Privacy Impact Assessment for the VA IT System called:

NSOC - LAN Assessing

(Network Security Operations Center- Local Area Network)

Veteran's Affairs Corporate Office (VACO)

Office of Information and Technology (OIT)

Date PIA submitted for review:

05/4/2023

System Contacts

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Derek Sterns	Derek.Sterns@va.gov	727-201-7464

	Name	E-mail	Phone Number
Information System Owner	John Gardner	John.Gardner@va.gov	202-461-4409

Abstract

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

Network Security Operations Center Assessing (NSOC – LAN) Assessing supports both the Trusted Internet Connection (TIC) and the Cybersecurity Operations Center (CSOC). NSOC - LAN Assessing- with associated personnel, devices and systems- delivers the necessary infrastructure for both the TIC and the CSOC by providing network transport, virtualization, shared storage, operating systems, applications, and enterprise monitoring tools to support dual missions. NSOC - LAN Assessing not only provides NSOC and CSOC personnel with a robust on-premises cloud, but it also supplies the tools and applications essential to deliver world class information security throughout the VA Enterprise to include Remote Access, Security Information & Event Management (SIEM), Intrusion Prevention (IPS), Nessus scanning, nmap - Enterprise Discovery Scanning, penetration testing, database scanning, WASA scanning, Fortify scanning, and forensics. The following minor applications are deployed on the NSOC-LAN: • Remote Access Information and Media Portal (Media Site) • Remote Access Portal (RAP) • External Assessment Services (EAS) Portal • Vulnerability Information Tracking and Assessments Library (VITAL) • Scan Registration Portal • Remote Connection Manager (Site to Site Tool) • Change Control Board (CCB)

Overview

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

1 General Description

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

Office of Information and Technology

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

The VA-NSOC - LAN Assessing supports the mission of the VA-NSOC (Veterans Affairs Network Security Operations Center). NSOC - LAN Assessing personnel, devices, and systems support the mission by monitoring, maintaining, and managing the availability and access to the VA Enterprise Network and to the Internet, as well as ensuring adequate perimeter security for the VA Enterprise. NSOC - LAN Assessing allows personnel to perform their duties by allowing access to network resources such as Microsoft Exchange for email, Microsoft SharePoint portal for document collaboration, Remedy ticketing system for incident reporting and asset management, CiscoVoice over IP phone system for voice collaboration, Cisco Meeting place for online meetings, and the Cisco Unified Call Center Express application, in support of the VA-

NSOC 24/7 mission. The VA-NSOC infrastructure facilitates access to the VA Network by means of standard workstations, servers, routers, and switches. There are also wireless access devices in place that are used for wireless access to the VA Network. Also connected to the Network are Voice- over Internet Protocols (VoIP) communications. These segments of the Network are controlled by VLANS, and access rules are used to control access requirements.

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

VA Owned and Operated

2. Information Collection and Sharing

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

This system has information of 200 VA employees who use NSOC - LAN Assessing. Additionally, the Remote Access Portal (RAP), a minor application within the system, includes information on approximately 290,000 individuals. These individuals include remote access users, approving officials (supervisors, CORs and area managers) and ISSOs.

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

For day-to-day operations of NSOC - LAN Assessing. Information related to RAP: 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.

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

Remote Access Protocol (RAP) Information sharing includes:

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.

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

Information is stored in two locations and same controls are used in both sites. SQL Server transactional replication is enabled to ensure the standby database is always in sync with the production database and provides the ability for 'point in time' recovery. Full backups are performed weekly and the transaction logs are backed up weekly.

3. Legal Authority and SORN

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

Privacy Act of 1974; System of Records
Department of Veterans Affairs Identity Management System(VAIDMS)-VA.146VA005Q3https://www.oprm.va.gov/docs/Current_SORN_List_2_25_2022.pdf

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?

No.

D. System Changes

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

No

K. Whether 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.

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

- ☒ Name
- ☐ Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

RAP Application Information Collected:
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
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)

PII Mapping of Components (Servers/Database)

The Remote Access Portal (RAP) application, a minor application within NSOC - LAN Assessing, consists of 2 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by NSOC LAN Assessing and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

Internal Database Connections

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

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?

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.

1.2b 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.

Authoritative information for the purposes of authentication and authorization are required to meet various National Institute of Standards and Technology (NIST) Access Control (AC), Audit and Accountability (AU), and Identification and Authentication (IA) controls.

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

Remote Access Protocol (RAP) provides various reports.

1.3 How is the information collected? To

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?

Remote Access Protocol (RAP) 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.

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

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 Remote Access Protocol (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).

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

N/A

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

Privacy Act of 1974; System of Records
Department of Veterans Affairs Identity Management System(VAIDMS)-
VA.146VA005Q3https://www.oprm.va.gov/docs/Current_SORN_List_2_25_2022.pdf

- 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
- National Archives and Records Administration (NARA) (44 U.S.C Chapter 21) c 2102 (a) (Pub. L. 98-497, § 103) (a)
- Records Management by the Archivist of the United States (44 U.S.C. Chapter 29) c 2901 .2 "Record Management; c 2605 (a) "Selective Retention of records; security measures.

- Executive Order 9397, Numbering System for Federal Accounts Relating to the Individual Persons
- 5 U.S.C. 552a, “Privacy Act,” c. 1974
- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- Federal Information Security Management Act (FISMA) of 2002

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: 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.

Information	Internal VA Use	External Use
Name	Identify VA user	Not used/shared
Active Directory Domain	Logical authentication	Not used/shared
VA Email	Send system emails to user	Not used/shared
Secondary Email	Send system emails to user	Not used/shared
Primary VA Phone	Contact 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 Office Code (optional)	Identify user's work unit	Not used/shared
Active Directory Globally Unique Identifier (GUID) (not visible within application)	Uniquely identify user's Active Directory record	Not used/shared
Active Directory User Identifier (UID) (not visible within application)	Uniquely identify user's Active Directory record	Not used/shared
Active Directory SECID (not visible within application)	Uniquely identify user's Active Directory record	Not used/shared
Remote Access Justification	Justify approval of remote access	Not used/shared
Date Remote Access Profile was Created	Audit requirement	Not used/shared
Remote Access Types Enabled	Logical authentication	Not used/shared
Remote Access Settings	Logical authentication	Not used/shared
2FA Exemption Information	Logical authentication	Not used/shared
VA Facility Affiliation	Identify user's physical location	Not used/shared
Company Affiliation (if contractor)	Identify contractor's company	Not used/shared
User's Supervisor/COR	Required to create approval workflow	Not used/shared
User's Account Expiration Date (if applicable)	Disables access on identified date	Not used/shared
VAVO User Name	Identity assigned to VAVO router	Not used/shared
VAVO Class	Combination of VAVO router model and preferred gateway	Not used/shared
VAVO Provisioning Email	Email address identified to push configuration information to	Not used/shared
VAVO IP Phone	Identifies if user has an IP Phone	Not used/shared
VAVO UC Primary IP	Identifies IP phone IP addresses to allow VAVO device to communicate with	Not used/shared
VAVO UC Secondary IP	Identifies IP phone IP addresses to allow VAVO device to communicate with	Not used/shared

VAVO Video DX80	Identifies if user has a video device	Not used/shared
VAVO Display Name	Unique username assigned to VAVO device	Not used/shared
VAVO Status	Identifies if VAVO is enabled or disabled	Not used/shared
VAVO ISP Speed	VAVO user's ISP speed	Not used/shared
VAVO Request Justification	User's justification to supervisor to approve VAVO	Not used/shared
VAVO DV Primary IP	Identifies video IP addresses to allow VAVO device to communicate with	Not used/shared
VAVO DV Secondary IP	Identifies video IP addresses to allow VAVO device to communicate with	Not used/shared
VAVO Serial Number	Serial number of user's VAVO router	Not used/shared
Approval Workflow initiations/status changes	Status of remote access request workflow	Not used/shared
Request Approvals/Denials	Audit of approval or denial of remote access request	Not used/shared
User Review Flows and Approvals/Denials	Audit of User Review initiations, actions and completion	Not used/shared
Transfers to Other Companies/Facilities/Supervisors/CORs (if applicable)	Audit to show changes in companies, facilities, and supervisors/CORs	Not used/shared
Conversion to Employee/Contractor (if applicable)	Audit to show change in user type from employee to contractor and vice versa	Not used/shared
Remote Access Types Enabled/Disabled	Status of each remote access method	Not used/shared
Account Deletion (if applicable)	Audit of account deletion	Not used/shared
ESD Actions Related to User (if applicable)	Audit of ESD actions (IE PIV exemption, re-enable account, delete account)	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.

The Remote Access Portal (RAP) interface for a user search includes the ability to search based on 1) lastname, firstname; 2) email address; 3)NTUserID. All searches require a minimum of three characters and include an implicit trailing wildcard. The RAP Self Service Portal retrieves a single record based on Active Directory authentication (where user's Active Directory Domain\NTUserID or GUID are an exact match).

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.

Remote Access Portal (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?
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. 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.

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 not collected

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

NSOC - LAN ASSESSING is hosted VA data centers that are in compliance with OMB Memorandum M-06-15 safeguards and security mechanisms ATO packages in eMASS for Hines, IL, Falling Waters, WV, Martinsburg, WV outlines all OMB Memorandum M-06-15 safeguards and security mechanisms.
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.

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?

Access to PII is determined by job role.

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

NSOC - LAN Assessing information system account types are limited to VA system administrators and NSOC - LAN Assessing system administrators. All access criteria, procedures, controls, and responsibilities are documented within NSOC - LAN Assessing A&A (assessment and authorization)

eMASS package. RAP restricts access based on roles defined within the application. RAP includes online Help for each RAP role.

2.4c Does access require manager approval?

Access to NSOC - LAN Assessing systems is determined by…….
General user access to Remote Access Portal (RAP) does not require manager approval. Any VA-authenticated user can access the RAP Self Service Portal. The ISSO role requires manager approval. ISSOs approve RAP approving officials. Approving officials approve Onboard Offboard Liaison Officials (OBLOs). Access to the Portal Support role is administered via AD security groups and requires a ServiceNOW ticket.

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

No

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

VA employees should safeguard their information when applicable. Data at rest and data in transit is safeguarded via encryption and role-based access.

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****. 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.*

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

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. 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. 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. (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: 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 NSOC LAN Assessing in 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

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***
Active Directory Account Management (ADAM)	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)	Domain, SAM Account (NTUserID), UPN, VA Email, Exemption Information	HTTPS
Trusted Internet Connection (TIC) Open LDAP Server	User remote access account attributes sent to LDAP for	UPN, Domain, SAM Account (NTUserID), Access types enabled,	Secure LDAP (Port 636)

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*
	authorization/access control	Access settings, 2FA Exemptions	
Manage Express Virtual Office (MEVO)	User remote access account attributes sent to MEVO for authorization/access control/device configuration Ac	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 DV Primary IP, VAVO DV Secondary IP,VAVO Serial Number	HTTPS via API

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 office or IT system***	***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 be more than one)***	***List the method of transmission and the measures in place to secure data***
None				

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

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.

(VAIDMS)-VA. 146VA005Q3 https://www.oprm.va.gov/docs/Current_SORN_List_2_25_2022.pdf

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

N/A

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.

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

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 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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:

<u>Privacy Risk:</u> 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?

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).

N/A

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.

N/A

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.

Remote Access Portal (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, VA email, secondary email, Primary VA Phone, Secondary Phone, Active Directory Office Code. Users contract 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.

VA employees are granted access to the system based on the employee's job role.The job roles for these employees determine their assigned Active Directory (AD) groups. If the VA employee requires Elevated Privilege (EP) they would submit an ePAS request and they would be assigned to AD groups via ePAS.

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?

N/A

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.

Administrator, User

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?

8.4a If Yes, provide:

1. *The Security Plan Status:* Current
2. *The System Security Plan Status Date:* Signed 4/11/2023
3. *The Authorization Status:* 3 Year ATO
4. *The Authorization Date:* 11/24/2020
5. *The Authorization Termination Date:* 11/24/2023
6. *The Risk Review Completion Date:* 11/7/2020
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

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), 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)*

N/A

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

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

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

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 –

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
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.

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.06.01 21:30:56 -04'00'

Privacy Officer, Tonya Facemire

DEREK STERNS

Digitally signed by DEREK STERNS
Date: 2023.06.01 15:02:59 -04'00'

Information System Security Officer, Derek Sterns

JOHN GARDNER

Digitally signed by JOHN GARDNER
Date: 2023.06.01 12:19:08 -04'00'

Information System 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).

SORN 146VA005Q3, Department of Veterans Affairs Identity Management System (VAIDMS)-VA. E8-6120.pdf

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices