Privacy Impact Assessment for the VA IT System called:

AEON -E

VACO

Office of Acquisition & Logistics (OAL)

eMASS ID # 2435

Date PIA submitted for review:

4/10/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov oitprivacy@VA.gov	202-632-8431
Information System Security Officer	J. Mark McGee	James.mcgee5@va.gov	520-358-3237
Information System Owner	Scottie Ross	scottie.ross@va.gov	478-595-1349

Abstract

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

AEON/ Automated Acquisition Management Solution (AAMS) is the contract document generation, milestone tracking, contract file management, and interfacing to the federally mandated E-Gov Integrated Award Environment (IAE).

AEON technology enables acquisition professionals to have ready access to their organization's documented base of facts, sources of information, and recommended workflows. AEON dynamically adapts to changing business drivers within customer environments to maximize the effectiveness of individuals in their organization's acquisition process.

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?

AEON/Automated Acquisition Management Solution (AAMS), managed by The Office of Acquisition &Logistics (OAL).

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

Office of Acquisition & Logistics (OAL) currently utilizes AEON, which is a component of Electronic Contract Management System (eCMS). It is the contract document generation, milestone tracking, contract file management tool. This is an end-to-end contract software solution that is linked to financial management systems such as the integrated financial and acquisition management solution (iFAMS), and the integrated Funds Distribution Control Point Activity Accounting & Procurement (IFCAP). It is a Web-based productivity tool that generates reports, posts announcements, and manages electronic contracts.

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

The system is owned and operated by the providing AEON SaaS vendor and will be managed by the Office of Acquisition & Logistics (OAL) program office.

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 AEON system contains VA vendor data populated from General Services Administration (GSA) System for Award Management (SAM.gov) Entity Information. The VA vendor data contains approximately 10 – 15 thousand vendors approved by SAM.gov.

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

AEON serves as a data repository for contract files within the VA. AEON was designed to house VA procurement and contracting data and provide lifecycle contract management capabilities and processes.

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

Information is collected through a combination of automated and manual processes. Information is automatically received via secured File Transfer Protocol (sFTP); and web service interface; and manually via email, fax, and U.S Mail sent to the Contracting Officer who then scans the printed copy and uploads the scanned document; or the Contracting Officer saves the information in an electronic file and uploads the file.

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?

AEON is a Cloud based system deployed on the Project Hosts GSS One-Azure system deployed in turn on Azure Government Virginia. Backups are off sited to Azure Gov Texas and are encrypted in transit and at rest. AEON is a Cloud based system deployed on the Project Hosts GSS One-Azure system deployed in turn on Azure Government Virginia.

3. Legal Authority and SORN

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

GSA/GOVT-9 System for Award Management (SAM) February, 19, 2013, 78FR11648 https://www.fpc.gov/resources/SORNs/#container

H. 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?

A SORN exists and the SORN number is 78FR11648. The SORN will not require amendment, revision or approval. The SORN does not specifically mention cloud usage or storage. It only references electronic records are stored electronically in secure locations.

4. System Changes

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

AEON business processes will not change.

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

AEON technology will not change.

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)

Other PII/PHI data elements: Business e-mail address

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

PII Mapping of Components (Servers/Database)

AEON consists of one key component (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 AEON 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
Automated Acquisition Management Solution (AAMS)	Yes	Yes	• Name • Business Email Address • Tax ID • SSN	• Vendor Identification	DMZ, Segregation, Access Controls, Pre-authenticated Traffic, Network Security Group Firewall Rules, Encryption in transit/ rest

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?

Information is collected through a combination of automated and manual processes from other systems such as the VISTA Prosthetic's GUI (Part of VHA), VISTA Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP) maintaining records of available funds, determining the status of a request, comparing vendors and items to determine the best purchase, recording the receipt of items into the warehouse, paying vendors, and time and attendance., GSA System for Award Management (SAM) is a website that provides the following; Register to do business with the U.S. government, Update or renew your entity registration, Check status of an entity registration, Search for entity registration and exclusion records and Law Enforcement Background Investigation system that provide Privacy Notice.

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.

Such information is collected to determine the status of a request, to compare vendors and items, in order to determine the best purchase. It is also utilized to record receipt of items into warehouses, paying vendors, and time and attendance. GSA System for Award Management (SAM) is a website that provides such the ability to update or renew your entity registration, check status of an entity registration, search for entity registration and exclusion records. It also provides a Law Enforcement Background Investigation system that provides Privacy Notice.

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

No. It does not create information; it collects information.

1.3 How is the information collected?

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

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

Information is collected through a combination of automated and manual processes. Information is automatically received via secured File Transfer Protocol (sFTP); and web service interface; and manually via email, fax, and U.S Mail sent to the Contracting Officer who then scans the printed copy and uploads the scanned document; or the Contracting Officer saves the information in an electronic file and uploads the file.

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: information is not collected on a form or subject to the Paperwork Reduction Act

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.

AEON does not check the data for accuracy. AEON receives the entity extracts from System for Award Management (SAM.gov) and updates the data in AEON daily and refreshes

the data monthly. AEON receives the entity extract that contains data validated through the entity registration process managed through the SAM.gov entity registration.

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?

Yes, Information is used to document and verify contractual information, such as payroll and veterans' addresses for delivery of items. The information is used so that AES can perform daily processes such as house all VA procurement and contracting data and provide lifecycle contract management capabilities and processes.

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

For System for Award Management (SAM.gov) Entity Management, the authorities for collecting the information and maintaining the system are the Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c). For the exclusions portion of the Performance Information functional area, the authorities for collecting the information and maintaining the system are FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989).

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: There is a risk inaccurate information is transmitted and received by the system.

Mitigation: If inaccurate information is received by the system, the contracting officer will contact the vendor to rectify the information.

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	Used to identify the veteran who contracted item will be delivered.	Not used
Business E-mail	Used as delivery point for contracted items	Not used
Tax ID	Used as unique identifiers for contracts and vendors	Not used
Social Security Number	Used as unique identifiers for contracts and vendors	Not used

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 data analysis is conducted on the vendor data.

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.

AEON receives the entity extracts from General Services Administration (GSA) - System for Award Management (SAM) when the data received is processed daily/refreshed monthly, it updates the existing vendor record in AEON/Automated Acquisitions Management System (AAMS)

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?

All Data in transit and at rest are encrypted using FIPS validated Algorithms and approved Ciphers.

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

All system databases are encrypted, all data is encrypted in transit and at rest compliant with FIPS 140-2. Users cannot look up the information and no information is shared with any external systems.

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

The environment is deployed in a defense in depth mannerism, all traffic is pre-authenticated and terminated at the DMZ servers which runs intrusion prevention/ detection software and does SSL/TLS offloading. All servers are running Antivirus/ HIPS software and encryption is all encrypted at rest leveraging FIPS validated Algorithms and ciphers. A SIEM solution is configured leveraging Log Analytics, Azure Monitor, Microsoft Defender for Cloud, Azure Sentinel, Microsoft Flow Logs, Azure Activity Logs. These logs are all correlated within the SIEM solution, and we have alerting configured to notify our SOC team of any potential incidents.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

<u>Principle of Transparency:</u> Is the PIA and SORN, if applicable, clear about the uses of the information?

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

Users in AEON/AAMS with a Contract Specialist or Contracting Officer role have access to vendor data. The access is provided after successful completion of the 3.5 days eCMS New User Training class and manager approval. Once approved, a user account is created in AEON/AAMS assigning the user with the Contract Specialist or Contracting Officer role.

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

Yes. Access controls and procedures are documented in the request ticketing system and monitored by the program office as documented in the eCMS Standard Operating Procedures (SOPs).

2.4c Does access require manager approval?

Yes, user accounts are created with a Contract Specialist or Contracting Officer role by the AEON/AAMS application coordinators with manager approval after receiving a ticket to create a new account following the eCMS Standard Operating Procedures.

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

Yes, AEON/AAMS tracks user activity in the system to include data accessed.

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

The AEON/AAMS system is behind DMZ subnets with web application proxies that enforce TLS 1.2 encryption to the components. All user access is via SSO from the VA ADFS servers. All data is encrypted using Azure Storage Service Encryption. All AEON/AAMS users must take annual VA Privacy and Information Security Awareness and Rules of Behavior training that is recorded in the Talent Management System (TMS).

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
Business E-mail address
Tax ID Number
SSN

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.*

Information may be retained for the length of the Contract the length of contracts varies considerably and may be extended by option years. Federal Acquisition Regulations govern retention of the contract information. (Temporary; destroy 3 years after completion of contract or conclusion of contract being subject to an enforcement action, but longer retention is authorized if required for business use.)

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, all records are stored within the system of record indicated on an approved disposition authority. General Record Schedule is the Records Control Schedule and Federal Acquisition Regulation (FAR)

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

General Record Schedule applies to contracting records:
GENERAL RECORDS SCHEDULE 1.1: Financial Management and Reporting Records
Item 011 Procuring goods and services,
Disposition: Temporary. Destroy when business use ceases.
Disposition Authority: DAA-GRS 2013-0003 0002
Link: https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

For this system the Federal Acquisition Regulation (FAR) disposition supersedes the General Records Schedule

Table 4-1—Retention Periods

Record Retention period
(1) Contracts (and related records or documents, including successful and unsuccessful proposals, except see paragraph (c)(2) of this section regarding contractor payrolls submitted under construction contracts)6 years after final payment.

(2) Contractor's payrolls submitted under construction contracts in accordance with Department of Labor regulations (29 CFR 5.5(a)(3)), with related certifications, anti-kickback affidavits, and other related records3 years after contract completion unless contract performance is the subject of an enforcement action on that date (see paragraph (c)(8) of this section).
(3) Unsolicited proposals not accepted by a department or agency Retain in accordance with agency procedures.
(4) Files for canceled solicitations6 years after cancellation.
(5) Other copies of procurement file records used for administrative purposes When business use ceases.
(6) Documents pertaining generally to the contractor as described at 4.801(c)(3)Until superseded or obsolete.
(7) Data submitted to the Federal Procurement Data System (FPDS). Electronic data file maintained by fiscal year, containing unclassified records of all procurements exceeding the micro-purchase threshold, and information required under 4.6036 years after submittal to FPDS.
(8) Investigations, cases pending or in litigation (including protests), or similar matters (including enforcement actions)Until final clearance or settlement, or, if related to a document identified in paragraphs (c)(1) through (7) of this section, for the retention period specified for the related document, 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.

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA Directive and Handbook 6500, Information Security Program Electronic Media Sanitization.
https://www.va.gov/vapubs/search_action.cfm?dType=1

Disposition of Printed Data:

Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the staff member responsible for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371a, Destruction of Temporary Paper Records. Records Retention Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

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.

AEON system does not use PII production information in testing, training, or research.

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: There is a risk that the information maintained by AEON could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: AEON adheres to the VBA VB-1 RCS_I Record Control Schedule for each category or data it maintains. AEON follows retention schedule VB-1 and retains information for as long as the RCS permits, dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)." AEON doesn't give access to retention information or logs.

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***
Centralized Administrative Accounting Transaction System (CAATS)	Information allows for the automated preparation, approval and processing of transactions into the accounting system	Contract information which includes Name, Tax ID, SSN	Web Service
Integrated Funds Distribution Control Point Activity, Accounting and Procurement (IFCAP)	Information used to obligate purchase orders.	Contract information which includes Name, Tax ID, SSN	Database View
EPIC	Records system and database	Contract information which includes Name, Tax ID, SSN	Web Service
Acquisition Service Bus (ASB)	Middleware routes that get and push data from various eCMS Databases Used to	Contract information which includes Name, Tax ID, SSN	Web Service

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*
	facilitate data requests from applications		

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: The privacy risk associated with maintaining vendor data within the Department of Veterans' Affairs is that the data may be disclosed to individuals who do not require access or have a need to know. Inappropriate/unauthorized disclosure heightens the threat of the information being misused. There is a risk that information may be shared with unauthorized VA program or system or that data could be shared.

Mitigation: Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors. The AEON/AAMS system is behind DMZ subnets with web application proxies that enforce TLS 1.2 encryption to the components. All user access is via SSO from the VA ADFS servers. All data is encrypted using Azure Storage Service Encryption. Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

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***
General Services Administration (GSA) - System for Award Management (SAM)	Vendor information received from SAM	Contract information which includes Name, Tax ID, SSN	Enterprise Agreement	Web Service

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: There is a risk inaccurate information is transmitted and received by the system.

Mitigation: Data quality procedures exist in the system to identify and address all scenarios that include inaccurate information. If inaccurate information is received by the system, the contracting officer will contact the vendor to rectify the information.

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.

AEON does not directly collect information from individuals. Data Extracts of information are received and loaded by AEON from SAM.gov entity extracts on a daily and monthly refresh basis. Upon a vendor selecting to begin an entity registration entry with System for Award Management (SAM.gov), the user receives a pop-up screen notifying them that PII will be collected, and they must accept this notice before proceeding. The user can access this screen when they navigate to SAM.gov and then proceed to the "Sign In" button located at the top right of the screen.

79VA10 / 85 FR 84114, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, 12/23/2020 ink: https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

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

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.

AEON does not directly collect information from individuals. Data Extracts of information are received and loaded by AEON from SAM.gov entity extracts on a daily and monthly refresh basis. System for Award Management (SAM.gov) collects necessary information from individuals and entities seeking to do business with the U.S Government. The information is required to create an entity record to establish and validate the applicant's identity, determining the eligibility of various awards/grants/programs/benefits. The notice screen in 6.1a cites the appropriate Federal Regulations code and GSA Policy.

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.

Yes, individuals have the right to decline but VA has the right to not accept the contract documents or award contracts without the required information as stated in FAR clauses and VA acquisition directives and handbook The individual shall not be denied any right, benefit, or privilege provided by law (see 38 CFR 1.575(a)).

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.

AEON does not directly collect information from individuals. Data Extracts of information are received and loaded by AEON from SAM.gov entity extracts on a daily and monthly refresh basis. VA uses vendor Tax ID Number (TIN) to ensure reporting of appropriate value awarded to correct vendor. An individual may register to do business with the VA in General Service Administration (GSA) System of Award Management (SAM.gov). The VA has no control over this however still has the obligation to report contract awards appropriately.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that the vendor may not have received all notices and fully understand how their information is being collected, maintained, processed, or disseminated by System for Award Management (SAM.gov).

Mitigation: GSA has a published notice on how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act. Vendors are aware that System for Award Management (SAM.gov) contains a record of them because they created their entity registration through a self-registration portal and accept the notice provided on the following screen. The notice appears upon a vendor selecting to begin an entity registration entry with System for Award Management (SAM.gov), the user receives a pop-up screen notifying them that PII will be collected, and they must accept this notice before proceeding. The user can access this screen when they navigate to SAM.gov and then proceed to the "Sign In" button located at the top right of the screen. Department of Veterans Affairs has also published a SORN. The SORN number is 78FR11648. the user receives a pop-up screen notifying them that PII will be collected, and they must accept this notice before proceeding.

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.***

AEON does not directly collect information from individuals. Data Extracts of information are received and loaded by AEON from SAM.gov entity extracts on a daily and monthly refresh basis. Vendor entities create the entity registration record in System for Award Management (SAM.gov) through a self-registration portal, there are no restriction or limitation to managing such data. Users can delete, update, or amend the record at will. However, individuals can contact the SAM.gov system manager with questions about the operation of the Entity Management functional area.

How to make a Freedom of Information Act Request:
https://department.va.gov/accountability/freedom-of-information-act-and-privacy-act-requests/how-to-make-a-freedom-of-information-act-foia-request/

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)?

The system is not exempt.

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?

AEON does not directly collect information from individuals. Data Extracts of information are received and loaded by AEON from SAM.gov entity extracts on a daily and monthly refresh basis. All vendors have access to their information by going to General Service Administration (GSA) and System for Award Management (SAM.gov) to gain access to their information. The updated information will be uploaded to AEON/AAMS through the daily entity extracts. As outlined in SORN 78FR11648, individuals seeking information regarding access to records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

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.

All vendors have access to their information by going to General Service Administration (GSA) and System for Award Management (SAM.gov) to make updates, corrections to their information. The updated information will be received by the VA through the daily entity extracts received from SAM.gov.

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.

AEON does not directly responsible for correction of collected information. SAM is responsible for communicating with the vendor regarding any issues pertaining to their information.

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.

Vendors are allowed to update their entity registration through System for Award Management (SAM.gov) Entity Information.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the individual accidentally provides incorrect information in their entity registration.

Mitigation: The individual may register or make correction to do business within VA in General Service Administration (GSA) System of Award Management (SAM) and may decide to use their SSN instead of obtaining a separate incorporated TINs. The VA has no control over this. However, still has obligation to report contract award appropriately.

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?

Users in AEON/AAMS with a Contract Specialist or Contracting Officer role have access to vendor data. The access is provided after successful completion of the 3.5 days eCMS New User Training class and manager approval. Once approved, a user account is created in AEON/AAMS assigning the user with the Contract Specialist or Contracting Officer role.

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

Users from other agencies are not granted access to the system.

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.

Users in AEON/AAMS with a Contract Specialist or Contracting Officer role have read only access to vendor data.

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.

VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS) and must sign a non-disclosure agreement (NDA). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program

Manager, and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

Contractor confidentiality agreements, Business Associate Agreements (BAA), and Non-Disclosure Agreements (NDA) have been developed for contractors who work on the system

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.

Prior to receiving access, the user must complete and sign the User Access Request Form. The user must complete, acknowledge, and electronically sign the VA Rules of Behavior. The user also must complete mandatory security and privacy awareness training. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training via the VA's TMS.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date: 03/24/2023*
3. *The Authorization Status: FedRAMP Authorized*
4. *The Authorization Date:* 4/8/2019
5. *The Authorization Termination Date: VA ATO not yet granted*
6. *The Risk Review Completion Date:* July 2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate.

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

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

Not Applicable.

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)*

This system is a Software as a Service (SaaS) housed on the Azure.gov technology. The system is currently FedRAMP Authorized and active on the FedRAMP Marketplace under FedRAMP ID FR1805752046.

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.*

The Department of Veterans Affairs has ownership rights over all data per awarded contract number: 47QTCA18D0095.

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.

No Ancillary Data is collected.

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.

Yes, this is in the contract for implementation of AEON/AAMS in the FedRAMP authorized environment.

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).

AEON/AAMS uses software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. RPA (SharePoint Workflow) is currently used to support the API closeout process.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2024.05.16 08:11:05 -06'00'

Privacy Officer, Julie Drake

JAMES MCGEE Digitally signed by JAMES MCGEE
Date: 2024.05.16 15:05:06 -07'00'

Information System Security Officer, J. Mark McGee

SCOTTIE ROSS Digitally signed by SCOTTIE ROSS
Date: 2024.05.20 10:01:06 -04'00'

Information System Owner, Scottie Ross

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).

https://www.va.gov/oig/pubs/VAOIG-11-04376-81.pdf

https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc

https://www.va.gov/vapubs/search_action.cfm?dType=1

System Title: Department of Veterans Affairs Identity Management System (VAIDMS)-VA; SORN #

GSA/GOVT-9 System for Award Management (SAM) February, 19, 2013, 78FR11648 https://www.fpc.gov/resources/SORNs/#container

Link: https://www.oprm.va.gov/privacy/systems_of_records.aspx.

146VA005Q3/73 FR 16093; Link: https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf

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