Privacy Impact Assessment for the VA IT System called:

Salesforce: Personnel Security Investigations Portal (PSIP)

Veterans Benefits Administration

Office of Mission Support

Date PIA submitted for review:

10/05/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Chiquita Dixon	Chiquita.dixson@va.gov	(202) 632-8923
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000 x4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

The 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. This Salesforce tool will facilitate as a metric for tracking, reporting, and monitoring the background verification requests from intake to completion for increased visibility by Contracting Officer's Representative (CORs) and VA leadership. This system intends to alleviate missed packets (submissions), duplicate entries, streamline processes as well as allow Personnel Supporting Specialist (PSS) to keep better track of their assigned cases. The tool is intended to streamline all the intake at the Veterans Service Organization (VSO) level rather than being at the local Point of Contact (POC) level.

The system allows VA Contractors or Employees such as 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 PSS to begin processing the background investigation request. The data captured in this tool will be extracted and manually fed into the VA Centralized Adjudication Background Investigation System (VA-CABS). In addition, security documentation will be saved to the repository which will include any court proceedings, credit reporting, selective service records and other applicant identifying information.

Overview

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

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

- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

Salesforce: Personnel Security Investigations Portal (PSIP) is owned by the Veteran Benefits Administration Office of Mission Support. The Salesforce platform is owned by Office of Information Technology (OIT) as it is a Software as a Service (SaaS) system.

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.

This Salesforce tool will facilitate as a metric for tracking, reporting, 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 Personnel Support Specialists (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.

The PSIP collects data such as full name, social security number (SSN), date of birth (DOB), current and former addresses, phone numbers, email id and other PII information from VA Contractors. In addition, security documentation will be saved to the repository which will include any court proceedings, credit reporting, selective service records and other applicant identifying information. The tool is said to be used by up to 300 users.

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 Support Specialist (PSS) to begin processing the background investigation request. The data captured in this tool will be extracted and manually fed into the VA Centralized Adjudication Background Investigation System (VA-CABS).

PSIP tool will be used only at the VBA Office of Mission Support for supporting CORs at the Office of Administration and Facilities. This tools success metrics will facilitate the future expansion to other facilities such as Talent Management Office.

This tool is a standalone and has no interconnections to other modules.
Although PSIP data is stored in the Salesforce FedRAMP Government 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 Categorization of High, with the impacts of a data compromise being identified in the PSIP Data Security Categorization (DSC) memo. The Privacy Act is the legal authority to utilize this information.

PSIP system will not

- Cause any business processes to change,
- Cause any technology changes, nor
- Affect the relevant SORN applicable for the system mentioned below. The SORN covers all Personally Identifiable Information (PII) used in PSIP.
    - Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA 145VA005Q3/ 73 FR 15852
    - Department of Veterans Affairs Identity Management System (VAIDMS)-VA 146VA005Q3/73 FR 16093).

Section 1. Characterization of the Information

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Current Medications
- ☒ Previous Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Other Unique Identifying Information (list below)

Place of Birth, Other names, Former Address, Resume, Criminal History, Financial Standing and Credit report, Fingerprint location.

PII Mapping of Components

Salesforce: Personnel Security Investigations Portal consists of one key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Salesforce: Personnel Security Investigations Portal** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Salesforce Gov Cloud Plus	Yes	Yes	First Name, Last Name, Date of Birth (DOB), Place of birth, Other Names, Current & former address, Email ID, Phone Number, Social Security Number, Resume, Criminal History, Financial	To validate the contractor information applying for a VA contractor position.	Site to site encrypted with transmission Layer Security (TLS) 1.2

			standing & Credit report, Medication & drugs, Fingerprint location		

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

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

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

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

The information collected by the Personnel Security Investigations Portal (PSIP) is provided by the VA contractors being submitted for a contractor position. This information is directly collected from the individual.

1.3 How is the information collected?

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

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

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

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

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

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

The CORs review information for accuracy. If information is incorrect data will be rejected to COR to resolve. The COR then contact the individual and validate the discrepancy of information depending on the rejection.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation, use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under

- 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.
- 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.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:
Privacy Risk: 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 will be used in support of the program's business purpose.

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

VA Contracts information is collected by the PSIP tool.
First and Last Name: Used as an identifier
Date of Birth (DOB): used as an identifier
Place of birth: used as an identifier
Other Names: used as an alternate identifier
Current & former address: used as an identifier
Email ID: used to contact the individual
Phone Number: used to contact the individual and alternate identifier
Social Security Number: used as an identifier
Resume: used to assess the candidate's eligibility for the applied position required document for hiring
Criminal History: used to validate the credibility of the individual required additional document for hiring
Financial standing & Credit report: used to validate the credibility of individual
Medication & drugs: used to assess the health conditions of the individual
Fingerprint location: used to validate the location where the candidate provided the fingerprint required for hiring.

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

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

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

Salesforce Gov Cloud Plus 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.

2.3 How is the information in the system secured?

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

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

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

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

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

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>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.</u>

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

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

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

VA Contractors with PIV card or VA Employee/COR with PIV will submit the request in the portal. This request is transmitted to the responsible business line supervisor who will assign these requests to Personnel Supporting Specialist (PSS). PSS are VA employees with PIV card who can access the PII information of the individual.

Section 3. Retention of Information

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

3.1 What information is retained?

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

The information retained of the VA contractor are:
First Name, Last Name, Date of Birth (DOB), Place of birth, Other Names, Current & former address, Email ID, Phone Number, Social Security Number, Resume, Criminal History, Financial standing & Credit report, Medication & drugs, Fingerprint location.

3.2 How long is information retained?

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

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

The information is retained following the policies and schedules of VA's Records management Service and NARA in "Department of Veterans 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 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

The retention schedule for the Salesforce Government Cloud Plus – 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]

3.4 What are the procedures for the elimination of SPI?

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

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

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.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The

proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

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

Follow the format below:
Privacy Risk: 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.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.10 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

There is no data being shared internally with PSIP tool.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
N/A			

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:
Privacy Risk: There is a potential loss of information due to theft or destruction with the sharing of information. PSIP is a standalone tracking system which doesn't connect to other system/ modules.

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 procedures.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.11 on Privacy Threshold Analysis should be used to answer this question.
Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A				

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

No additional protection requirements as outlined in the OMB memoranda.

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

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

Follow the format below:
Privacy Risk: N/A

Mitigation: N/A

Section 6. Notice

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

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

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

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

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

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

Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA
https://www.oprm.va.gov/privacy/systems_of_records.aspx).
145VA005Q3/ 73 FR 15852.

Department of Veterans Affairs Identity Management System (VAIDMS)-VA
https://www.oprm.va.gov/privacy/systems_of_records.aspx).
146VA005Q3/73 FR 16093

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 <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.

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

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

Follow the format below:
Privacy Risk: 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 What are the procedures that allow individuals to gain access to their information?

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

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

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

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.

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 inform 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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

VA Contracting POC will notify applicant 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.

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

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

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

Follow the format below:
Privacy Risk: 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 either through email

Mitigation: The information provided by 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.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

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

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

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

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

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.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

Content is granted to those who submit applicant's information only. CORs will have visibility because of their role to supervise the contract, as well as the Contractor. 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 Has Authorization and Accreditation (A&A) been completed for the system?

If Yes, provide:

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

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

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

The FIPS 199 classification of the system is HIGH (C/I/A – H/H/M).

PSIP falls under the Salesforce Government Cloud Plus -Enterprise (SFGCP -E) ATO. The ATO process is in flight - IOC 12/02/2021

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, 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.

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

Yes, PSIP system utilizes Salesforce Gov Cloud Plus. The controls under Salesforce Gov Cloud Plus is inherited by the module. Salesforce Gov Cloud already has a FedRAMP authorization -E package.

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

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

This software utilizes the PaaS Service of Salesforce Gov Cloud Plus.

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

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

Yes, VA has full ownership of the PII that will be used by PSIP platform. The contract agreement with CSP has clearly defined that the data utilized by the tool is still under the ownership of VA and within the VAEC boundary.

9.4 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.

No ancillary data is collected by this module.

9.5 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

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

Yes, it is, as VA is utilizing Salesforce Gov Cloud Plus. Information is only shared internally.

9.6 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).

PSIP tool does not utilize RPA.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Chiquita Dixson 126558

Digitally signed by Chiquita Dixson 126558
Date: 2021.10.18 14:58:57 -04'00'

Privacy Officer, Chiquita Dixon

James C. Boring 149438

Digitally signed by James C. Boring 149438
Date: 2021.10.19 07:44:48 -04'00'

Information Systems Security Officer, James Boring

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2021.10.21 10:27:29 -04'00'

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).

OPRM website for SORN: https://www.oprm.va.gov/privacy/systems_of_records.aspx

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

NARA website link