Privacy Impact Assessment for the VA IT System called:

Personnel Security Investigations Portal (PSIP)

Veterans Benefits Administration

Office of Human Capital Services

eMASS ID # 1798

CAM ID# AP0020815

Date PIA submitted for review:

12/29/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.harvey@va.gov	314-964-5469
Information System Security Officer (ISSO)	Joseph Facciolli	Joseph.facciolli@va.gov	215-842-2000 x2012
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 Personnel Security Investigation Portal (PSIP) is a secure internal web-portal that will be used to capture required background investigation submissions for VA
Contractors to be processed by the VBA Personnel Security Office. The system allows VA Contractors or Employees such as Contracting Officer's Representative (COR) with PIV cards to submit an individual background investigation request with documentation. Once the information is submitted, it is then transmitted to the business line supervisor who subsequently will assign the request to a Personnel Supporting Specialist (PSS) to begin processing the background investigation request.

The data captured in this tool will be integrated with the VA Centralized Adjudication Background Investigation System (VA-CABS) to share relevant PII and adjudication data as appropriate. The PSIP collects data such as name, other name(s), social security number (SSN), date of birth (DOB), current and former addresses, phone numbers, personal email address and other PlI information from VA employees and contractors. In addition, security documentation will be saved to PSIP as a repository which will include any court proceedings, credit reporting, selective service records and other applicant identifying information. Additionally, PSIP consumes investigation update data from VA-CABS via the Digital Transformation Center (DTC) Integration Platform (DIP) - CABS Broker API and notifies PSIP users when background information has been updated. This integration is facilitated via the reuse of the CABS broker application hosted on DIP.

This Salesforce tool will facilitate as a metric for tracking, reporting, applicant status, and monitoring the background verification requests from intake to completion for increased visibility by CORs and VA leadership. This system intends to alleviate missed packets (submissions), duplicate entries, streamline processes as well as allow PSS to keep better track of their assigned cases. The tool is intended to streamline all intake at the Veterans Service Organization (VSO) level rather than being at the local POC level. In addition, this tool allows affiliate applicants access to determine background status through external access.

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?

PSIP is a secure internal web-portal that will be used to capture required background investigation submissions for VA Contractors to be processed by the VBA Personnel Security Office.

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.

PSIP is a VA-owned Salesforce-controlled system built on the Salesforce Government Cloud Plus (SFGCP) platform for the Office of Human Capital Services.

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?

There are approximately 200,000 projected individuals' information stored in the system.

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?

Personnel Security Investigation Portal (PSIP) is a secure internal web-portal that will be used to capture required background investigation submissions for VA Contractors to be processed by the VBA Personnel Security Office. The system allows VA Contractors or

Employees such as Contracting Officer's Representative (COR) with PIV cards to submit an individual background investigation request with documentation. Once the information is submitted, it is then transmitted to the business line supervisor who subsequently will assign the request to a Personnel Supporting Specialist (PSS) to begin processing the background investigation request. The data captured in this tool will be integrated with the VA Centralized Adjudication Background Investigation System (VA-CABS) to share relevant PII and adjudication data as appropriate. This Salesforce tool will facilitate as a metric for tracking, reporting, applicant status, and monitoring the background verification requests from intake to completion for increased visibility by CORs and VA leadership. The tool is intended to streamline all intake at the Veterans Service Organization (VSO) level rather than being at the local POC level. In addition, this tool allows affiliate applicants access to determine background status through external access.

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

Personal Identifiable Information (PII) data will be shared with VA Centralized Adjudication Background Investigation System (VA-CABS). PSIP consumes investigation updated data from VA-CABS via the Digital Transformation Center (DTC) Integration Platform (DIP) - CABS Broker API.

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?

PSIP is a single cloud-based platform operated from one site that shares information with VA-CABS which also is a single cloud-based platform in which both systems utilize the Salesforce cloud platform and its governance.

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

H. What is the citation of the legal authority?

145VA005Q3 / 87 FR 39592 Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA
https://www.govinfo.gov/content/pkg/FR-2022-07-01/pdf/2022-14118.pdf
Executive Orders 9397, 10450, 10865, 12333, and 12356; 5 U.S.C 3301 and 9101; 42 U.S.C 2165 and 2201; 50 U.S.C 781 to 887; 5 C.F.R 5, 732, and 736; and Homeland Security Presidential Directive 12.

146VA005Q3 / 73 FR 16093 Department of Veterans Affairs Identity Management System
(VAIDMS)-VA

https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf
5 U.S.C. 301; 38 U.S.C. 501; 40 U.S.C. 11331; 44 U.S.C 3544; Executive Order 9397; Homeland Security Presidential Directive 12; Federal Information Processing Standard 201–1.

I. What is the SORN?

145VA005Q3 / 87 FR 39592 Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA

146VA005Q3 / 73 FR 16093 Department of Veterans Affairs Identity Management System
(VAIDMS)-VA

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

No amendment or revision and approval required.

4. System Changes

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

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

- ☒ Name
- ☒ **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
- ☐ 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: Place of Birth, Other Name(s), Current & Former Mailing Address (City, Country Code, Postal Code, State Code), Resume, Criminal History, Financial & Credit Report (Fall under Financial information), Fingerprinting Location, Related Background Investigation (BI) Case, Investigation and Adjudication Information (status, case ID, date, name), eAPP Register Number, Individual Tax Identification Number (ITIN), Salesforce ID, Suffix and Prefix, User ID, and Contact ID.

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?

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

The information is collected directly from the individual.

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.

The individual is the source of system. PSIP is a secure internal web-portal that will be used to capture required background investigation submissions for VA Contractors to be processed. PSIP will share with VA-VABS for Personnel Supporting Specialist (PSS) team to perform with their assigned background investigation.

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

Yes

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 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?

PSIP tool is an internal web-portal for VBA Personnel Security Office. VA Employees, Contractors, affiliates with PIV card will be able to submit the request on behalf of the applicant. The information is collected through email.

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?

The individual's information is not collected on a paper form. There is no OMB control number and agency form number.

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.

The information is collected directly from the individual who is submitting for a position. The CORs review information for accuracy. Application alert sent if data is incorrect in comparison to the data in VA-CABS. The system does not check against another source of information. If the information is incorrect, the data will be rejected. The COR then contacts the individual and validates the discrepancy of information depending on the rejection.

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

No, the system does not check for accuracy by accessing a commercial aggregator of 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

145VA005Q3 / 87 FR 39592, Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA

- Executive Orders 9397, 10450, 10865, 12333, and 12356; 5 U.S.C 3301 and 9101; 42 U.S.C 2165 and 2201; 50 U.S.C 781 to 887; 5 C.F.R 5, 732, and 736; and Homeland Security Presidential Directive 12.

146VA005Q3 / 73 FR 16093, Department of Veterans Affairs Identity Management System (VAIDMS)-VA

- 5 U.S.C. 301; 38 U.S.C. 501; 40 U.S.C. 11331; 44 U.S.C 3544; Executive Order 9397; Homeland Security Presidential Directive 12; Federal Information Processing Standard 201–1.

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: 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: VA Contractors information is at risk of exposure. The information is collected directly from the individual or via an email request. Without the information of the contractor, it would be difficult to track the applicants and/or applications for a VA contractor position. The program tries to collect information directly from the VA contracts with PIV card. Contractors with no PIV card can submit a request in PSIP portal with the aid of a VA employee/ Contracting Officer's Representative (COR) submitting on their behalf.

Mitigation: The information exchange is through a site to site encrypted with Transmission Layer Security. Only a VA Employee, COR or assigned Contractor with PIV card will be able to submit a request.

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
First and Last Name	Used as an identifier	Internal
Date of Birth (DOB)	Used as an identifier	Internal
Place of Birth	Used as an identifier	Internal
Other Name(s)	Used as an identifier	Internal
Current & Former Mailing Address	Used as an identifier	Internal
Personal Email Address	Used as an identifier	Internal
Personal Phone Number	Used as an identifier	Internal
Full Social Security Number (SSN)	Used as an identifier	Internal
Resume	Used to assess the candidate's eligibility for the applied	Internal

	position required document for hiring	
Criminal History	Used to validate the credibility of the individual required additional document for hiring Financial standing	Internal
Financial Standing & Credit Report	Used to validate the credibility of individual	Internal
Medication & Drugs	Used to assess the health conditions of the individual	Internal
Fingerprint Location	used to validate the location where the candidate provided the fingerprint required for hiring.	Internal
Race/Ethnicity	Used as an identifier	Internal
Medical Records		Internal
Internal Control Number (ICN)	Used as an identifier	Internal
Related Background Investigation (BI) Case	Used as an identifier	Internal
Investigation and Adjudication Information (status, case ID, date, name)	Used to accurately update and track BI Case records within PSIP, ensuring key adjudication milestones are reflected downstream.	Internal
eAPP Register Number	Used as an identifier	Internal
Individual Tax Identification Number (ITIN)	Used as an identifier	Internal
Mother's Maiden Name	Used as an identifier	Internal
Salesforce ID	Used as an identifier	Internal
Suffix and Prefix	Used as an identifier	Internal
User ID	Used as an identifier	Internal
Date of Death (DOD)	Used as an identifier	Internal
Contact ID	Used as an identifier	Internal

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 Government Cloud Plus Enterprise (SFGCP-E) is used to track the data in the system. Based on the data entered by the contractor or COR with PIV card, the information will be used to track the application progress of the VA contractor applicant.

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.

Information from CABS (via DIPs) will be used to accurately update and track BI Case records within PSIP, ensuring key adjudication milestones are reflected downstream.

Access and use of such information will be governed by role-based access controls, need-to-know principles, and applicable privacy and data protection policies.

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?

PSIP is an encrypted secure system. Data in transit are protected by HTTPS encryption. PII data are encrypted at rest with Salesforce Shield encryption. VA CORs, VA Employees and Contractor POCs will have access to applicants on their specific contract only.

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).

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

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

No additional protection requirements as outlined in the OMB memoranda.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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?

VA Contractors - A Company POC (designated Contracting Company BI Submitter) will submit through the portal to the VA Employee COR. The COR will submit the request to Personnel Security. This request is transmitted to the business line supervisor responsible who will assign these requests to Personnel Security Specialist (PSS). PSSs are VA employees with PIV card who can access the PII information of the individual.

VA Affiliates- VA Employee, CMA with a PIV Card will submit the request in the portal. This request is transmitted to the business line supervisor responsible who will assign these requests to Personnel Security Specialist (PSS). PSSs are VA employees with PIV card who can access the PII information of the individual.

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?

Yes, the criteria and procedures are documented. We are using Persona Tracker, which helps manage and document access-related responsibilities. In addition, there is a SOP that is stored on the PSS SharePoint Site

2.4c Does access require manager approval?

Yes, access must be approved by the individual's manager or Contracting Officer's Representative (COR) through the formal request process before it is granted.

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

Yes, history tracking is enabled. All access to PII is logged and monitored according to VA's security and compliance policies, ensuring auditability and accountability.

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

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 Access VA. All users are required to complete the security awareness training thus ensuring that they are aware of their role and responsibility in safeguarding PII, with the oversight of the ISO, ISSO and Privacy Officer.

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*

- First Name and Last Name
- Date of Birth (DOB)
- Place of Birth
- Other Name(s)
- Current & Former Mailing Address (City, Country Code, Postal Code, State Code)
- Personal Email Address
- Phone Number
- Full Social Security Number (SSN)
- Resume
- Criminal History
- Financial Standing & Credit Report
- Medication & Drugs
- Fingerprint Location
- Race/Ethnicity
- Medical Records
- Internal Control Number (ICN)
- Related Background Investigation (BI) Case
  Investigation and Adjudication Information (status, case ID, date, name)
- eAPP Register Number
- Individual Tax Identification Number (ITIN)
- Mother's Maiden Name
- Salesforce ID
- Suffix and Prefix
- User ID
- Date of Death (DOD)

- Contact ID

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 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 and NARA in "Department of Veterans Affairs 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

GRS 5.6, item 181, DAA-GRS-2017-0006-0025 - Personnel Security Clearance Files. The information is destroyed upon notification of death, or not later than 5 years after separation or transfer or employee, or no later than 5 years after contract relationship expires, whichever is applicable.

Records relating to persons covered by this system are retained in accordance with General Records Schedule 18, Item 17. Unless retained for specific, ongoing security investigations, and in accordance with NARA, all of the PIV collected data will be retained for a minimum of 7.5 years beyond the term of employment, unless otherwise directed. In accordance with HSPD–12, PIV Cards are deactivated within 18 hours from the notification time for cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by shredding, typically within 90 days after deactivation.

GRS 5.6, item 120, DAA-GRS2017-0006- 0016 - Personal Identification Credentials and Cards. Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use.

GRS 5.6, item 130, DAA-GRS2017-0006- 0018 - Local Facility Identification and Card Access Records. Destroy upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner, but longer retention is authorized if required for business use.

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?

The retention schedule for the Salesforce Government Cloud Plus – Enterprise (SFGCP - E) also applies for PSIP module.

Personnel Security Clearance Files 312-1, Personnel security clearance case files created under Office of Personnel Management (OPM) procedures and regulations and related indexes maintained by the Security Management Division (BX). Disposition type/ authority follows GRS 2.2 item 181.

Credentials Files 649-1. Identification credentials including cards, badges, photographs, and property; visitors' passes; and other identification credentials. Disposition type/authority follow GRS_5-6 -120, 130

[NARA website link]

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

The information is retained following the policies and schedules of VA's Records management Service and NARA in "Department of Veterans Affairs 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

GRS 5.6, item 181, DAA-GRS-2017-0006-0025 - Personnel Security Clearance Files. The information is destroyed upon notification of death, or not later than 5 years after separation or transfer or employee, or no later than 5 years after contract relationship expires, whichever is applicable.

Records relating to persons covered by this system are retained in accordance with General Records Schedule 18, Item 17. Unless retained for specific, ongoing security investigations, and in accordance with NARA, all of the PIV collected data will be retained for a minimum of 7.5 years beyond the term of employment, unless otherwise directed. In accordance with HSPD–12, PIV Cards are deactivated within 18 hours from the notification time for cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by shredding, typically within 90 days after deactivation.

GRS 5.6, item 120, DAA-GRS2017-0006- 0016 - Personal Identification Credentials and Cards. Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card 6 years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use.

GRS 5.6, item 130, DAA-GRS2017-0006- 0018 - Local Facility Identification and Card Access Records. Destroy upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner, but longer retention is authorized if required for business use.

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.

PSIP follows the standard VA policy in disposal of digital data, following the guidelines identified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-81, Revision 2. Since these procedures change with the storage technology and medium being used, PSIP personnel consult SP 800-81R2 and additional OIS guidance prior to disposing of digital data.

Additionally, all records will be destroyed as per the Records Schedules and NARA retention guidance described. Data can be deleted per business requirement. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), https://www.va.gov/vapubs. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), https://www.va.gov/vapubs. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.

Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization."

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.

PSIP does not use PII for research, testing or training.

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 in 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: The retention risk pertains to the PII and PHI information of the individuals being at risk of exposure due to the quality of data available. There is a risk that unauthorized personnel will attempt to access the data without permission.

Mitigation: To mitigate the risk posed by information retention, PSIP 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 650

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 **Personnel Security Investigation Portal (PSIP)** consists of **4** 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 **PSIP** 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

Salesforce Government Cloud Plus – Enterprise (SFGCP-E)	Yes	Yes	First and Last Name, Date of Birth (DOB), Place of Birth, Other Name(s), Current & Former Mailing Address (City, Country Code, Postal Code, State Code), Personal Email Address, Phone Number, Full Social Security Number (SSN), Resume, Criminal History, Financial Standing & Credit Report, Medication & Drugs, Fingerprint Location, Race/Ethnicity, Medical Records, Internal Control Number (ICN), Related Background Investigation (BI) Case, Investigation and Adjudication Information (status, case ID, date, name), eAPP Register Number, Individual Tax Identification Number (ITIN), Mother's Maiden Name, Salesforce ID, Suffix and Prefix, User ID, DOD, Contact ID	To validate the contractor information applying for a VA contractor position.	VA Identity and Access Management Programs and mandatory annual Privacy, HIPAA, and information security training.
ID.me	Yes	Yes	First and Last Name, DOB, Full SSN	Veteran identification verification	VA Identity and Access Management Programs and mandatory annual Privacy, HIPAA, and information security

					training.
Master Person Index Enterprise (MPIe)	Yes	Yes	First and Last Name, Personal Email Address	Veteran identification verification	VA Identity and Access Management Programs and mandatory annual Privacy, HIPAA, and information security training.
DTC Integration Platform (DIP) - VA Centralized Adjudication Background Investigation System (VA-CABS) Broker API	Yes	Yes	First and Last Name, DOB, Place of birth, Other Name(s), Current & Former Mailing Address (City, Country Code, Postal Code, State Code), Personal Email Address, Phone Number, Full SSN, Resume, Criminal History, Financial standing & Credit report, Medication & Drugs, Fingerprint location, Investigation and Adjudication Information (status, case id, date, name), DOD, eAPP Register Number, ICN, Individual Tax Identification Number (ITIN), Mother's Maiden Name, Phone Number, Contact ID	To check on the application status.	HTTP with TLS encryption, TIC port

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

NOTE: Question 3.9b (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. l

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 systemi***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Master Person Index Enterprise (MPIe)	MPI does not share information. It is used to verify identification verification.	First and Last Name, Email Address, Full SSN, ICN	Site-to-site Encrypted Transmission
VA Centralized Adjudication Background Investigation System (VA-CABS)	To share relevant PII and adjudication data as appropriate for candidates security review.	Related BI Case	One way data transmission from DIP-CABS Broker API using Salesforce APEX integration

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 systemi*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
DTC Integration Platform (DIP)	A middleware platform to allow data transfer.	First and Last Name, DOB, Place of Birth, Other Name(s), Current & Former Mailing Address (City, Country Code, Postal Code, State, Code), Personal Email Address, Phone Number, Full SSN, Resume, Criminal History, Financial standing & Credit report, Medication & Drugs, Fingerprint location, Investigation and Adjudication Information (status, case id, date, name), eAPP Register Number, ICN, Individual Tax Identification Number (ITIN), Mother's Maiden Name, Salesforce ID, Suffix and Prefix, User ID, Contact ID	VA CABS data transmitted through DIP middleware is consumed by Salesforce-PSIP. DIP does this through Java Springboot application. This process combines HTTPS/TLS/HTTP

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: There is a potential loss of information due to theft or destruction with the sharing of information.

Mitigation: Every internal system with which PSIP shares data has an Authorization to Operate (ATO) that describes how PII and PHI are to be protected. Through Continuous Monitoring, data is protected in accordance with the security and privacy controls outlined in their System Security Plans (SSPs) and VA policies and procedure.

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.

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 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***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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: There is no external sharing.

Mitigation: There is no external sharing.

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.

The SORNs define the information collected from Veterans, use of the information, and how the information is accessed and stored

145VA005Q3 / 87 FR 39592, Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA

146VA005Q3 / 73 FR 16093, Department of Veterans Affairs Identity Management System (VAIDMS)-VA

This Privacy Impact Assessment (PIA) also serves as notice of the system. As required by the eGovernment Act of 2002, Pub.L.107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." It can be found at this website: https://www.oprm.va.gov/privacy/pia.aspx.

6.1b If notice was not provided, explain why.

Notice is provided as detailed above in 6.1

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

The notice provided at the time of collection meets the purpose of use for this system by explicitly informing users about the nature and scope of the data being collected, its intended uses, and the relevant constraints. This ensures transparency and compliance with legal and regulatory requirements regarding data privacy and protection. The notice helps users understand the context and limitations of the system's use.

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.

No, the individual cannot decline if they are in consideration for a VA Contractor position.

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.

Yes, the individuals have the right to consent to particular use of information. If there is any inconsistency in the information provided by the individual, they consent to be contacted by the COR. The information provided by the individual will be used to track their consideration for a VA Employee/ Contractor position.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

Principle of Transparency: 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: As PII and PHI information of the contractors are gathered, there is a potential risk of exposure of the individual identity.

Mitigation: VA contractors applying for the position are informed about their PII/PHI collection when completing relevant forms such as SF-85 and fingerprint request. All data is encrypted at a database level as per FIPS 140-2 encryption.

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.***

Applicants will not have access to the secure system. Application forms will be signed by applicant. They will have the opportunity to view information and check for accuracy prior to submission and uploading into the portal by the VA COR or Employee.

Individuals may submit a FOIA request by visiting www.foia.gov; then searching for the Department of Veterans Affairs, and then navigating to the Veterans Health Administration (VHA) and following the prompts. An alternate method would be to send an email to the VHA FOIA Public Liaison at vhafoiahelp@va.gov, or by calling +1 (833) 880-8500.

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)?

PSIP is not exempt from 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?

PSIP is a Privacy Act System.

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

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

VA CORs and VA employees will be able to self-correct erroneous inputted information along with uploading any documents/forms relevant to the applicant in the secure portal.

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.

Within the PSIP system, the PSS will notify the VA COR/Contractor POC that the record is to be returned for correction. The VA contractor POC informs the VA contractor applicant through the preferred choice of communication.

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 Contracting POC will notify applicants if information needs to be amended.

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: The individual submitting for a VA Contractor/ VA employee position is aware the system does maintain a record. Inaccurate information can be readdressed by the individual. The individual needs to provide accurate information through email.

Mitigation: The information provided by an individual is not being used for other purposes. Only a COR and PSS will have access to the individual. All data is encrypted.

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?

Salesforce provides permission to different items and objects which should prevent individuals that should not have access to have access. Access to the PSIP portal is granted using a PIV card for validation by select VA Employees including CORs and PSS staff, along with Contractor POCs who have been designated by the COR to upload, update, and access the portal.

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?

There are no other agencies accessing the system.

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.

Roles	**Access Type**
COR (Contractor Officer Representative) / BI Submitter	Can Create and Edit contractor Case and Applicant records.
VSO (Veteran Service Officers) Users	Can Create and Edit affiliate Case and Applicant records.
HR Users	Can Create and Edit employee case and Applicant records.
PSS Users (Personnel Security Specialists)	1. Have access to all record types (contractor, employee, and affiliate) BI Case and BI Applicant. 2. Can create and Edit employee and affiliate BI Case and Applicant records. 3. Can Edit Contractor BI case records 4. Can work on cases tied to specific case types assigned to their employee record.
PSS Supervisors	1. Have access to all record types on BI Case and Applicant. 2. Can create and Edit employee and affiliate BI Case and Applicant records. 3. Can Edit Contractor BI case records 4. Can assign PSS users to All case RecordTypes.
PERSEC Project Manager (PM)	1. Has access to all record types on BI Case and Applicant. 2. Can create and Edit employee and affiliate BI Case and Applicant records. 3. Can Edit Contractor BI case records

	4. Can assign PSS users to All case RecordTypes.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Yes, the contractor has a signed non-Disclosure Agreement in place.

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?

Office of Information and Technology (OIT) Contractors will have access for the duration of the contract for development, deployment, and any enhancements. VA contractors including system integrators, DTC and possibly from the Contract being managed by the COR will have access to the development and production environments. VA Contractors are required to complete the Privacy and Information Security Agreement yearly, also known as the Rules of Behavior. Signing the Rules of Behavior ensures proper conduct and management of sensitive information.

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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's Talent Management System 2.0 (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS 2.0 system.

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

8.4a If completed, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 07/24/2024
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 07/24/2023
5. *The Authorization Termination Date:* 07/24/2026
6. *The Risk Review Completion Date:* 02/15/2024
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 not completed 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. ***(Refer to question 1.8 of the PTA)***

Yes, PSIP utilizes Salesforce Government Cloud Plus – Enterprise (SFGCP-E) and it is hosted in the AWS GovCloud. The SFGCP-E is built on the underlying Salesforce.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This software utilizes the PaaS Service of SFGCP-E.

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). ***(Refer to question 3.3.1 of the PTA)*** *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 shared through the PSIP platform. Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B, Order Number: 36C10B9F0460. CLIN SWF-5700

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.

Yes, VA has full ownership of the ancillary data stored in the 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.

The cloud service provider does not collect ancillary data.

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).

No robotic process automation (RPA) is used in this system.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

MARVIS HARVEY

Digitally signed by MARVIS HARVEY
Date: 2026.02.17 07:30:43 -06'00'

Privacy Officer, Marvis Harvey

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2026.02.25 11:44:34 -05'00'

Information System Security Officer, Joseph Facciolli

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2026.02.24 11:32:53 -05'00'

Information System 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).

145VA005Q3 / 87 FR 39592, Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA

146VA005Q3 / 73 FR 16093, Department of Veterans Affairs Identity Management System (VAIDMS)-VA

This Privacy Impact Assessment (PIA) also serves as notice of the system. As required by the eGovernment Act of 2002, Pub.L.107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." It can be found at this website: https://www.oprm.va.gov/privacy/pia.aspx.

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)