Privacy Impact Assessment for the VA IT System called:

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

VA Central Office (VACO)

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

eMASS ID #2015

Date PIA submitted for review:

October 22, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	Gina.Siefert@va.gov	(202)632-8430
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000x4613
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 for VA?".

The Veterans Affairs Centralized Adjudication Background Investigations System (VA CABS 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 Privacy Impact Assessment (PIA). A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

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

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 2.0 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.

The SORN, VA (VAPSFS) 145VA005Q3 - Department of Veterans Affairs Personnel Security File System (VAPSFS) —145VA005Q3/ 87 FR 39592. 2022-14118.pdf (govinfo.gov), covers all Personally Identifiable Information (PII) used in VA CABS 2.0.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

VA Controlled / non-VA Owned and Operated

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

The VA CABS 2.0 module contains roughly 600,000 individuals in the system. Individuals could be VA Employees, VA Contractors, Volunteers, and Clinical Trainees.

Check if Applicable	Demographic of individuals
☐	Veterans or Dependents
☒	VA Employees
☒	Clinical Trainees
☒	VA Contractors
☐	Members of the Public/Individuals
☒	Volunteers

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

The information contained in VA CABS 2.0 is used for the background investigations and suitability adjudication of VA employees, contractors, volunteers and clinical trainees.

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

Yes, data is shared with several VA systems (source systems), Identity and Access Management (IAM) Onboarding Service (OBS), Master Person Index (MPI), and Human Resources - Payroll Application Services (HR-PAS).

F. Are the modules/subsystems only applicable if information is shared?

Yes

G. Is the system operated in more than one site to include primary and secondary site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

The system is only operated in one site.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority and SORN to operate the IT system?

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.

The SORN, VA (VAPSFS) 145VA005Q3 - Department of Veterans Affairs Personnel Security File System (VAPSFS) —145VA005Q3/ 87 FR 39592. 2022-14118.pdf (govinfo.gov), covers all Personally Identifiable Information (PII) used in VA CABS 2.0.

I. What is the SORN?

VA (VAPSFS) 145VA005Q3 - Department of Veterans Affairs Personnel Security File System (VAPSFS)

J. SORN revisions/modification

The SORN does not require revision/modification.

K. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

The SORN is not being modified and will not require amendment or revision.

4. System Changes

L. Will the business processes change due to the information collection and sharing?

☐ *Yes*
☒ *No*
if yes,

M. Will the technology changes impact information collection and sharing?

☐ *Yes*
☒ *No*
if yes,

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 Information 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.

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
☒ **Full** Social Security Number
☐ **Partial** Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account Numbers

☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender/Sex
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Date of Death
☐ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI) ☐ Other Data Elements (list below)

Other PII/PHI data elements: City of Birth, State of Birth, Country of Birth, Country of Citizenship, Security Identifier (SEC ID), Alien Registration Number, Passport Number, VISA Number

1.2 List the sources of the information in the system
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

VA CABS 2.0 receives information from multiple source systems: Identity and Access Management (IAM) Onboarding Service (OBS), Master Person Index (MPI), and Human Resources - Payroll Application Services (HR-PAS).

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Information is collected via electronic transmission from various source systems; DCSA, MPI, HR-PAS, IAM, APDS.

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

The system does not create information.

1.3 Methods of information collection

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

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from

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

another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Information is received via electronic transmission from DCSA, HR-PAS, IAM, APDS, and MPI to the VA CABS system.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

Information is not collected on a form; therefore, it is not subject to the Paperwork Reduction Act.

1.4 Information checks for accuracy, and how often will it be checked.

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

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.

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

No, VA CABS 2.0 does not check for accuracy. The accuracy of the information depends on the source system information.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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 VA CABS 2.0 falls 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 number.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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 mitigations are as follows:

- 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 in PIAs of the following source systems: HR-PAS, APDS, DCSA, IAM, and MPI. The SORN Department of Veterans Affairs Personnel Security File System- VA (VAPSFS) 145VA005Q3 is publicly posted and provides the following information: Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	used for identifying the individual.	used for identifying the individual.
Social Security Number (SSN)	used to validate the identity of the individual.	used to validate the identity of the individual.
Gender	used to identify the demographic data and validate the identity of individual.	Not used
Date of Birth (DOB)	used to validate the identity of the individual.	used to validate the identity of the individual.
City of Birth	used to validate the identity of individual	Not used
State of Birth	used to validate the identity of individual	Not used
Country of Birth	used to validate the identity of individual	Not used
Personal Email Address	used to contact the individual and primary or secondary means of communication based on preference.	Not used
Personal Phone Number	used to contact the individual and primary or secondary means of communication based on preference.	Not used

Personal Mailing Address	validate the identity and also used as a means of recordkeeping in case the individual is approved to work at VA.	Not used
Country of Citizenship	used to validate the identity of individual	Not used
Integrated Control Number (ICN)	used to validate the identity of the individual.	Not Used
Security Identifier (SEC ID)	used to validate the identity of the individual.	used to validate the identity of the individual.
Alien Registration Number	used to validate the identity of the individual.	used to validate the identity of the individual.
Passport Number	used to validate the identity of the individual.	used to validate the identity of the individual.
VISA Number	used to validate the identity of the individual.	used to validate the identity of the individual.

2.2 Describe the types of tools used to analyze data and what type of data may be produced.
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

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.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

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 the information in the system is secured.

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

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.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

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.

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

VA CABS 2.0 system (Salesforce) is an encrypted secure system. Data and files in transit are protected by HTTPS site-to-site encryption, allowing for the safeguards of PHI/PII as required by OMB M-06-15.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

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.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

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.

2.4c Does access require manager approval?

Yes, 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.

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

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.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

The ISO and ISSO are responsible for ensuring the safeguards of the sensitive information within VA CAB 2.0.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

Name, Social Security Number (SSN), Prefix, Gender, Date of Birth (DOB), City of Birth, State of Birth, Country of Birth, Personal Email Identification, Personal Phone number, Personal Mailing Address, Country of Citizenship, Security Identifier (SEC ID), Identifying Correlation Number (ICN), Alien Registration Number, Passport Number, VISA Number.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? 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. Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States. Records on government employees and contractor personnel are retained for 5 years after the employee or contractor relationship ends, but longer retention is authorized if required for business use in accordance with General Records Schedule 5.6, item 181. The records on applicants not selected and separated employees are destroyed or sent to the Federal Records Center in accordance with General Records Schedule 5.6, item 180.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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

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

Yes, Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States. National Archives | Home

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

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. Records Control Schedule 10-1 (va.gov)

3.4 What are the procedures for the elimination or transfer of SPI?

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

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. 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. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe policies and procedures for how PII that is no longer relevant and necessary is purged.
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that data within VA-CABS is kept longer than approved retention times. This increases the risk that information can be compromised or breached.

Mitigation: To mitigate the risk posed by information retention, VA-CABS adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, VA-CABS user will submit a support ticket to delete 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.

PII Mapping of Components

4.1a VA CABS 2.0 consists of 0 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VA CABS 2.0 and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Identity and Access Management (IAM) Account Provisioning and Deprovisioning Service (APDS)	Validate and process the adjudication for VA employees, contractors, volunteers, and trainees.	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Personal Email Address, Security Identifier (SEC ID), Country of Citizenship, Alien Registration Number, Passport Number, VISA Number	Encrypted data transfer
Master Person Index (MPI)	Validate and process the adjudication for VA employees, contractors, volunteers, and trainees.	Name, Gender, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Personal Email Address, Identifying Correlation Number (ICN)	Encrypted data transfer

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
Human Resources - Payroll Application Services (HR-PAS)	Validate and process the adjudication for VA employees, contractors, volunteers, and trainees.	Name, Social Security Number (SSN), Date of Birth (DOB), City of Birth, State of Birth, Country of Birth, Personal 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 VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).

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-CABS2.0 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 VAOIT.
- 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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.

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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. 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	For adjudication of	Social Security Number, Name, Date of Birth (DOB),	National ISA/ MOU and the SORN: Department of	Direct Connect (IBM)

and Security Agency (DCSA) suite of applications	background investigations for VA Employees, VA Contractors, volunteers, and trainees.		Veterans Affairs Personnel Security File System (VAPSFS) — 145VA005Q3/ 73 FR 15852. PER the SORN, Routine Use 16 states: Federal Agencies, for Employment: To a Federal agency, except the United States Postal Service, or to the District of Columbia government, in response to its request, in connection with that agency's decision on the hiring, transfer, or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit by that agency.	

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Follow the format below:

Privacy Risk: In sharing information externally, there is a risk of disclosure to unauthorized individuals.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

Information contained within this system is not collected from individuals. All data within the VA-CABS is collected through source systems. Notice before the collection of information is provided by various source systems with the publication of System of Record Notice (SORN) in the Federal Register and the publicly available Privacy Impact Assessment for the source systems.

6.1b If notice was not provided, explain why.

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 APDS 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.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

VA CABS 2.0 has no role in the collection of information directly from persons. Notice before the collection of information is provided by various source systems with the publication of System of Record Notices (SORN) in the Federal Register and the publicly available Privacy Impact Assessment for the system.

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. The right to decline to provide information would be provided by the source system. Individuals communicating with the VA do have the opportunity and right to decline to provide information. However, failure to provide requested identifying information will affect the adjudication and hiring process.

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 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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

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

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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 Principal 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 The procedures that allow individuals to gain access to their information.
These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

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.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

This system is not exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

This system is a Privacy Act system. Per the SORN an individual can request information regarding him/her by sending a signed written request to the Systems Manager. Access to VA (VAPSFS) 145VA005Q3 - Department of Veterans Affairs Personnel Security File System (VAPSFS) —145VA005Q3/ 87 FR 39592. 2022-14118.pdf (govinfo.gov), covers all Personally Identifiable Information (PII) used in VA CABS 2.0.

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. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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.*** *(Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their 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: Individuals seeking to contest or amend records in this system should contact the source system manager in writing as indicated in the applicable SORN. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

Only assigned VA users can access VA CABS 2.0. 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.

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

Users from other agencies do not have access to VA CABS 2.0.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Persona	Access Level
Case Manager Persona	*Read + Edit Access*
Compliance Specialist Persona	*Read + Edit Access*
Insider Threat Reviewer Persona	*Read + Edit Access*
PSAC Members persona	*Read + Edit Access*
Read-Only Reviewer Persona	*Read Only*
Security Assistant Persona	*Read + Edit Access*
Security Specialist Persona	*Read + Edit Access*
Senior Security Specialist Persona	*Read + Edit Access*

System Owner persona	*Read + Edit Access*
Module Support persona	*Read + Edit Access*

8.2a. Will VA contractors have access to the system and the PII?

Yes

8.2b. What involvement will contractors have with the design and maintenance of the system?

The contractors will design, build, and provide technical support for the system.

8.2c. Does the contractor have a signed confidentiality agreement?

Yes

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

Unknown

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
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 CABS 2.0 contract is currently expiring January 3rd 2025. Clearance is required for VA Contractors as to address issues with the production environment to better provide support for the users and the application.

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.

All users with access to VA Systems are required to complete VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176).

Additionally VA employees and contractors who have access to Protected Health Information (PHI) are also required to complete Privacy and HIPAA Focused Training (VA TMS ID: 10203).

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* APPROVED
2. *The System Security Plan Status Date:* 11/13/2023
3. *The Authorization Status:* Authority to Operate
4. *The Authorization Date:* 12/28/2023
5. *The Authorization Termination Date:* 12/27/2025
6. *The Risk Review Completion Date:* 12/27/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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

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

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

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 Hosting 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 VA CABS 2.0 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

ID	Privacy Controls
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.

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2024.11.14 09:55:07 -06'00'

Privacy Officer, Gina Siefert

JAMES BORING Digitally signed by JAMES BORING
Date: 2024.11.14 07:29:59 -05'00'

Information Systems Security Officer, James Boring

MICHAEL DOMANSKI Digitally signed by MICHAEL DOMANSKI
Date: 2024.11.13 16:05:45 -05'00'

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; screen shot of a website collection privacy notice).

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)