Privacy Impact Assessment for the VA IT System called:

Environmental Agents Service Registries
Veterans Healthcare Administration (VHA)
Office of the Assistant Deputy Under Secretary for Health for Policy and Planning
eMASS ID #111

11/21/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.Katz-Johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Neil Cruz	Neil.Cruz@va.gov	202-632-7422
Information System Owner	Temperance Leister	Temperance.Leister@va.gov	484-432-6161

Abstract

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

The Environmental Agent Service Registries (EAS/R) is a combination of application inputs for the Ionizing Radiation Registry (IRR), the Agent Orange Registry (AOR), and the Gulf War Registry (GWR). EAS/R is used to record, track and monitor the health of specific groups of Veterans. It provides a mechanism to catalogue prominent symptoms, reproductive health, reported exposures and diagnoses. It is not designed or intended to be a research tool or to confer benefits. However, the voluntary, self-selected nature of the registry makes it valuable for health surveillance.

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?

Environmental Agents Service Registries (EASR)
Veterans Healthcare Administration (VHA), Office of the Assistant Deputy Under Secretary for Health for Policy and Planning

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

The Environmental Agent Service Registries (EASR) is a combination of application inputs for the Ionizing Radiation Registry (IRR), the Agent Orange Registry (AOR), and the Gulf War Registry (GWR). EAS/R is used to record, track and monitor the health of specific groups of Veterans. It provides a mechanism to catalogue prominent symptoms, reproductive health, reported exposures and diagnoses. It is not designed or intended to be a research tool or to confer benefits. However, the voluntary, self-selected nature of the registry makes it valuable for health surveillance.

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

VA owned and VA operated.
Veterans Healthcare Administration (VHA) Office of the Assistant Deputy Under Secretary for Health for Policy and Planning

2. Information Collection and Sharing

C. 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 expected number of individuals (veterans) is over 4000.

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

The general description is that it is used to record, track and monitor the health of a specific group of veterans.

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

This Application does not share information or data with other Applications.
Below are components of the system
Webserver, Name, DOB, SSN, Address
Database Name, DOB, SSN, Address
Server, Linux Name, DOB, SSN, Address

F. 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?

The system is operated in one site.

3. Legal Authority and SORN

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

SYSTEM NAME AND NUMBER: Agent Orange Registry—VA (105VA10P4Q) SECURITY CLASSIFICATION: Unclassified. SYSTEM LOCATION: Character-based data from Agent Orange Registry (AOR) are maintained in a registry database at the Austin Information Technology Center (AITC), 1615 Woodward Street, Austin, Texas 78772. The secure Web-based data entry system is maintained by the AITC and provides retrievable images to users. SYSTEM MANAGER(S): Deputy Chief Consultant, Post Deployment Health Services (10P4Q), VA Central Office, 810 Vermont Avenue NW, Washington, DC 20420.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code (U.S.C.) 527, 1116, 1710(e)(1)(B) and 1720E, Public Law 102–585 Section 703, and Public Law 100–687.

SYSTEM NAME Gulf War Registry—VA (93VA10) SECURITY CLASSIFICATION: Unclassified. SYSTEM LOCATION: Character-based data from Gulf War Registry (GWR) Code Sheets are maintained in a registry data set at the Austin Information Technology Center (AITC), 1615 Woodward Street, Austin, Texas 78772 and may be maintained at contracted data repository sites, such as the Cerner Technology Centers (CTC): Primary Data Center in Kansas City, MO and Continuity of Operations/Disaster Recovery (COOP/DR) Data Center in Lee Summit, MO. Since the data set at the AITC is not all-inclusive, i.e., narratives, signatures, etc., noted on the code sheets are not entered into this system, images of the code sheets are maintained at the Department of Veterans Affairs, Post Deployment Health Services (12POP5), 810 Vermont Avenue NW, Washington, DC 0420. These are electronic images of paper records,

i.e., code sheets, medical records, questionnaires and correspondence. SYSTEM MANAGER(S): Deputy Chief Consultant, Post Deployment Health Services (12POP5). VA Central Office, 810 Vermont Avenue NW, Washington, DC 20420. Telephone number 202–266–4511 (this is not a toll- free number). AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code (U.S.C.) 1117, Public Laws 102–585 and 100– 687.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code (U.S.C.) 527, 1116, 1710(e)(1)(B) and 1720E, Public Law 102–585 Section 703, and Public Law 100–687.

SYSTEM NAME: Ionizing Radiation Registry-VA 69VA10 / 86 FR 23048. SECURITY CLASSIFICATION: Unclassified. SYSTEM LOCATION: Character-based data from Ionizing Radiation Code Sheets are maintained in a registry data set at the Austin Information Technology Center (AITC), 1615 Woodward Street, Austin, Texas 78772. Since the data set at the AITC is not all-inclusive, i.e., narratives, signatures, etc., noted on the code sheets are not entered into this system, images of the code sheets are maintained at the Department of Veterans Affairs, Post Deployment Health Services (10P4Q), 810 Vermont Avenue NW, Washington, DC 20420. These are electronic images of paper records, i.e., code sheets, medical records, questionnaires and correspondence. SYSTEM MANAGER(S): Deputy Chief Consultant, Post Deployment Health Services (10P4Q). VA Central Office, 810 Vermont Avenue NW., Washington, DC 20420. Telephone number (202) 266–4511 (Note: this is not a toll-free number).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code (U.S.C.) 527, 1116, 1710(e)(1)(B) and 1720E, Public Law 102–585 Section 703, and Public Law 100–687.

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?

I. The system is not in the process of being modified, and it is not in the clouds.

4. System Changes

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

This will not result in changes to the business process.

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

No, this should not result in technology changes.

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:

Name, SSN, Facility Number, Date of Exam, Branch of Service, Exposure Periods, Location, Exposures, Self-Assessment (Health), Birth Data, Veterans Children, Consultation for Health Disposition, Symptoms, Diagnoses, ICD Codes, Examiner Name, Veterans Areas server, Military Occupational Specialty (MOS), Exposures, Did Veteran Smoke, Depleted Uranium, Mustard Gas, Sodium Dichromate Exposure, Date of Sodium Dichromate Exam, Experiences, Self-Assessment, Veterans health after Persian Gulf Service, Veterans Children, Child Birth Defects, Infertility in Veterans Spouse, Infant Death, Consultations, Disposition, Symptoms, VDRL, Vitamin B-12, HIV, T4, TSH, Urinalysis, TB Skin Test, Chest Xray, CAPS, Consultations, Diagnoses, Unexplained Illness, Thyroid Cancer, Leukemia, Lung

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

Cancer Breast Cancer, Bone Cancer, Pancreatic Cancer, Urinary Bladder Cancer, Salivary Gland Cancer, Multiple Myeloma, Stomach Cancer, Diseases.

PII Mapping of Components (Servers/Database)

EAS consists of 3 key components (one webserver, one database server, one linux server). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by EAS 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
Webserver	Yes	Yes	Name, DOB, SSN,	Patient Assessment	Virtual server at AITC (2)
Database Server 1	Yes	Yes	Name, DOB, SSN,	Required for processing veteran information	Oracle Database server in AITC (1)
Linux Server	Yes	Yes	Name, DOB, SSN,	Required for processing veteran information	Virtual server in AITC (2)

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 provided by the patient directly to the clinician who enters that into the system.

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.

Information is provided by the patient directly to the clinician who enters the into the system.

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

The system does not create information.

1.3 How is the information collected?

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

No form is used; it is collected in the EAS application itself from the patient by the clinician for demographic and health information and retained in the appropriate database tables.

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

VA Health Clinic clinicians gather patient history and complaint information and store it in EAS so that it may be used for studies of patterns of war-related diseases and in some cases, determination of benefits eligibility. EAS also pulls demographic and health history from the National Patient Care (NPC) database using a one-way connection. Information is collected from NPC and retained in the EAS database table, Health Information is collected from NPC/the patient/VA Health Clinic and retained in the EAS database tables: Agent Orange (AO) Exam, Gulf War (GW) Exam, Gulf War (GW) II Exam, Ionizing Radiation (IR) Exam, Diagnosis, and Symptom.

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 Clinicians input the Veterans information into the application directly.

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.

Information is gathered directed from the patient and entered in the system by the clinician. The patient has access and redress rights and can validate the information.

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

No, the system does not check for accuracy.

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

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

The legal authority to operate the system as well as authority to collect information is: The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38 United States Code, VHA directive 1301 (Ionizing Radiation Registry), Public Laws 102-585 (Veterans Health Care Act of 1992) and 100-687 (Agent Orange Act of 1991), Public Law 102-190 (Gulf War), Public Law 103-445 and VHA Directive 99-019 (Gulf War Dependents), The official System of Records Notices (SORNs) for EAS are:

"Agent Orange Registry" 105VA10P4Q / 85 FR 7407
"Gulf War Registry" 93VA10 / 86 FR 52546
"Ionizing Radiation Registry" 69VA10 / 86 FR 23048

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: The EAS application collects Personally Identifiable Information (PII) and other highly delicate Sensitive Personal Information (SPI). If this information were to be breached or

accidentally released inappropriately, it could result in personal, and/or emotional harm to the individuals whose information is contained in the system.

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.

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 Veteran	Not used
Social Security Number	Used to verify identity of Veteran	Not used
Date of Birth	Used to verify identify of Veteran	Not used
Mailing Address	Used to verify identity of Veteran/Correspondence	Not used
Zip Code	Used to verify identify of Veteran/Correspondence Service Information	Not used
Phone Number	Used to verify identify of Veteran/Correspondence	Not used
Service Information	Used to verify eligibility of Veteran and identified dependents	Not used
Symptoms and Diagnosis	Used to record health history/medical conditions and symptoms of the Veteran.	Not used
Health Information	Used to record health history/medical conditions and symptoms of the Veteran.	Not used

Agent Orange registry	Used to record health history/medical conditions and symptoms of the Veteran	Not used
Gulf War Dependents registry	Used to record health history/medical conditions and symptoms of the Veteran.	Not used
Ionizing Radiation registry	Used to record health history/medical conditions and symptoms of the Veteran.	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?

EAS does not analyze patient data. It does collect and store it for use in war-related diseases and pattern analysis studies. Also, it may be used for studies of patterns of war-related diseases and in some cases, determination of benefits eligibility. The goal for EAS is to provide a structured approach for gathering information on a patient's history, symptoms, and complaints for: Agent Orange registry, Gulf War registry, and Ionizing Radiation registry.

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.

EAS does not analyze patient data. It does collect and store it for use in war-related diseases pattern analysis studies. Also, it may be used for studies of patterns of war related. The goal for EAS is to provide a structured approach for gathering information on a patient's history, symptoms, and complaints for: Agent Orange registry, Gulf War registry, Depleted Uranium registry, and Ionizing Radiation registry.

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 EAS Data is protected by storage level Encryption when it rests, and protected by SSL when the data is in transit.

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

Yes, the last four numbers of the Social Security numbers are scrambled.

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

Safeguarded by storage level encryption when it rests, and protected by SSL when the data is in transit.

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?

All employees with access to Veteran's information are required to have the appropriate level background investigation and must complete the VA Privacy and Information Security awareness training and rules of behavior annually.

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

Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.

2.4c Does access require manager approval?

Individual users are given access to Veteran's data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication.

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

The user's user ID limits the access to only the information required to enable the user to complete their job.

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

The minimum-security controls for the EAS application cover 17 security areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The FFP application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks.

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*

EAS retains Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number, Service Information, Symptoms and Diagnosis, Health Information, Agent Orange Registry, Gulf War Dependents Registry, Ionizing Radiation registry.

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.*

Electronic Data remains in the database permanently. There is no paper record as all interview information is entered electronically. The update schedule for the AO, IR, and GW registries according to the NARA site is to submit five-year blocks. So, EAS should be covered until 2025 by the last update that was submitted. The last transmission was on 8/10/2020 per Aaron Davis the original EASR developer who left the project over 1 year ago.

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

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

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

Yes

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

The data retention schedule is detailed in the VA Record Control Schedule 10-1, dated January 2021. 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.

There is no elimination of SPI; all information is permanent.

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.
All data are stored in encrypted tablespace and in lower environment is redacted.

Techniques for accomplishing the minimization of risk regarding the use of SSNs shall include masking, scrambling, or modification of the SSN. Security plans are continually developed, and security controls implemented on EAS to minimize the use of PII during testing, training and research as in accordance with VA Policies and Directives. VA Directive 6507, Reducing the Use of SSN, VA Directive 6502, Enterprise Privacy Program, VA Directive 6500, Information Security Program.

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: All information is kept permanently.

Mitigation: In order to operate, EAS must meet all security requirements outlined in the Authority to Operation accreditation process. This included continuous monitoring as part of the Continuous Readiness in Information Security Program (CRISP). This includes regular scans and remediation tracking.

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***
Veterans Affairs Central Office (VACO)	Information is used to mail newletters to Veterans.	Name, SSN, Facility Number, Date of Exam, Branch of Service, Exposure Periods, Location, Exposures, Self-Assessment (Health), Birth data, Veterans Children, Consultations for Health Disposition, Symptoms, Diagnoses, ICD Codes	Electronic mailing list containing Veteran name, address and newsletter(s) selected is provided to VACO to mail newsletters.
Veterans Health Administration	Information is used to mail newsletters to Veterans.	Name, SSN, Facility Number, Date of Exam, Branch of Service, Exposure periods,	Provided electronically in a mailing list by VACO or by Veteran to receive.
EAS Agent Orange	Information is used to mail newsletters to Veterans	Location, Exposures, Self-Assessment (Health data), Birth Data, Veterans Children, Consultations for Health Disposition, Symptoms, Diagnoses and ICD Codes.	Provided electronically to requestor or clinician.

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: There is a risk that data contained in EAS may be shared with unauthorized individuals or that those individuals, even with permission to access the data, may share it with other individuals.

Mitigation: Safeguards are implemented to ensure data is not sent to the wrong VA organization and 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. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

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)***
NA			

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: Although EAS does not have any external connections. Privacy information may be released to unauthorized individuals.

Mitigation: All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

EAS adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).
• Information is shared in accordance with VA Handbook 6500.
• All personnel accessing Veteran's information must first have a successfully adjudicated fingerprint check. This fingerprint check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. Individual users are given access to Veteran's data through the

issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication.

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.

The notice is provided to the veteran in writing. The official SORNs for EAS are:

"Agent Orange Registry" 105VA10P4Q / 85 FR 7407

"Gulf War Registry" 93VA10 / 86 FR 52546

"Ionizing Radiation Registry" 69VA10 / 86 FR 23048

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

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

6.1a 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.

During the initial interview process, validation of information is done as the veteran's record is added to EAS.

Individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–6780.

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

Please provide response here
During the initial interview process, validation of information is done as the veteran's record is added to EAS.

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.

During the initial interview process, validation of information is done as the veteran's record is added to EAS.

Individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–6780.

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.

Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (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.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.
Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

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 veterans and other members of the public will not know that the EAS System exists and it process or collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and a System of Record 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.***

During the initial interview process, validation of information is done as the veteran's record is added to EAS.

Individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–6780.

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)?

During the initial interview process, validation of information is done as the veteran's record is added to EAS.

Individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–6780.

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?

During the initial interview process, validation of information is done as the veteran's record is added to EAS.

Individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–6780.

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.

Individuals wishing to obtain more information about access, redress, and record correction for the Environment Agents Service Registries should contact the Department of Veteran's Affairs regional office as directed in the System of Record Notices (SORNs) listed below:
Individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–6780. ""National Patient Databases-VA" (121VA10P2) at http://www.gpo.gov/fdsys/pkg/FR-2010-11-26/pdf/2010-29695.pdf

"Agent Orange Registry" 105VA10P4Q / 85 FR 7407
"Gulf War Registry" 93VA10 / 86 FR 52546
"Ionizing Radiation Registry" 69VA10 / 86 FR 23048

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.

Individuals seeking information regarding access, redress, record correction and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–6780.

"Agent Orange Registry" 105VA10P4Q / 85 FR 7407
"Gulf War Registry" 93VA10 / 86 FR 52546
"Ionizing Radiation Registry" 69VA10 / 86 FR 23048

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.

Individuals seeking information regarding access, redress, record correction and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–6780.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals may not know the steps to take to access or redress the records about them held by the VA and become frustrated with the results of their attempts.

Mitigation: By publishing this PIA and the applicable SORNs listed in Sections 7, the VA makes the public aware of the unique status of applications and evidence files. This document and the SORNs provide points of contact for members of the public who have questions or concerns about applications and evidence files.

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?

Requesting access to EAS Application:

1. Complete the appropriate VA Form 9957. (Click on your role)

   Coordinator
   Clinician

   Coder

   DU Follow-up

   Service Desk

2. Fill in Form 9957 as follows:

   Are you current on your signed Rules of Behavior?
   You must have completed the Cyber Security and Privacy Training submitting this form.

   Type of Access

   Select "OTHER (specify)" and type EAS Registries in the field provided.

   Type of Action Requested

   Select "CREATE NEW CUSTOMER".

   Item A

   Enter your full name including middle initial; this will be used to determine your user ID.

   Item B

   If you already have Time Sharing Option (TSO) access, you will have a user ID already assigned, if not leave blank.

   Item C

   Provide your work phone area code and number.

   Item D

   Provide your facility/station number including suffix.

Item E

Your mail stop code in case any information must be mailed to you.

Item F

Your Job title.

Item G

Leave blank.

Item H

Contractors only.

Item I

Contractors only.

Item J

Provide your Active Directory (AD) Username. If unknown, check with your local IRM.

Item K

Provide your Active Directory (AD) Domain. If unknown, check with your local IRM.

Item L

Provide your work e-mail address.

3. Get all the signatures required to gain the access you need.
4. Submit your 9957 by email to VHAHOMEEASAccount@va.gov
5. Complete the following online registration form: Registration Form
6. You will receive an email notification once your account has been activated.

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?

The EAS is only available to VA users, utilizes VPN for connection to the VA Network, following accessibility guidelines and requiring PIV authorization.

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.

Per VA Directive and Handbook 6330, every 5 years the Office of Information & Technology (OI&T) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

OI&T documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed under the Talent Management System (TMS).

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.

OI&T provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training for new users, when required by system changes and annually thereafter. Each contract is reviewed prior to approval based on the contract guidelines by the appropriate Contracting Officer's Representative. This review is conducted each time the contract period expires.
• Individuals are subject to a background investigation before given access to Veteran's information.
• All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
• VA maintains Business Associate Agreements (BAA) and Non-Disclosure Agreements with contracted resources in order to maintain confidentiality of the information.
• Personnel including contractors that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. 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. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.
• After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS 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.

VA requires Privacy and Information Security Awareness training be completed on an annual basis. The Talent Management System offers the following applicable privacy courses:
VA 10176: Privacy and Information Security Awareness and Rules of Behavior
VA 10203: Privacy and HIPPA Training
VA 3812493: Annual Government Ethics

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

Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* November 1, 2023
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* February 13, 2023
5. *The Authorization Termination Date:* February 13, 2024
6. *The Risk Review Completion Date:* January 12, 2023
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.***

System is already in production.

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)*

System does not use Cloud Technology

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 – System does not use RPA

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.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.01.04 08:31:59 -05'00'

Privacy Officer, Nancy Katz-Johnson

NEIL CRUZ

Digitally signed by NEIL CRUZ
Date: 2024.01.03 12:30:24 -05'00'

Information System Security Officer, Neil Cruz

TEMPERANCE LEISTER

Digitally signed by TEMPERANCE LEISTER
Date: 2024.01.03 08:53:13 -06'00'

Information System Owner, Temperance Leister

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).

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