Privacy Impact Assessment for the VA IT System called:

Veterans Affairs Centralized Adjudication Background Investigation System (VA-CABS)

Office of Operations, Security, and Preparedness

Veterans Affairs Central Office (VACO)

Date PIA submitted for review:

5/13/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	gina.siefert@va.gov	(202) 632-8430

	Name	E-mail	Phone Number
Information System Security Officer (ISSO)	Andrew Compton	Andrew Compton@va.gov	405-317-5876
Information System Owner	Tiffiney Benton	Tiffiney Benton@va.gov	980-565-7059

Abstract

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

Veterans Affairs Centralized Adjudication Background Investigation System (VA-CABS) is comprised of the Security Manager Commercial-Off-The-Shelf (COTS) software product deployed within VA Enterprise Cloud (VAEC). VA-CABS leverages common services and security controls available in VAEC through VA Enterprise Cloud Program. VA-CABS solution serves as VA's System of Record and authoritative source for all Background Investigation (BI), re-investigation, and adjudication decision information. In this document, BI and re-investigations are combined under the BI term. VA-CABS provides a centralized repository for all BI and adjudication data. This solution streamlines, automates, and expedites the completion of BI business processes. VA-CABS has a uni-directional interface to the Defense Counterintelligence and Security Agency (DCSA) systems to enable DCSA to push adjudication decisions to VA-CABS via e-Delivery. VA-CABS also has a bi-directional interface to the Identity and Access Management (IAM) Onboarding Solution (OBS) to support data exchanges in support of the BI and Onboarding business processes.

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?*

VA-CABS provides a centralized and holistic solution for BIs, case management, and adjudication for suitability for Employees, Contractors, Trainees, Volunteers, and Affiliates. A collaboration between the Office of Identity, Credential, and Access Management (Business Owner) and the Office of Information Technology, Enterprise Program Management Office (Acquisition, IT, and Sustainment Support), this solution provides fitness determinations for VA subjects in performance of their duties in the service of Veterans and their ability to safeguard VA subjects and Veteran data. The Program Office leverages VA-CABS to implement standardized business rules and processes that significantly enhance the timeliness and efficiency in completing BI and adjudication processes across the VA.

VA-CABS is an enterprise-wide system. In order to align with all current and on-going BIs in the VA and manage the daily increase in investigation numbers, it has the capacity to scale to over 2,000,000 records during its lifetime. For each employee, contractor, affiliate, trainee, and volunteer, VA-CABS creates and maintains a Subject Profile comprised of numerous Personally Identifiable Information (PII) data elements (e.g., Name, Date of Birth, Social Security Number) required to execute BI business processes. In addition, VA-CABS contains case information related to the BI and adjudication processes as part of the overall onboarding process. In accordance with VA standards, the system has been assessed as "High Impact."

VA-CABS receives adjudication decisions from DCSA through its e-Delivery process. [NOTE: DCSA has assumed the BI responsibilities formerly managed by the Office of Personnel Management (OPM.] In addition, VA-CABS receives person and position data elements from the IAM OBS. VA-CABS also provides BI and adjudication decision information back to the OBS.

The system is deployed at two locations: a primary site at the VAEC Cloud located in Virginia and a Disaster Recovery (DR) site at the VAEC in Texas. Data is spooled simultaneously to both locations. In the event of a prolonged or catastrophic loss at the primary site, the DR site will be promoted to the primary site in accordance with the Disaster Recovery Plan implemented and managed by VAEC Team. VA-CABS is hosted in a Federal Risk and Authorization Management Program (FEDRAMP) certified High environment within VAEC. The security controls protecting the PII data within VA-CABS are documented in the approved VAEC Authority to Operate (ATO). VA-CABS leverages the security controls as part of the common services offered by VAEC. The specific security controls leveraged by VA-CABS, in addition to a detailed description of VA-CABS/VAEC security boundaries, are documented in VA-CABS System Security Plan.

Cloud Service Provider and VA-CABS contracts establish VA has ownership rights of all data. Furthermore, the VA-CABS contract stipulates the contractor shall not retain any copies of data in full, or in part, at the completion of the period of performance. The data shall contain no proprietary elements that would preclude VA from migrating the data to a different hosting environment or preclude VA from using a different case management solution. The National Institute of Standards

and Technology (NIST) 800-144 principal stating that "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf" is covered in VA-CABS's VAEC contract documents.

The VA-CABS Business Requirements Document cites the following legal authority references:

- 5 Code of Federal Regulations (CFR) 1400 Designation of National Security Positions in the Competitive Service, and Related Matters, etc.
- 5 CFR 731 – Suitability Actions by OPM & Other Agencies
- 5 CFR 1400 Designation of National Security Positions
- 36 CFR 1194 – Information and Communication Technology Standards and Guidelines
- Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information
- Executive Order 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust
- FEDERAL INVESTIGATIONS NOTICES (FIN 16-02), Federal Investigative Standards for Tier 3 and Tier 3 Reinvestigation
- Homeland Security Presidential Directive 12 (HSPD 12) - Policy for Common Identification Standard for Federal Employees & Contractors
- National Institute of Standards & Technology (NIST) Special Publication 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
- Office of Personnel Management Memorandum for Heads of Departments and Agencies, Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12
- OMB 06-16 Protection of Sensitive Agency Information
- United States Code (USC), Title 5, Government Organization and Employees

This PIA will not result in circumstances that require changes to business processes and is not expected to result in technology changes. The information in this PIA compliments the current business and security processes. VA-CABS is in sustainment, with modifications of minor enhancements and bug fixes. The System of Records Notice (SORN) (145VA005Q3) was created when the system was built. [NOTE: SORN 145VA005Q3 update is in route for concurrence and approval.]

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)

Add Additional Information Collected But Not Listed Above:

- Position Group or Division
- City of Birth
- State of Birth
- Country of Birth
- Country of Citizenship
- Duty Station ID
- Position Title
- VA Supervisor
- VA COR Email (if applicable)
- Effective Date
- Duty Phone Number
- Position Designation Record (PDR)
- Clearance Level
- Security Identified (SEC ID)
- Background Investigation Information
- VA COR (if applicable)

The following information is used by the system, but not retained in the system:

- Report of Investigation, which could include interview responses, criminal history, credit, education, and medical checks

PII Mapping of Components

VA-CABS consists of two key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VA-CABS and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

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
Primary Web Server (Azure PaaS SQL Server)	Yes	Yes	VA Subject Profile Data Elements Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s) Email Address	Background Investigation Business Process	FIPS 140-2 encryption at rest and in transit; HTTPS web connection to database; FEDRAMP certified "High" security controls within VAEC environment; Two factor authentication; Security Manager configured to limit data access according to role and organizational assignments
Disaster Recovery (Azure PaaS SQL Server)	Yes	Yes	VA Subject	Background Investigation	FIPS 140-2 encryption at

			Profile Data Elements Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number(s) Email Address	**Business Process**	**rest and in transit; HTTPS web connection to database; FEDRAMP certified "High" security controls within VAEC environment; Two factor authentication; Security Manager configured to limit data access according to role and organizational assignments**

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.

This system does not create information. The direct sources of the PII data elements within VA-CABS include the following:

- Automated data transfer from the IAM OBS
- Adjudication determinations provided from DCSA via an automated e-Delivery process

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 technology 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.

Automated Data Collection - IAM OBS
USA Staffing's New Hire Interconnection (NHI) supports data transfer with Human Resources (HR) Information Technology systems that handle identity management, credentialing, provisioning, and personnel security processes. Upon receipt of a Tentative Offer transaction from USA Staffing, the IAM OBS creates a Subject Profile for that employee, with the PII data received from USA Staffing, and forwards that profile to VA-CABS. All data is encrypted during this collection process.

Automated Data Collection - DCSA
VA-CABS initiates the BI process. When DCSA completes the adjudication process, DCSA "pushes" the adjudication decision to VA-CABS via the DCSA mandated e-Delivery process, which is an inbound, uni-directional interface from DCSA to VA-CABS.

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.

IAM is the Authoritative Data Source for all identity data within the VA and IAM is responsible for ensuring that all data it receives from HR systems is accurate and complete. DCSA is the Authoritative Source for adjudication decisions. Name, Social Security Number, and Date of Birth are the specific PII data elements used to map and track identity data on the HR side to adjudication decisions on the DCSA side. If there is a discrepancy between IAM and DCSA related to the three data elements cited above, IAM has the action to research where the discrepancy occurred and resolve it with DCSA. VA-CABS is not responsible for remediating any issues related to the accuracy of data received from IAM.

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 authorities that authorize VA-CABS to collect and retain PII are as follows:

- Code of Federal Regulations, Title 5 part 731, Suitability
- Code of Federal Regulations, Title 5 part 1400, Designation of National Security Positions
- Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors
- SORN 145VA005Q3 - Department of Veterans Affairs Personnel Security File System (VAPSFS) - VA

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.

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.

Privacy Risk: If appropriate safeguards are not deployed, then Sensitive Personal Information may be exposed or released to unauthorized individuals.

Mitigation:

- Only data elements required to execute the BI business processes are collected
- VA-CABS does not collect identity or privacy data directly from individuals. VA-CABS receives the data from Authoritative Data Sources authorized to collect the data
- VA-CABS system adheres to information security requirements instituted by VA Office of Information Technology (OIT) and VAEC Program
- All PII data is encrypted during transport and encrypted at rest
- VA-CABS role holders access the data using two factor authentication and a secure (HTTPS) web connection
- VA-CABS System Architecture within the VAEC cloud prevents personnel from outside VA network to access the Virtual Machine resources where the data is stored
- VA-CABS System Categorization Level is High, and the data is stored in a FEDRAMP certified High environment protected by High level security controls
- Both contractor and VA employees are required to take Privacy, Health Insurance Portability and Accountability Act (HIPAA), and information security training annually
- VA-CABS access is granted only to Role Holders with a need to access the data. The total number of Role Holders at the time of initial deployment will not exceed 1,000
- VA-CABS Business Owner defined the software product configuration requirements to customize data access needs for each role holder category, as well as limiting access within organizational boundaries

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.

The following PII data elements from Section 1.1 will be used to complete a VA Subject Profile in support of VA BI Business Processes:

- Name: Used as search criteria to located cases within VA-CABS; Used to map data transfers from DCSA to VA-CABS
- Social Security Number: Used as search criteria to located cases within VA-CABS; Used to map data transfers from DCSA to VA-CABS
- Date of Birth: Used as search criteria to located cases within VA-CABS; Used to map data transfers from DCSA to VA-CABS
- Mailing Address: Used to contact individual
- Zip Code: Used to contact individual
- Phone Number: Used to contact individual

- Email Address: Used to contact individual

The below are used solely to complete a VA Subject Profile and will not be used for any other purpose.

- Gender
- Position Group or Division
- City of Birth
- Effective Date
- State of Birth
- Duty Phone Number
- Country of Birth
- Position Designation Record (PDR)
- Country of Citizenship
- Clearance Level
- Duty Station ID
- Security Identified (SEC ID)
- Position Title
- BI Information
- VA Supervisor
- VA COR (if applicable)
- VA COR Email (if applicable)
- Report of Investigation which could include interview responses, criminal history, credit, education, and medical checks. This information is used to make adjudicative determinations.

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

VA-CABS does not perform data analysis or create data from data analysis. VA-CABS does not create or make available new or previously unutilized information about an individual.

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?

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

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

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

VA-CABS 1.0 is an encrypted secure system. Data and files in transit are protected by HTTPS site-to-site encryption. PII data and files are encrypted at rest via SSE (Server-Side Encryption). SSN is PII data, encrypted at rest via SSE. Additional data encryption is also available depending on the business team requirement. Information from DCSA is secured with additional password encryption so the information is secured in transit.

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.

VA-CABS Business Owner is the Executive Director, Office of Identity, Credential, & Access Management. VA-CABS Business Owner or delegate will determine the individuals that require access to VA-CABS and approve all access. VA-CABS Business Owner or delegate is responsible for managing VA-CABS licenses, which includes tracking the users currently authorized to access the system, removing access privileges for those no longer authorized to access the system, as well as tracking the remaining number of available licenses. In addition, VA-CABS Business Owner or delegate documented the business requirements in VA-CABS Business Requirements Document, which describes how the information in VA-CABS is used to

execute the mission of that office and is responsible for ensuring PII is safeguarded in accordance with VA security standards.

VA-CABS users are categorized into ten different role holder categories that execute different tasks associated with background investigation business use case processes. There is a hierarchy to the role holders and access privileges increase up the hierarchy. Each role holder has specific access privileges within VA-CABS that are limited to the specific data access needs for that role holder. For example, the Security Assistant role has the least data access privileges, and the System Owner role has the most. VA-CABS software product is configured to deny role holders from accessing information beyond the access privileges assigned to their role. VA-CABS training, as well as local instruction from the employee's supervisor, are clear about the uses of information in the background investigation process.

In addition, each VA-CABS user is assigned to a specific Submitting Office Number (SON) and Submitting Office Identifier. Doing so enables VA-CABS software product to further restrict data access to the role holder's specific location. For example, VA-CABS software product prevents a Security Assistant in a Veterans Health Administration facility in VISN 4 from being able to access PII data associated with a VA Subject under the National Cemetery Administration.

A key security control implemented is all VA-CABS data is encrypted at rest and encrypted in transit. This prevents all VA-CABS data from being accessed, or identifiable, by internal and external parties. The only time the data is visible is when and authorized role holder accesses the data via a secure (HTTPS) web connection to VA-CABS product.

The VA-CABS Business Owner has implemented a registration process associated with all role holder access requests. This registration process requires the completion of applicable VA-CABS specific training, as well as completing and maintaining Privacy and HIPAA training. If a VA-CABS role holder's required Privacy training lapses, IT Workforce Development (ITWD) informs the Information Security Officer, who notifies the employee. Disciplinary action for individuals inappropriately using the information can include disciplinary action or termination.

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 following information from Section 1.1 will be retained:
- Name
- Social Security Number

- Date of Birth
- Mailing Address
- Zip Code
- Phone Number
- Email Address

As stated in Section 1.1, the following additional information is collected and retained by the system:

- Gender
- City of Birth
- State of Birth
- Country of Birth
- Country of Citizenship
- Duty Station ID
- Position Title
- VA Supervisor
- VA COR Email (if applicable)
- Position Group or Division
- Effective Date
- Duty Phone Number
- Position Designation Record (PDR)
- Clearance Level
- Security Identified (SEC ID)
- BI Information
- VA COR (if applicable)

3.2 How long is information retained?

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

VA Subject Profile data is required to be retained for seven (7) years from the date VA Subject no longer has a relationship with VA.

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.

VA-CABS complies with all VA retention and disposal procedures specified in VA Directive and Handbook 6300. Records contained in the VA-CABS BI data will be retained for 7 years

after separation or transfer of employee, upon death, or 7 years after contract relationships expires, VA-CABS records are retained according to Record Control Schedule 10-1.

https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

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

In accordance with SORN 145VA005Q3, records are disposed in accordance with Records Control Schedule 10-1 approved by NARA. Records are destroyed upon notification of death or not later than seven years after separation or transfer, whichever is applicable. Paper records are shredded. Electronic records will be permanently deleted from VA-CABS by the System Administrator in accordance with NARA standards.

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

The Business Owner or delegate will screen all VA Role Holders that will have access to the PII data within VA-CABS. Only approved VA Role Holders will have access to VA-CABS data for the sole purpose of conducting BIs to determine the suitability of employees, affiliates, trainees, volunteers, and contractors to perform duties specific to a job or contract. There is currently no VA-CABS requirement or Use Case that approves the use of PII data for testing new applications or information systems. Unless otherwise approved by a senior VA executive, use of PII within VA-CABS for testing new applications or information systems is an inappropriate use of VA-CABS data.

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.

Privacy Risk: If information is retained longer than specified, privacy information may be released to unauthorized individuals.

Mitigation:
The risk associated with the length of time the data is retained is considered minimal. VA-CABS contract requires the system have sufficient capacity to store all data in a single repository. This data repository is VAEC. Consequently, there is no vulnerability risk to having archived records and active records existing in different locations, and there is no risk of the data scaling above the available system capacity. In addition, all data at rest within VA-CABS security boundary is encrypted in accordance with FIPS 140-2, as well as protected by FEDRAMP certified "High" security controls. Collectively, these controls within VA-CABS security boundary provide maximum protection to all VA-CABS data. VA-CABS only retains the required information related to background investigation processes. VA-CABS data retention timeframe is based on NARA requirements.

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***
Identity and Access Management (IAM) Onboarding Service (OBS) / VA Master Person Index (VA MPI)	The OBS creates and updates subject records in VA-CABS. VA-CABS and VA MPI exchange data and VA-CABS sends updates to VA MPI. VA MPI is the authoritative data source for identity data.	Name, SSN, Date of Birth, Mailing Address, Zip Code, Phone Number, Email Address	Encrypted data transfer

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: If appropriate safeguards are not in place, then Privacy information shared within the Department may result in unauthorized data access.

Mitigation:

- Only data elements required to execute the BI business processes are collected.
- VA-CABS does not collect identity or privacy data directly from individuals. VA-CABS receives the data from Authoritative Data Sources authorized to collect the data.

- VA-CABS system adheres to information security requirements instituted by the VA OIT and the VAEC Program.
- All PII data is encrypted during transport and encrypted at rest.
- VA-CABS role holders access the data using two-factor authentication and a secure (HTTPS) web connection.
- VA-CABS System Architecture within VAEC prevents personnel from outside VA network to access the Virtual Machine resources where the data is stored.
- VA-CABS System Categorization Level is High, and the data is stored in a FEDRAMP certified High environment protected by High level security controls.
- Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.
- VA-CABS access is granted only to Role Holders with a need to access the data.
- VA-CABS Business Owner or delegate defined the software product configuration requirements to customize data access needs for each role holder category, as well as limiting access within organizational boundaries.
- Release of PII to unauthorized individuals is prohibited by the Privacy standards mandated to all VA employees, affiliates, trainees, volunteers, and contractors.

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***
Defense Counterintelligence and Security Agency (DCSA) / Personnel Investigations Processing System (PIPS)	DCSA is the authoritative data source for background adjudicative decisions	Social Security Number, DOB, Name, Address, Report of Investigation (which could include interview responses, criminal history, credit, education, and medical checks)	Code of Federal Regulations, Title 5 part 731, Suitability Code of Federal Regulations, Title 5 part 1400, Designation of National Security Positions Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors	Encrypted data transfer via DCSA mandated e-Delivery process

			DCSA OPIS eDelivery - VA - CABS Interconnection Security Agreement (ISA)	

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: If the required data access controls and protocols are not implemented, then the e-Delivery connection to VA-CABS can serve as an entry point to access PII data.

Mitigation:

- DCSA has implemented System Categorization Level "High" security controls for adjudication decision data
- VA-CABS is System Categorization Level "High" and is hosted within the VAEC MAG which has implemented FEDRAMP certified "High" security controls approved in VAEC ATO.
- There is an existing MOU and an existing ISA between VA-CABS Business Owner and DCSA (the successor organization to OPM). The MOU and ISA are maintained over the project lifecycle. VA-CABS is supporting the data transfer protocols and processes dictated by DCSA. These are mature and effective data transfer mechanisms proven to be effective with numerous Government agencies. The data will be encrypted in accordance with FIPS 140-2 during transport. Both ends of the data transfer have a system categorization level HIGH classification.
- VA-CABS does not initiate any data transfers to DCSA using e-Delivery. All data transfers between DCSA and VA-CABS are initiated by DCSA. When DCSA initiates a data transfer action, the action is logged and tracked at DCSA. When VA-CABS receives the data, VA-CABS sends an acknowledgement is sent back to DCSA. If DCSA does not receive an acknowledgement from VA-CABS within many minutes, the DCSA rep contacts VA-CABS counterpart to confirm data receipt or investigate why the confirmation was not received.

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.

VA-CABS has no role in the collection of information directly from persons. Consequently, VA-CABS provides no notice to individuals before collection of information. The collection of data, as well as notices related to the collection of data, are executed through processes that are governed and managed by DCSA and the VA HR department. The information is collected by VA HR and DCSA when an individual applies for a position. Upon receipt of a VA Onboarding Additional Information Form transaction from USA Staffing, VA OBS creates a Subject Profile for that employee and sends it to VA-CABS. VA-CABS neither collects the information directly, nor publishes notices to prospective employees regarding the collection of information.

VA-CABS operates under SORN 145VA005Q3.

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

The rights of individuals to decline to provide information are outside the scope of VA-CABS. These rights are addressed in HR processes and regulations that are governed and managed by DCSA.

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

The right to consent to particular uses of information is outside the scope of VA-CABS. These rights are addressed in HR processes and regulations that are managed and governed by DCSA.

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: If individuals are not provided sufficient notice prior to collection of data or advised appropriately of their rights associated with the collection of data, then individuals could initiate adverse personnel actions against the Government.

Mitigation: Mitigation related to the Principle of Transparency and Principle of Use Limitation are not applicable to VA-CABS because the notice provided to individuals as part of the hiring process is addressed through HR processes that are managed and governed by DCSA. Once VA-CABS receives the required information from the IAM OBS, VA-CABS uses the data solely complete background investigations under the legal authorities cited in the Overview section above.

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.

VA-CABS neither approves, nor grants, individuals with access to their data. Individuals must process all requests for data access through DCSA. If DCSA determines an individual requires access to their data that access will not occur through VA-CABS.

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.

VA-CABS collects data provided by VA HR, IAM OBS, and DCSA. Individuals are not able to access or redress their information directly within VA-CABS. The correction procedures are the same as those given in question 7.1.

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.

VA-CABS collects data provided by HR, IAM OBS, and DCSA. Individuals are not able to access or redress their information directly within VA-CABS. The correction procedures are the same as those given in question 7.1.

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.

VA-CABS collects data provided by VA HR, IAM OBS, and DCSA. Individuals are not able to access or redress their information directly within VA-CABS. The correction procedures are the same as those given in question 7.1.

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.

Privacy Risk: If individuals are not provided sufficient guidance regarding the access, redress, and correction of their data, then individuals could initiate adverse personnel actions against the Government.

Mitigation: VA-CABS cannot implement a mitigation for this risk because access, redress, and correction of information is outside the scope of VA-CABS. Access, redress, and correction notice, rights, and actions are governed by DCSA.

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.

No individuals outside VA will have access to VA-CABS.

VA-CABS Business Owner or delegate will determine the individuals that require access to VA-CABS and approve all access requests. VA-CABS Business Owner or delegate is responsible for managing VA-CABS licenses, which includes tracking the users currently authorized to access the system, removing access privileges for those no longer authorized to access the system, as well as tracking the remaining number of available licenses.

VA-CABS Business Owner or delegate executes a registration process associated with all role holder access requests. This registration process requires the completion of applicable VA-CABS specific training, as well as completing and maintaining Privacy and HIPAA training. Disciplinary action for individuals inappropriately using the information can include disciplinary action or termination.

VA-CABS users are categorized into ten different role holder categories that execute different tasks associated with background investigation business use case processes. There is a hierarchy to the role holders and access privileges increase up the hierarchy. Each role holder has specific access privileges within VA-CABS that are limited to the specific data access needs for that role holder. For example, the Security Assistant role has the least data access privileges and the System Owner role has the most. VA-CABS software product is configured to deny role holders from accessing information beyond the access privileges assigned to their role. VA-CABS training, as well as local instruction from the employee's supervisor, are clear about the uses of information in the background investigation process.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and

Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

Yes, VA contractors will have access to the PII within VA-CABS. VA-CABS solution is a commercial product, called Security Manager. VA contractors are required to deploy and configure the product, provide operations and maintenance for the product and data, as well as perform system administration tasks within the product. These requirements cannot be met unless the contractor has full and open access to its commercial product and the data within the hosting environment. VA project team was aware of this in the project planning phase and incorporated the appropriate PII data protection provisions into the contract.

The performance of the contractor is reviewed quarterly throughout the entire period of performance by the Product Owner, Project Manager and Contracting Officer's Representative. The contract requires adequate security controls for collecting, processing, transmitting, and storing PII must be in place in accordance with VA policies. VA-CABS contract requires contractors to comply with the following:

- The Privacy Act of 1974
- VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Analysis
- VA Handbook 6508.1, Procedures for Privacy Threshold Analysis and Privacy Impact Analysis
- VA Handbook 6500.6 Appendix C, VA Information Systems Security/Privacy Language
- Complete annual HIPAA training
- Accept VA Contractor Rules of Behavior

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-CABS role holders are subjected to same annual privacy and security training requirements as all VA employees. VA-CABS role holders are also required to annually sign Rules of Behavior.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*

3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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.***

The VA-CABS RMF Security Plan was completed on May 3, 2022.

VA-CABS was granted a full, three-year ATO on October 6, 2021. The ATO expires on October 6, 2024.

The VA-CABS Risk Review was completed on May 25, 2022.

The system's FIPS 199 classification is HIGH.

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.

VA-CABS is hosted on the VA Enterprise Cloud (VAEC), which is FedRAMP authorized.

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.

See answer in 9.1.

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.

This is not applicable for VA-CABS. VA has full ownership over the data stored in the VA-CABS cloud. See answer in 9.1.

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.

VA has full authority over data stored in VA-CABS. See answer in 9.1.

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).

VA-CABS 2.0 does not utilize RPA. See answer in 9.1.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Gina A Siefert 273290

Digitally signed by Gina A Siefert 273290
Date: 2022.06.02 08:58:08 -05'00'

Privacy Officer, Gina Siefert

Andrew A. Compton 244894

Digitally signed by Andrew A. Compton 244894
Date: 2022.06.07 12:14:03 -05'00'

Information System Security Officer, Andrew Compton

Tiffiney D. Benton 3555052

Digitally signed by Tiffiney D. Benton 3555052
Date: 2022.06.07 14:25:01 -04'00'

Information System Owner, Tiffiney Benton

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).

This is not applicable to VA-CABS.