the event attempts are made to establish a connection over HTTP.

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 Microsoft (MS) Active Directory (AD) Assessing (1001)
- Identity and Access Management (IAM)
- Active Directory Account Management (ADAM)
- OIT SPLUNK
- Individual Remote Access Users

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.

VA Microsoft (MS) Active Directory (AD) Assessing (1001) is the authoritative source for user information and account information which is required to authorize, manage, audit, and support remote access.

Identity and Access Management (IAM) is the VA's authoritative onboard solution. Use of the IAM Onboarding service is required by the VA.

Active Directory Account Management (ADAM) is a tool used by the ESD to facilitate actions in AD. ADAM includes a RAP integration that allows the ESD to send Personal Identity and Verification (PIV) exemption information to RAP when network PIV exemptions are granted.

OIT SPLUNK is the VA logging solution and is used to retrieve user connection data via a reporting interface in RAP. Data is transferred via TLS, 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.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

No

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?

VA Microsoft (MS) Active Directory (AD) Assessing (1001): For AD communication, RAP utilizes "Principal Context" with SSL 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.

Identity and Access Management (IAM): RAP API transfers data via TLS, 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 TLS, 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.

OIT SPLUNK: Data is transferred via TLS, 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.

Individual Remote Access Users: 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.

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

N/A

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.

Each time a user visits the RAP Self Service Portal, RAP utilizes the AD 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 authoritative sources (IE Human Resources (HR Smart), Electronic Contract Management System (ECMS) and Master Patient Index (MPI)).

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No

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 (NIS) 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 Version Date: October 1, 2021Page 10 of 35system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317. The existing Privacy Act system of records that covers this system is Department of Veterans Affairs Identity Management System (VAIDMS)-VA. 146VA005Q3.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

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

<u>Principle of Minimization:</u> Is the information directly relevant and necessary to accomplish the specific purposes of the program?

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

<u>Principle of Data Quality and Integrity:</u> 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, AD 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 that 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.

PII/PHI Data Element	Internal Use	External Use
Name	Identify VA user	Not used/shared
VA Email	Send system emails to user	Not used/shared
Secondary Email	Send system emails to user	Not used/shared
Secondary Phone	Contact user	Not used/shared
Active Directory NTUserID	Logical authentication	Not used/shared
Active Directory Distinguished Name	Allows mapping of user to VA facility	Not used/shared
Active Directory User Principal Name (UPN)	Logical authentication	Not used/shared
Active Directory Globally Unique Identifier (GUID)	Uniquely identify user's Active Directory record	Not used/shared
Active Directory User Identifier (UID)	Uniquely identify user's Active Directory record	Not used/shared
Active Directory Security Identifier (SECID)	Uniquely identify user's Active Directory record	Not used/shared

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?

No

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.

RAP updates information in the existing record. Updates are reflected in the user's audit trail, showing the old value and new value. Example: When an existing remote access user transfers from supervisor to another. Updates in RAP include the old supervisor being replaced with the new supervisor; the 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?

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?

Data at Rest: The RAP database is SQL19 and adheres to the VA SQL 19 Baseline. 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 Virtual Machines (VMs) and TLS 1.2 is enabled. Data transfers between the RAP application and user are sent via TLS, 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.

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

No

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

In addition to Data at Rest and Data in Transit safeguards identified in 2.3.a above, there are physical controls in place at each datacenter. Access to the data center floors is restricted to authorized personnel only, and all access is logged.

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?

RAP roles control who has access to user information - the Information System Security Officer (ISSO) role access is determined by Information System Security Managers (ISSMs) and District Information Security Directors (DISDs); the Approving Official role access is determined by the Designated Approver Capability (DAC) role; the DAC role access is determined by ISSOs; the Portal Support role access is determined by Active Directory Security Group memberships which are maintained via ServiceNOW tickets; the On Boarding / Off Boarding Liaison Official (OBLO) Portal access is determined by RAP Approving Officials. The RAP Access Control Policy provides additional detail.

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

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

2.4c Does access require manager approval?

Yes, the various modules utilize hierarchical management structures for approval.

RAP ISSO Portal Module – The ISSO role is managed by the ISSO hierarchical chain of command. District Information Security Directors (DISDs) manage Information System Security Managers (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.

RAP DAC Portal Module –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).

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

RAP Portal Support Module– 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.

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

RAP OBLO Portal Module – OBLOs are generally 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 approving official and company affiliation.

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

View access is not monitored. All changes to data are recorded.

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

Web application developers and database administrators are responsible for implementing security safeguards for PII.

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 Email
User's Secondary Email
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)

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.*

Active records are archived as soon as the affiliated user account becomes disabled i.e., due to inactivity, directly deleted by an authorized RAP role, or offboarded. Secondary email and secondary phone are deleted when the record is archived. Archived 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)?

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. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
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?

Yes

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

GENERAL RECORDS SCHEDULE 3.2: Information Systems Security Records Disposition Authority: DAA-GRS-2013-0006-0003. Retention period is six years after user account is terminated or when no longer needed for investigative or security purposes, whichever is later.

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.

All records are electronic. To date, none have been destroyed or eliminated. There are no paper records. At the end of the retention period, electronic records will be manually destroyed by permanently deleting the data from the database tables using a database stored procedure. RAP receives offboards (deletes) from Identity and Access Management, which is integrated with HR Smart for VA Employee Offboards; Electronic Contract Management System (ECMS) for contractor offboards; and Active Directory (AD) for VA network account deletions.

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.

Data is not used for research or training.

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. 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. (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: Users' secondary email address and/or secondary phone number (if provided) are deleted when the user's account becomes inactive in RAP. The ability to view users' names and AD account information (covered under the Rolodex exception) after account is inactive is the only remaining risk.

Mitigation: Accounts become inactive in RAP a variety of ways: 1) via an offboard request from the IAM 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. The user's secondary email address and/or secondary phone number (if provided) are deleted from the user's RAP record when they become inactive. 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

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***
VA Microsoft (MS) Active Directory (AD) Assessing (1001)	User information and account information are received from AD and are used for remote access authorization and RAP authorization/access.	Primary Phone, First Name, Middle Initial, Last Name, NTUserID, UPN, Distinguished Name, VA Email, GUID, VA UID, SECID)	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.
Identity and Access Management (IAM)	User information and account information received from IAM.	Primary Phone, First Name, Middle Initial, Last Name, NTUserID, UPN, Distinguished Name, VA Email, Secondary Email, GUID, VA UID, SECID, Distinguished name	RAP API transfers data via TLS, utilizing a single domain SSL certificate that cryptographically establishes an encrypted link

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*
			the web server and a browser. 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.
Enterprise Service Desk (ESD) Active Directory Account Management (ADAM) Tool	ADAM database sends user PIV exemption information to RAMP database (databases within same SQL instance)	NTUserID, User Principal Name (UPN), VA Email	ADAM transfers data via TLS, utilizing a single domain SSL certificate that cryptographically establishes an encrypted link the web server and a browser. The RAP Server safeguards against unencrypted sessions by forcing clients to send requests over https by sending a HTTP response header "Strict-Transport-

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*
			Security" in the event attempts are made to establish a connection over HTTP. A database job runs every five minutes for the ADAM database to update the RAMP database - they are within the same SQL instance – no data is transmitted outside of the SQL instance.
Trusted Internet Connection (TIC) OpenLDAP Server	User remote access account attributes sent to LDAP for authorization/access control	NTUserID, User Principal Name (UPN)	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.

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*
OIT SPLUNK	User historical connection information received from SPLUNK presented to user via reporting (audit requirement – data is not stored in RAMP)	NTUserID, User Principal Name (UPN), VA IP address, User IP address	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. 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.
OIT ManageExpress Virtual Office (MEVO)	User remote access account attributes sent to MEVO for authorization/access control/device configuration	VAVO User Name	The RAMP database transfers data to MEVO API via TLS, utilizing a single domain SSL certificate that

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*
			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.

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: 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

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program***	***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 use, etc. that permit external sharing (can***	***List the method of transmission and the measures in place to secure data***

	office or IT system		***be more than one)***	
N/A	N/A	N/A	N/A	N/A

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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 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.

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://department.va.gov/privacy/system-of-records-notices/

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

Users see the data collected

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.

No, RAP does not provide a Privacy Notice, but notices are provided at the VA Privacy website through this PIA and through the SORN.

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. (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: System users don't know there is a PIA or SOR.

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?

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.***

> 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

7.1b 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)?

> This system is not a Privacy Act exempt system.

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?

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. ***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.

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.*** *(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: 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, secondary email, Primary VA Phone, Secondary Phone, Active Directory Office Code. An AD sync tool allows auto update of AD account information. 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?

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?

Information System Security Officer (ISSO): RAP includes three ISSO roles: DISD, ISSM and ISSO. DISDs are managed (added/removed) by RAP application personnel. DISDs can add/remove access for all ISSM and ISSO user roles within their respective District(s). ISSMs can add/remove ISSO user roles within their respective Territory(ies).

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 have access to user information within their respective facility(ies). 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 primarily to support CORs who manage large contracts, although VA supervisors may elect to designate OBLOs. OBLOs can initiate new remote access requests on behalf of approving officials 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 approving officials and access is restricted based on users assigned to that COR, along with the user's affiliated company (if a contractor).

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.

8.1b 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?

There will be no users from other agencies.

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.

Read only access is granted to all RAP roles (remote access users who do not have a RAP role may only see their own information). Edit capabilities are restricted to: remote access users (who may edit their own record only); ISSOs who may edit user information affiliated with facilities within their management / audit purview; approving officials (supervisors/CORs/delegates) who may edit user information who are under their direct supervision; area managers who may edit user information for users affiliated with facilities under their management purview; ESD personnel who may edit user information based on tickets opened up by, or on behalf of, users, supervisors/CORs, or ISSOs; and on boarding/off boarding liaisons who may edit user information for specific users affiliated with specific supervisors/CORs and company (if a contractor).

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.

VA and Contract 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? No

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

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. 1/31/24***

RAP is a minor application within the NSOC LAN Assessing. ATO was granted on 11/15/2023 and expires on 11/14/2025. 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), 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)*

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). (*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.*

N/A Application is on-prem.

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.

N/A Application is on-prem.

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.

N/A Application is on-prem.

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.

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

ID	Privacy Controls
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 they provided in this Privacy Impact Assessment is true and accurate.

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2024.01.12 08:43:17 -07'00'

Privacy Officer, Julie Drake

DEREK STERNS Digitally signed by DEREK STERNS
Date: 2024.01.16 08:57:51 -05'00'

Information System Security Officer, Derek Sterns

DANIEL MESIMER Digitally signed by DANIEL MESIMER
Date: 2024.01.31 07:19:10 -06'00'

Information System Owner, Daniel Mesimer

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; screen shot of a website collection privacy notice).

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

Privacy Act System of Records Notices (SORNs) - Privacy

Current System Notice

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

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