Privacy Impact Assessment for the VA IT System called:

Veterans Affairs – Centralized Adjudication Background Investigation System 2.0 (VA-CABS 2.0)

Office of Human Resources and Administration and the Office of Operations, Security, and Preparedness (OSP)

VA Corporate

Date PIA submitted for review:

05/20/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.Drake@va.gov	(202) 632-8431
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000 x4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

The Veterans Affairs Centralized Adjudication Background Investigations System 2.0 is a Salesforce tool which provides the Personnel Suitability and Security (PSS) team with an efficient platform managing pre-appointment, suitability, and security clearance processes to onboard VA employees, contractors, affiliates, trainees, and volunteers. This solution provides a fitness determination for VA subjects in performance of their duties in the service of Veterans and their ability to safeguard VA subjects and Veteran data.

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?*

  Veterans Affairs- Centralized Adjudication Background Investigations Systems 2.0 (VA-CABS 2.0) is owned by Office of Human Resources and Administration and the Office of Operations, Security, and Preparedness (OSP). The Salesforce platform is owned by Office of Information Technology (OIT) as it is a Software as a Service (SaaS) system.

  VA-CABS 2.0 is an enterprise-wide solution. The PII and security controls are inherited from Salesforce Government Cloud Plus platform. The data and files at rest and in transit are encrypted by Salesforce shield encryption. This solution is a modernization of the existing VA-CABS Commercial Off-the-Shelf (COTS) solution which will be decommissioned.

The Salesforce VA-CABS 2.0 tool provides the Personnel Security Specialists (PSS) team with an efficient platform managing pre-appointment, suitability, and security clearance processes for each case. This system will be used to onboard VA employees, contractors, affiliates, trainees, and volunteers. This solution provides a fitness determination for VA subjects in performance of their duties in the service of Veterans and their ability to safeguard VA Subjects and Veteran data. The tool will also provide as a single source for continuous background investigation conducted for each vetted individual through their tenure in VA.

The tool will be utilized by 800-1000 VA employees within the PSS office to adjudicate the suitability of candidates applying for a staff position with Veterans Affairs, as well as those currently on staff. The system receives BI and adjudication decision information from the Defense Counterintelligence and Security Agency (DCSA) and VA Master Person Index (VA MPI).

Although VA-CABS 2.0 data is stored in the Salesforce FedRAMP cloud, it remains the property of the VA and as such, the VA remains responsible for the security and privacy of this data. The VA enforces these protection requirements through the implementation of its cybersecurity policies and the Risk Management Framework (RMF) process. Under the RMF process, the system has a Data Security Categorization of High, with the impacts of a data compromise being identified in the VA-CABS 2.0 Data Security Categorization (DSC) memo. The Privacy Act of 1974 , set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12. 31 CFR § 1.32 - Use and disclosure of social security.

This PIA for VA-CABS 2.0 will not:

- Cause any business processes to change
- Cause any technology changes
- Affect the relevant SORN applicable for the system

The SORN, Department of Veterans Affairs Personnel Security File System (VAPSFS)—145VA005Q3/ 73 FR 15852, covers all Personally Identifiable Information (PII) used in VA-CABS 2.0. The SORN is being updated currently to reflect the CABS tool usage of PII of the individual.

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)

Duty Station ID, Position Title, Position Group or Division, Effective Date, Duty Phone Number, Position Designation Record (PDR), Clearance Level, VA Supervisor, VA Supervisor Email, VA Contracting Officer Representative (COR) (if applicable), VA COR Email (if applicable), Security Identifier (SEC ID), Background Investigation Information, VA Contractor Contact information (i.e., Contract Number and Contract End, if applicable), Court records, list of references, driver's license/ state issued ID, City of Birth, State of Birth, Country of Birth, Country of Citizenship.

PII Mapping of Components

Veterans Affairs – Centralized Adjudication Background Investigations Systems 2.0 consists of 0 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 2.0 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
N/A					

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.

VA-CABS 2.0 receives information from multiple sources such as Master Person Index, communications to Human Resource personnel and DCSA.

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 via electronic transmission from the systems listed in section 1.2.

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.

MPI is the primary system for assigning and maintaining unique person identifiers. MPI is the authoritative identity service within VA, establishing, maintaining and synchronizing identities for all VA persons of interest (e.g. Veterans, beneficiaries, dependents, employees, contractors, health professional trainees). DCSA is the Authoritative Source for adjudication decisions. Specific PII data elements (e.g., Name, Social Security Number, Date of Birth) and identifiers (such as SEC ID) will be used to map and track identity data on the HR side to adjudication decisions on the DCSA side. VA-CABS 2.0 is not responsible for remediating any issues related to the accuracy of data received from the source systems.

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 Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12. 31 CFR § 1.32 - Use and disclosure of social security.

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.

Follow the format below when entering your risk assessment:

Privacy Risk: the information collected by the tool is highly sensitive PII information of the individual. The risk of exposure is very high based on FIPS categorization to the individual's information. There is a potential risk of data being transferred into VA-CABS 2.0 from other systems not being accurate.

Mitigation:

- VA-CABS 2.0 is leveraging Salesforce FedRAMP certified High environment protected by High level security.
- Only data elements required to execute the BI business processes are collected
- VA-CABS 2.0 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 2.0 system adheres to information security requirements instituted by VA Office of Information Technology (OIT), & DCSA.
- All PII data is encrypted during transport and encrypted at rest.
- VA-CABS 2.0 role holders access the data using two factor authentication and a secure (HTTPS) web connection
- VA-CABS 2.0 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 2.0 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
- Users can only see records and fields that are required for them to process adjudication appropriately. VA CABS 2.0 users cannot see their own adjudication and information regarding to their adjudication.
- Inaccurate information of the individuals can be corrected by following the procedures set forth by the source system.

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.

VA-CABS 2.0 collects information of VA employees, contractors, volunteers, and clinical trainees data listed below:

- Social Security Number (SSN): used to validate the identity of the individual.
- First, Last and Middle Name: used for identifying the individual.
- Prefix: used for salutation.
- Gender: used to identify the demographic data and validate the identity of individual.
- Date of Birth (DoB): used to validate the identity of the individual.
- City of Birth: used to validate the identity of individual
- State of Birth: used to validate the identity of individual
- Country of Birth: used to validate the identity of individual.
- External Email Identification: used to contact the individual and primary or secondary means of communication based on preference.
- Home or Contact Phone: used to contact the individual and primary or secondary means of communication based on preference.
- Residential and Local Address: validate the identity and also used as a means of recordkeeping in case the individual is approved to work at VA.
- Country of Citizenship: used to validate the identity of individual
- Duty Station ID: to adjudicate in favor to the individual into the VA
- Position Title: to adjudicate in favor to the individual into the VA
- Position Group or Division: to adjudicate in favor to the individual into the VA
- Effective Date: to adjudicate in favor to the individual into the VA
- Duty Phone Number: to adjudicate in favor to the individual into the VA
- Position Designation Record (PDR): to adjudicate in favor to the individual into the VA
- Clearance Level: to adjudicate in favor to the individual into the VA
- VA Supervisor: to adjudicate in favor to the individual into the VA and validate the information provided by the individual.
- VA Supervisor Email: to adjudicate in favor to the individual into the VA
- VA Contracting Officer Representative (COR) (if applicable): to adjudicate in favor to the individual into the VA
- VA COR Email (if applicable): to adjudicate in favor to the individual into the VA
- Security Identifier (SEC ID): to adjudicate in favor to the individual into the VA
- Background Investigation Information: to adjudicate in favor to the individual into the VA
- VA Contractor Contact information (i.e., Contract Number and Contract End, if applicable): to adjudicate in favor to the individual into the VA

- Mother's Maiden name: to adjudicate in favor to the individual into the VA.
- Financial Account information: to adjudicate in favor to the individual into the VA.
- Certificate/ License Number: to adjudicate in favor to the individual into the VA.
- Current Medication: to adjudicate in favor to the individual into the VA.
- Vehicle license plate number: to adjudicate in favor to the individual into the VA.
- Integration Control Number (ICN): to adjudicate in favor to the individual into the VA.
- Military Service/ connection: to adjudicate in favor to the individual into the VA.
- Court Records: to adjudicate in favor to the individual into the VA.
- List of References: to adjudicate in favor to the individual into the VA.
- Driver's License: to adjudicate in favor to the individual into the VA.

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

Salesforce reporting dashboards are used for reporting metrics to leadership on the adjudicated individuals to the VA. No additional data analysis is done by this tool.

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 2.0 system (Salesforce) 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 with

Salesforce shield encryption. SSN is PII data, encrypted at rest with Salesforce shield encryption. 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.

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for Information Technology [the VA Authorizing Official (AO)]. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored, and protected.

Access Control:
Accessibility to data is granted based on the permission sets and role-based hierarchy applied based on FedRAMP Salesforce Gov Cloud Plus platform. Account creation is managed and offered through VA via two factor authentication (2FA) Personal Identity Verification (PIV) card and/or AccessVA. Single Sign On external (SSOe) is used to provide credential access to VA modules/communities residing in the Salesforce application, the determinant of access is organizational affiliation rather than personal identity. For some module(s) the required organizational e-mail confirmation and multi-factor authentication (MFA) will be enforced (IAL1), but no identity proofing (IAL2) and vice versa. The managers will reject any applications from individuals who do not work with them, do not require access, or are not using

the correct e-mail address. IAM systems verify credential and collect audit logs based on access requested and may contain PII that might have been captured into order to authenticate to the resource. Additionally, VA – CABS 2.0 users cannot see their own adjudication and information relating to their process. User edits to data is captured by the tool.

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

VA-CABS 2.0 collects information of VA employees, contractors, volunteers, and clinical trainees data such as:

Social Security Number (SSN), First Name, Last Name and Middle Name, Prefix, Gender, Date of Birth (DoB), City of Birth, State of Birth, Country of Birth, External Email Identification, Home or Contact Phone, Residential and Local Address, Country of Citizenship, Duty Station ID, Position Title, Position Group or Division, Effective Date, Duty Phone Number, Position Designation Record (PDR), Clearance Level, VA Supervisor, VA Supervisor Email, VA Contracting Officer Representative (COR) (if applicable), VA COR Email (if applicable), Security Identifier (SEC ID), Background Investigation Information, VA Contractor Contact information (i.e., Contract Number and Contract End, if applicable), Mother's Maiden name, Financial Account information, Certificate/ License Number, Current Medication, Vehicle license plate number, Integration Control Number (ICN), Military Service/ Connection, Court Records, List of References, Driver's License/ state issued ID, City of Birth, State of Birth, Country of Birth, Country of Citizenship.

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.

The information is retained following the policies and schedules of VA's Records management Service and NARA in "Department of Veterans Health Administrative Records Control Schedule 10-1". Record Control Schedule 10-1 can be found at the following link: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf. OIT retains audit records for a defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and VA information retention requirements.

As per Personnel Security and Access Clearance Records, there are two retention times for the records. Records of people not issued clearances – Disposition Instructions: Temporary. Destroy one (1) year after consideration of the candidate ends. Records of people clearances – Disposition Instructions: Temporary. Destroy five (5) years after employee or contractor relationship ends, 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 retention schedule for the Salesforce Government Cloud Plus (SFGCP) also applies to VA-CABS 2.0 module.

SFGCP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with National Archives and Records Administration (NARA) approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFGCP records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records)

In addition, as per Record Control Schedule for Personnel Security and Access Clearance Records, follows disposition authority GRS 5.6, item 181, DAA-GRS-2017-0006- 0025 and GRS 5.6, item 180, DAA-GRS-2017-0006- 0024. The SORN applicable for VA-CABS 2.0 is undergoing General Council and OIT approval.

As per the SORN, these records are retained and disposed of in accordance with General Records Schedule 18, item 22, approved by the NARA. Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable.

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

VA-CABS 2.0 tool adheres to the VA RC Schedule 10-1. All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500 https://www.va.gov/vapubs/search_action.cfm?dType=1

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

No PII/live data is used in the VA-CABS 2.0 for research, testing, or training purposes.

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: Depending on the retention time, PII and sensitive information of the individual is at high risk of exposure to unauthorized individuals. The information retained by the system is stored for vetting and adjudication of the individual into the VA and henceforth the continuous background investigation of the vetted individual through their tenure in the VA.

Mitigation: All data at rest within the SFGCP security boundary is encrypted in accordance with FIPS 140-2, as well as protected by FedRAMP certified "HIGH" security controls. Use of FedRAMP HIGH controls implemented under the FedRAMP ATO. Collectively, these controls within the SFGCP security boundary provide maximum protection to all VA Salesforce data.

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***
Master Person Index (MPI)	Validate and process the adjudication for VA employees, contractors, volunteers, and trainees	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 background investigation business processes are collected.
- VA-CABS 2.0 does not collect identity or privacy data directly from individuals. VA-CABS 2.0 receives the data from Authoritative Data Sources authorized to collect the data.
- VA-CABS 2.0 system adheres to information security requirements instituted by the VA OIT.
- All PII data is encrypted during transport and encrypted at rest.
- VA-CABS 2.0 role holders access the data using two-factor authentication and a secure (HTTPS) web connection.
- VA-CABS 2.0 system categorization level is High, and the data is stored in a FedRAMP certified Salesforce 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 2.0 access is granted only to Role Holders with a need to access the data.
- VA-CABS 2.0 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	For adjudication of background investigations for VA Employees, VA Contractors,	Investigation documents, Social Security Number, First Name, Last Name and Middle Name, Prefix, Gender, Date of Birth	National ISA/ MOU and the SORN: Department of Veterans Affairs Personnel	IBM Connect Direct

(DCSA) suite of applications	volunteers, and trainees.	(DoB), City of Birth, State of Birth, Country of Birth, External Email Identification, Home or Contact Phone, Residential and Local Address, Country of Citizenship, Duty Station ID, Position Title, Position Group or Division, Effective Date, Duty Phone Number, Position Designation Record (PDR), Clearance Level, VA Supervisor, VA Supervisor Email, VA Contracting Officer Representative (COR) (if applicable), VA COR Email (if applicable), Security Identifier (SEC ID), Background Investigation Information, VA Contractor Contact information (i.e., Contract Number and Contract End, if applicable), Mother's Maiden name, Financial Account information, Certificate/ License Number, Current Medication, Vehicle license plate number, Integration Control Number (ICN), Military Service/ Connection, Court Records, List of References, Driver's License/ state issued	Security File System (VAPSFS) — 145VA005Q3/ 73 FR 15852. Routine use as per SORN: Disclosure may be made to individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, in order for the contractor, subcontractor, public or private agency, or other entity or individual with whom VA has an agreement or contract to perform the services of the contract or agreement. This routine use includes disclosures by the individual or entity performing the service for VA to	

		ID.	any secondary entity or individual to perform an activity that is necessary for individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to provide the service to VA.	

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: Individual PII information captured in VA-CABS 2.0 is a high risk of exposure to unauthorized personnel. The MOU/ISA between DCSA and VA describes the risk, audit log trails and annual review of audit trails in detail.

Mitigation: eDelivery of the release of investigative documents and results to VA is a dedicated one-way transmission. All VA-CABS 2.0 users with access to the data received from DCSA have been previously authorized by VA to access Office of Personnel Management PIPS Imaging System (OPIS) eDelivery based on a need-to-know and appropriate access privileges granted for the sole purpose of supporting the VA Background Investigation mission. VA personnel or contractor personnel with access to the investigative materials and information provided by DCSA pursuant to this ISA must have the appropriate level of background investigation as required by the Suitability, Credentialing and Security Executive Agent(s). User Access control is managed by strong authentication method and must be assigned on the "Least Privilege" Principal. VA utilizes "two-factor authentication" for general users. Information from DCSA is secured by site-to-site

transcription along with additional password/ token encryption so the information is secured in transit and at rest.

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.

The SORN defines the information collected from VA employees, contractors, volunteers, and clinical trainees, use of the information, and how the information is accessed and stored. SORN for system is: Department of Veterans Affairs Personnel Security File System (VAPSFS) — 145VA005Q3/ 73 FR 15852. (https://www.govinfo.gov/content/pkg/FR-2008-03-25/pdf/E8-5969.pdf)

VA-CABS 2.0 has no role in the collection of information directly from persons. Consequently, VA-CABS 2.0 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 HR processes that are governed and managed by DCSA. The information is collected by 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 2.0. VA-CABS 2.0 neither collects the information directly, nor publishes notices to prospective employees regarding the collection of information.

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 2.0. These rights are addressed in HR processes, Federal hiring process, 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 rights of individuals to consent to particular uses of information are outside the scope of VA-CABS 2.0. The individuals consent to their use of information when initiating a request for federal employment and by providing requested information. Subsequently, individuals are subjected to background investigation conducted by DCSA who captures and maintains individual information. All information acquired by DSCA is passed along to VA-CABS 2.0 which then adjudicates the individuals into the VA. When the individual's objects to the use/collection of their data this results in rescinding the offer of employment/contract with the VA and updated in the DSCA as appropriate.

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 members of the public may not know VA-CABS 2.0 exists within the Department of Veterans Affairs for the adjudication of the individual applicant and henceforth the continuous background investigation of the vetted individual through their tenure in the VA.

Mitigation: The VA mitigates this risk by providing the public with one form of notice that the VA-CABS 2.0 exists through the Privacy Impact Assessment (PIA).
Mitigation related to the Principle of Transparency and Principle Use Limitation are not applicable to VA-CABS 2.0 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 2.0 receives the required information from VA MPI, VA-CABS 2.0 uses the data solely to 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.

As per the SORN, an individual can determine if this system contains a record pertaining to him/her by sending a signed written request to the Systems Manager. When requesting notification of or access to records covered by this Notice, an individual should provide his/her full name, date of birth, agency name, and work location. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to access, such as a government-issued photo ID. Individuals requesting notification via mail or telephone must furnish, at minimum, name, date of birth, social security number, and home address in order to establish identity.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are not able to access or redress their information directly within VA-CABS 2.0. As per the SORN, an individual can determine if this system contains a record pertaining to him/her by sending a signed written request to the Systems Manager. When requesting notification of or access to records covered by this Notice, an individual should provide his/her full name, date of birth, agency name, and work location. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to access, such as a government-issued photo ID. Individuals requesting notification via mail or telephone must furnish, at minimum, name, date of birth, social security number, and home address in order to establish identity. Requesters should also reasonably identify the record, specify the information they are contesting, state the corrective action sought and the reasons for the correction along with supporting justification showing why the record is not accurate, timely, relevant, or complete.

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

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

Records needs to be corrected in the source system. Additionally, per the SORN, an individual can determine if this system contains a record pertaining to him/her by sending a signed written request to the Systems Manager. When requesting notification of or access to records covered by this Notice, an individual should provide his/her full name, date of birth, agency name, and work location. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to access, such as a government-issued photo ID. Individuals requesting notification via mail or telephone must furnish, at minimum, name, date of birth, social security number, and home address in order to establish identity. Requesters should also reasonably identify the record, specify the information they are contesting, state the corrective action sought and the reasons for the correction along with supporting justification showing why the record is not accurate, timely, relevant, or complete

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
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 2.0 collects data provided by MPI and DCSA. Individuals are not able to access or redress their information directly within VA-CABS. Correction will need to occur at the source

system level, the record subject may request Redress through the Privacy Act and Freedom of Information Act (FOIA), in accordance with the source systems SORN.

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: If individuals are not provided sufficient guidance regarding the access, redress, and correction of their data, then individuals could initiate adverse personnel actions against themselves and in their role for supporting government activities.

Mitigation:
Incorrect information will be corrected in VA-CABS 2.0 by notice received from Defense Counterintelligence and Security Agency (DCSA). Individuals will have to reach out to DCSA to get their information corrected. 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.

Only assigned VA users can access VA-CABS. Salesforce uses role-based hierarchy to limit access within the system. Users must use Single Sign On (SSO) and two-factor authentication to log into the VA-CABS 2.0 platform. Additionally, field audit trails and event monitoring provided by the Salesforce platform assists in ensuring only assigned users have access to the specific records on VA-CABS 2.0.

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, data migration and technical support are done with the aid of contractors. Each individual contractor will have to sign an NDA, confidentiality agreement and all addition access forms to clear a background check successfully before they can access the VA-CABS 2.0 system.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

General Training includes VA Privacy and Information Security Awareness and Rules of Behavior, TMS 10203 - Privacy and Health Insurance Portability and Accountability Act (HIPAA), VA on-boarding enterprise-wide training, and information security training annually.

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.***

7. The FIPS 199 classification of the system is High (*High/High/Moderate – C/I/A*).

The VA-CABS 2.0 ATO (ID:2015) is under development and is expected to be awarded prior to Go Live. IOC is 10/30/2022.

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.

Yes, VA-CABS 2.0 system utilizes Salesforce Gov Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This is under the contract: "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus.

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.

Yes, VA has full ownership of the PII that will be used by Dayton VAMC CRM platform under contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B.

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 2.0 tool. VA has full ownership over the data stored in the VA-CABS 2.0 system.

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 2.0.

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.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

JULIE C. DRAKE 969177

Digitally signed by JULIE C. DRAKE 969177
Date: 2022.05.25 12:57:18 -06'00'

Privacy Officer, Julie Drake

James C. Boring 149438

Digitally signed by James C. Boring 149438
Date: 2022.05.25 15:50:50 -04'00'

Information Systems Security Officer, James Boring

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2022.06.03 11:22:13 -04'00'

Information Systems Owner, Michael Domanski

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).

The Privacy Act of 1974 , 5 U.S.C. 552a.

31 CFR § 1.32 - Use and disclosure of social security

SORN: Department of Veterans Affairs Personnel Security File System (VAPSFS) — 145VA005Q3 (https://www.govinfo.gov/content/pkg/FR-2008-03-25/pdf/E8-5969.pdf)

Record Schedule 10-1: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

NARA website link

VA Directive 6500: VA Publication

Privacy Notice information section 6.0

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys,

psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Accept

USA Jobs:

Requirements

Conditions of Employment

- If you are selected, a pre-employment background check is required.
- You must submit a resume and required documents (see How to Apply section).

If you are selected, you will be required to complete a Confidential Financial Disclosure form within 30 days of your first day of employment and annually thereafter.

This position is designated as Moderate Risk and requires a background investigation. Unless an appropriate background investigation is already on record with the Office of Personnel Management, you must undergo a background investigation.

You must meet time in grade requirements no later than 30 calendar days after the closing date of this announcement.

Fair & Transparent

The Federal hiring process is setup to be fair and transparent. Please read the following guidance.

- Equal Employment Opportunity (EEO) Policy
- Reasonable accommodation policy
- Financial suitability
- Selective Service
- New employee probationary period
- Signature and false statements
- Privacy Act
- Social security number request