Privacy Impact Assessment for the VA IT System called:

Enterprise Acquisition System (EAS)

Office of Acquisitions and Logistics

Date PIA submitted for review:

3/17/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.Facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Bernadette Bowen-Welch	Bernadette.bowen-welch1@va.gov	202-340-8970
Information System Owner	Randy Harvel	Randy.harvel@va.gov	501-257-1038

Abstract

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

The Enterprise Acquisitions System (EAS, also known as eCMS or ECC) serves as a data repository for all contract files within the VA. EAS was designed to house all VA procurement and contracting data and provide lifecycle contract management capabilities and processes.

It also provides VA with enterprise-level Business Intelligence (BI) reporting on procurement and contracting activities. The contract files consist of approximately 3 million acquisition records.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

EAS is an integration of proprietary Commercial-of-the-Shelf (COTS) products, existing Government off-the-Shelf (GOTS) software, and custom integration and software to meet VA specific needs.

The EAS information is shared internally with: Veterans Benefit Administration (VBA) and National Cemetery Administration (NCA), Centralized Administrative Accounting Transaction System (CAATS), Office of Acquisition Logistics and Construction (OALC) Construction and Facilities Management (CFM) TRIRIGA, Veterans Health Administration (VHA) Community Liaison Office (CLO); and gathers information from the external General Services Administration (GSA). EAS is a web-based system that serves the entire VA's Acquisition Workforce (approximately 4000 users).

This integration makes up the following components (or subsystems) within the EAS accreditation boundary:

• Automated Acquisition Management System (AAMS)
• Contract Catalog Search Tool (CCST)
• Task Order Management System (TOMS), also called EPIC
• Center for Acquisition Resource Excellence (CARE)
• Acquisition Service Bus (ASB), also called ESB
• Forecast of Opportunities and Requirements Center for Excellence (FORCE)
• MicroStrategy (MS), a reporting tool
• Vendor Portal (VP), a public-facing website
• Electronic Contracting Officer's Representative (eCOR), a hub for CORs
• Ordering Officer Delegation (OOD), nomination and approval workflow
• Electronic Certification (eCERT), serving acquisition workforce
• Suspension and Department (S&D), case management subsystem

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

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

☒ Name
☒ Social Security Number
☐ Date of Birth
☐ Mother's Maiden Name

☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integration Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Other Unique Identifying Information (list below)

Vendor Name, Tax ID Number (Social Security Number SSN), Dollars Obligated and Detailed Line-Item Info.

PII Mapping of Components

Enterprise Acquisition System (EAS) Assessing consists of **one** key component (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Enterprise Acquisition System (EAS) Assessing and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
AAMS	Yes	Yes	Name Vendor number (SAM ID) Mailing Address Zip Code Email Address	Items are often shipped to Veterans for their medical needs.	Access to the system is restricted and access to specific information is limited to need to know.

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

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is collected through a combination of automated and manual processes. Information is automatically received via secured File Transfer Protocol (sFPT); 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.

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

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

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 EAS 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

Title 38, United States Code, section 7301(a). The data service pulls the information directly from VistA. The information cannot be altered, or accuracy check in AAMS.

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.

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?

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: Payroll information, vendor data contains tax id numbers and delivery information could contain individual's names and business addresses. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation: Payroll information not necessary for historical purposes is redacted from documents. Access to the system is limited to need to know only. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA.

Dept. of Veterans Affairs obtain SSN, as Tax ID Number (TINs) within their contracting procedure that Enterprise Acquisition System (EAS) gather as a data repository for all contract files within the VA. Authority: additionally, under the Electronic Code of Federal Regulations- Acquisition Regulations 48 CFR § 4.1103 - Procedures. It states: (d) The contracting officer shall, on contractual documents transmitted to the payment office, provide the unique entity identifier, or, if applicable, the Electronic Funds Transfer indicator, in accordance with agency procedures.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained.
This question is related to privacy control AP-2, Purpose Specification.

- Internal to VA - Name: Used to identify the veteran who contracted item will be delivered. Used to document contractor's employees working on a project.
- Internal to VA - SSN: Tax ID use as contract to identify.
- Internal to VA - Mailing Address: Used delivery point for contracted items.
- Internal to VA - Zip Code: Used delivery point for contracted items.

- Internal to VA – Personal Phone Number use as contract to identify.
- Internal to VA - Vender Name use as contract to identify.
- Internal to VA – Dollar Obligated can be used as contract to identify.
- Internal to VA – Detailed Line-item info can be used as contract to identify.

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

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

No tools are used to analyze data matching, relationship, scoring or pattern analysis for EAS.

2.3 **How is the information in the system secured?**

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

- The EAS data is encrypted at rest and in transit by VAEC and EAS environment's network encryption standards.

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

- General end users do not have access to patient or employee SSN in according with EAS system architecture. End users who need access to such data must request authorization from the information system owner.

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

- The EAS data is encrypted and secured within the VAEC and EAS network with appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

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

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

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Enterprise Acquisition System (EAS) is High Impact that covers 17 security-related areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include:

1) Access control
2) Awareness and training
3) Audit and accountability
4) Certification, accreditation, and security assessments
5) Configuration management
6) Contingency planning
7) Identification and authentication
8) Incident response
9) Maintenance
10) Media protection
11) Physical and environmental protection
12) Planning
13) Personnel security
14) Risk assessment
15) Systems and services acquisition
16) System and communications protection
17) System and information integrity

The EAS 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. VA Records Management Policy and the VA Rules of Behavior recorded in the Talent Management System (TMS), a VA annual training system, govern how veterans' information is used, stored, and protected.

Authorized users of VA IS will be receiving an initial cybersecurity awareness orientation as a condition of access and, thereafter, participate annually in both VA and the Administration's enterprise cybersecurity awareness program. VA will provide VA employees or contractor personnel with cybersecurity awareness education and training to perform their information security-related duties and responsibilities consistent with VA policies, procedures, and agreements. Authorized users will be appropriate in security and privacy training based on the assigned roles and responsibilities of individuals, specific VA security and privacy requirements, and the systems to which personnel have authorized access.

Accounts in different modules are acquired differently. For FORCE self-registration is used but requires application coordinator approval. FORCE has not sensitive data risks. In the contract module AAMS users must receive training before access is given. The training is conducted by AAMS admin, and the account is provisioned and approved.

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

The only information identified in question 1.1 retained by the system are the fields captured in the system audit log. EAS captures specific flagged information in the system log for auditing purposes only. This information is retained to meet the requirements for the accounting for disclosure provisions of the Privacy Act, the HIPAA Privacy Rule, and Freedom of Information Act, which is outlined in VA Handbook 1605.1, Privacy and Release of Information. The information captured in the system log is:

- Name
- Mailing Address
- Zip Code
- Email Address
- Tax ID (SSN)
- Vendor Name

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

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)? If so please indicate the name of the records retention schedule.

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

The VA procedures for eliminating data are available from the VBA Records Control Schedule, VB1. The retention schedule has been approved by the National Archives and Records Administration (NARA). Link: https://www.va.gov/oig/pubs/VAOIG-11-04376-81.pdf or https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc

The VHA Records Officer responsible for the VHA Records Management Office, is the direct manager of that office and is the individual with direct responsibility for ensuring the efficient and appropriate management of the VHA records program and compliance with all applicable records management statutes, regulations, NARA policy, and the requirements of related handbooks and directives.

VHA DIRECTIVE 6300 - https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8113

- 6300 8(d) Appraise each series of records and formulate specific disposition instructions per RCS 10-1 and NARA GRS schedules, including retention periods for temporary records, disposal of non-record material, instructions for the retirement of inactive records to offsite storage facilities, and time periods for transfer of permanent records to the National Archives, when applicable.

National Cemetery Administration (NCA) –
https://www.cem.va.gov/history/sources_records.asp?_ga=2.107677698.1645053245.1554306473-1529059023.1498149304

- By 2012, NCA completely digitized its original burial system: hand-written ledgers from the 1860s to 1960s. Through a partnership with Ancestry.com, NCA's ledgers — along with others in the National Archives & Records Administration (NARA) collection — are available to Ancestry.com subscribers and free to visitors to NARA facilities.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?
This question is related to privacy control DM-2, Data Retention and Disposal

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500 HB 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 6371. 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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

ECC 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.

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 EAS 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: EAS adheres to the VA RCS schedules for each category or data it maintains. ECC 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)." ECC 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 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***
VBA, VHA and NCA CAATS	Provides identification information to EAS in identifying contracts.	Contract information which includes vendor name, tax id number, Web Service Version Date: January 2, 2019, Page 14 of 19 dollars obligated, and detailed line-item info.	Web Service
OALC CFM TRIRIGA	Provides identification information to EAS in identifying contracts.	Contract information which includes vendor name, dollars obligated, and detailed line-item info.	Web Service
VHA CLO's Office	Provides identification information to EAS in identifying contracts.	Contract information which includes vendor name, dollars obligated, and detailed line-item info.	Database view

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining SPI 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: 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***
N/A	**N/A**	**N/A**	**N/A**	**N/A**

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: N/A.

Mitigation: N/A.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.
This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

EAS serves as a data repository for all contract files within the VA. EAS was designed to house all VA procurement and contracting data and provide lifecycle contract management capabilities and processes. It also provides VA with enterprise-level Business Intelligence (BI) reporting on procurement and contracting activities.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:

1) SORN (79VA10) Veterans Health Information Systems and Technology Architecture (VistA) Records-VA provides authority for the Enterprise Acquisition System Assessing (EAS) Assessing system. The SORN is approved and published in the Federal Register and is also available on the VA's public website https://www.oprm.va.gov/privacy/systems_of_records.aspx

2) This Privacy Impact Assessment (PIA) also serves as notice of the PITC Insurance Payment System. 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."

6.2 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

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

EAS uses Contractor Tax ID Number (TIN) to ensure reporting of appropriate value awarded to correct contractor. An individual may register to do business with the 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.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

Follow the format below:

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by ECC prior to providing the information to the ECC.

Mitigation: Mitigation is provided by making the System of Record Notice (SORN) 79VA10 and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

All vendors have access to their information by going to General Service Administration (GSA) and System Award Management (SAM) to gain access to their information. The updated information will be uploaded to EAS overnight. As outlined in SORN 79VA10, 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 Award Management (SAM) to make updates, corrections or erroneous to their information. The updated information will be uploaded to EAS overnight. As outlined in SORN 79VA10, individuals seeking information regarding contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

SORN # 79VA10. Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.oprm.va.gov/docs/Current_SORN_List_10_19_2021.pdf

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

All vendors have access to redress their information by going to General Service Administration (GSA) and System Award Management (SAM) to make updates, corrections or erroneous to their information.

The updated information will be uploaded to EAS overnight. The VA has no control over this. However, still has an obligation to report contract award appropriately.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that the individual accidentally provides incorrect information in their correspondence.

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?

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

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

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

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

Enterprise Acquisition System (EAS) is categorized as High Impact that covers 17 security-related areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include:

1) Access control
2) Awareness and training
3) Audit and accountability
4) Certification, accreditation, and security assessments
5) Configuration management
6) Contingency planning
7) Identification and authentication
8) Incident response
9) Maintenance
10) Media protection
11) Physical and environmental protection
12) Planning
13) Personnel security
14) Risk assessment
15) Systems and services acquisition
16) System and communications protection
17) System and information integrity

The EAS 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. VA Records Management Policy and the VA Rules of Behavior recorded in the Talent Management System (TMS), a VA annual training system, govern how veterans' information is used, stored, and protected.

Authorized users of VA will be receiving an initial cybersecurity awareness orientation as a condition of access and, thereafter, participate annually in both VA and the Administration's enterprise cybersecurity awareness program. VA will provide VA employees or contractor personnel with cybersecurity awareness education and training to perform their information security-related duties and responsibilities consistent with VA policies, procedures, and agreements. Authorized users will be appropriate in security and privacy training based on the assigned roles and responsibilities of individuals, specific VA security and privacy requirements, and the systems to which personnel have authorized access.

Accounts in different modules are acquired differently. For FORCE self-registration is used but requires application coordinator approval. FORCE has not sensitive data risks. In the contract module AAMS users must receive training before access is given. The training is conducted by AAMS admin, and the account is provisioned and approved.

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). 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.

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 electronic signs he/she will abide by 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. OIT 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. 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's TMS.

8.4 Has Authorization and Accreditation (A&A) been completed for the Enterprise Acquisition System (EAS) Assessing.

If Yes, provide:

1. *The Security Plan Status: Active*
2. *The Security Plan Status Date: 25 March 2022*
3. *The Authorization Status: ATO granted*
4. *The Authorization Date: 09 December 2021*
5. *The Authorization Termination Date: 07 June 2022*
6. *The Risk Review Completion Date:01 December 2021*
7. *The FIPS 199 classification of the system: MODERATE.*

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

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

EAS was granted 180 days ATO on 9 Dec 2021 which expires 7 Jun 2022 with a FIPS 199 Classification of Moderate.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

The Enterprise Acquisition System (EAS) is using the VA Enterprise Cloud (VAEC).

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

EAS and VA have ownership rights over data to include PII. Please see the contract between Dell Financial Services and VA. This is the contract that covers the Microsoft Azure Government (Includes Dynamics 365) FedRAMP connection. EAS does not have access to the contract at the project level. VA has access to this contract # VA118-17-F-1888.

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.

All ancillary data is property of the Department of Veterans Affairs.

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, the ultimate accountability for the security and privacy held by the cloud provider on VA's behalf is described in the BAA contract # VA118-17-F-1888.

Department of Veterans Affairs is the owner of all data to include PII for EAS. Please see the contract between Dell Financial Services and VA. This is the contract that covers the Microsoft Azure Government (Includes Dynamics 365) FedRAMP connection. EAS does not have access to the contract at the project level. VA has access to this contract # VA118-17-F-1888.

The primary and backup datacenter are both owned by Microsoft who is a VA contracted cloud service provider (CSP). At those sites with direct connections to the VA Trusted Internet Connection (TIC) from each respective location. The magnitude of potential harm to the VA privacy release data is low to moderate due to the potential of identity theft or unauthorized release of PII. An unauthorized disclosure could negatively affect the reputation of the VA and Microsoft as well as a reduction of public trust.

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).

EAS is not using robotic process automation (RPA) at this time.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2022.04.29 09:31:54 -04'00'

Privacy Officer, Tonya Facemire

Bernadette Bowen-Welch 111245

Digitally signed by Bernadette Bowen-Welch 111245
Date: 2022.04.29 08:59:10 -04'00'

Information Systems Security Officer, Bernadette Bowen-Welch

Randy L Harvel 387406

Digitally signed by Randy L Harvel 387406
Date: 2022.04.29 07:09:10 -05'00'

Information Systems Owner, Randy Harvel

APPENDIX A-6.1 Enterprise Acquisition System (EAS) Assessing.

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).

Enterprise Acquisition System (AES) Assessing, SORN # 79VA10). Veterans Health Information Systems and Technology Architecture (VistA) Records-VA
https://www.oprm.va.gov/docs/Current_SORN_List_10_19_2021.pdf

Link to VA Privacy Website: https://www.va.gov/privacy/