Privacy Impact Assessment for the VA IT System called:

Salesforce - VHA Recruitment Marketing CRM (SF-VHARM)

Veteran Health Administration

Workforce Management Consulting (WMC)

eMASS ID #: 2568

Date PIA submitted for review:

02/04/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Harash Katyal	harash.katyal@va.gov	908-864-3107
Information System Security Officer (ISSO)	Joseph Facciolli	joseph.facciolli@va.gov	215-842-2000 Ext: 2012
Information System Owner	Michael Domanski	michael.domanski@va.gov	727-482-1398

Abstract

The abstract provides the simplest explanation for "what does the system do for VA?".

Salesforce - VHA Recruitment Marketing CRM (SF-VHARM) system is hosted in VA Line of Business. (VALOB) org. This tool will function as a Candidate Relationship Management (CRM) tool that will enable VA Careers to capture, retain, and analyze historical information about candidates, enabling follow-up with promising candidates. This tool will facilitate a seamless candidate journey that makes it easier to express interest and enables VHA to nurture high-quality potential hires through automation. The tool will enable recruiters with the ability to identify promising candidates who have not applied or were not selected on their first application.

SF-VHARM has an external facing interest form that sits on a Salesforce Experience site, which allows candidates to submit basic Personal Identity Identification (PII) information without the need to authenticate. The web portal can be accessible on a mobile. Candidate information is then stored in SF-VHARM and utilized for marketing of opportunities and upcoming campaigns. Internal users accessing SF- VHARM, such as sources will be able to identify promising candidates for opportunities in VHA.

The tool will include analytical capabilities to support data queries, filtering, and visualizations, along with the ability to develop dashboards and reports (using CRM Analytics). The tool will include a master dashboard that enables ongoing understanding of VHA's candidate pipeline across priority positions by stakeholders.

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?

This tool will facilitate a seamless candidate journey that makes it easier to express interest and enables VHA to nurture high-quality potential hires through automation. The tool will enable recruiters with the ability to identify promising candidates who have not applied or were not selected on their first application.

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.

Salesforce Government Cloud Plus (SFGCP) is a cloud platform, data in the platform is controlled by VA but non-VA Owned and Operated. Ownership rights to PII data should be covered in the Salesforce contract. Per NIST 800-144, it is understood that the organization (VA) is ultimately accountable for security and privacy of data held by Salesforce on our behalf.

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?*

Expecting to be upwards to 2,500,000 individuals whose information is stored in the system, the system is being used to store information for candidates who are interested at some of level of applying to the Veteran's Health Administration, both clinical and non-clinical; therefore, the number will be high. SF-VHARM anticipates access to less than 30 internal users and no authentication needed for external personnel since they do not have access to the application.

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

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

The CRM is going to store basic personal information about the candidates and their interest in working at the VHA and in what capacity/preference on type of location. The CRM is designed to effectively manage and organize prospective candidate data and will serve as a centralized hub for storing information related to them so the VHA can effectively market to them over time through email communications and newsletters.

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

SF-VHARM has an external facing interest form that will sit on an experience site (no authentication for external users) which allows candidates to submit basic PII information. The interest form is a web portal that can be accessible on a mobile as well. Candidate information is then stored in SF-VHARM.

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

Yes

G. Is the system operated in more than one site to include primary and secondary site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?
The CRM will employ an external web portal with cloud computing available for external personnel, and an internal application with cloud computing accessible only to authorized users. The external interest form is a web portal that will be accessible on mobile as well.

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

H. What is the citation of the legal authority?

Applicants for Employment Under Title 38, USC-VA
02VA135(https://department.va.gov/privacy/wp-content/uploads/sites/5/2023/05/SORNsPriorto1995.pdf)

The SORN for the system provides the authority for maintenance of the system: Executive Order 12564; Urgent Relief for the Homeless Supplemental Appropriations Act of 1987; Pub.L.100-71, section 503, 101 Stat. 468 (1987); and Title 38, United States Code, Chapter 3,section 210(c)(1); Chapter 73, section 4108 and Chapter 75, section 4202.

I. What is the SORN?

02VA135, Applicants for Employment Under Title 38, USC-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.

Yes, the SORN Point of Contact (POC) is notified.

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: Veteran or Dependents Occupation, City, State, Area of Interest (location), Specialty, Employment Interest, Veteran Status. VA employee/VA Contractors username, login email,

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

Members of the Public/Individual Occupation, City, State, Area of Interest (location), Specialty, Employment Interest, Veteran Status.

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?

The information is collected from the individual candidates applying for available VHA positions.

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.

Refer to 1.2a.

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

Yes, the system will create reports/dashboards using the before mentioned data elements. Veteran or Dependents, Members of the Public/Individuals Name, Email, City, State, Area of Interest (location), Specialty and VA employees Name and User login Email.

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?

Means of collection is from the VHA candidate filling out the interest form.

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 information is not collected on paper.

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 collected from the individual candidate is only to learn their interest and general information, the data will live in a secure site. There is no matching in place to check accuracy.

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.

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

Applicants for Employment Under Title 38, USC-VA 02VA135
(https://department.va.gov/privacy/wp-content/uploads/sites/5/2023/05/SORNsPriorto1995.pdf)

The SORN for the system provides the authority for maintenance of the system: Executive Order 12564; Urgent Relief for the Homeless Supplemental Appropriations Act of 1987; Pub. L. 100-71, section 503, 101 Stat. 468 (1987); and Title 38, United States Code, Chapter 3, section 210(c)(1); Chapter 73, section 4108 and Chapter 75, section 4202.

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: Collecting PII involves several risks, including unauthorized access, data breaches legal non-compliance, and misuse of data. These risks can lead to significant consequences such as financial loss, reputational damage, and legal penalties.

Mitigation: Collecting PII involves several risks, which we mitigate through various measures. Data minimization, robust consent mechanisms, and encryption protect PII. Access controls and a data retention policy limit exposure, while employee training ensures proper handling. Audit trails and an incident response plan (through ATO) provide accountability and swift breach response. Regular security assessments keep protections up-to-date, collectively enhancing data privacy and security.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Identify potential candidate	Internal
Email	Identify potential candidate and used for communication	Internal
City	Identify potential candidate	Internal
State	Identify potential candidate	Internal
Occupation	Identify potential candidate	Internal
Areas of Interest (location)	Identify potential candidate	Internal
Specialty	Identify potential candidate	Internal
Employment Interest	Identify potential candidate	Internal
Veteran Status	Identify potential candidate	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 will identify duplicate entry by email address, a contact record is created when a new user submits an interest form.

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 is more marketing purposes only; duplicate records will be merged to one record. Once a contact record has been created, if they want to make any changes to their interest form, they will have to update the entire form again so that PII is not being brought out of the CRM onto the public-facing form.

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?

SF-VHARM is an encrypted secure system. Data in transit are protected by HTTPS site-to site encryption. PII data are encrypted at rest with Salesforce Shield encryption.

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).

This does not apply, SF-VHARM is not collecting SSN.

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

Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. Personnel 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.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Users are provided access to PII only on a need-to-know basis to execute/ facilitate a work tracking request within the SF-VHARM application. Assignment by PM/COR, internal users will have VA access background and identification PIV. Profile based settings is applicable to the tool limiting the type of information accessed by individual users authenticated by PIV Single Sign On (SSO). Additionally, the SORN defines the use of the information and how the information is accessed, contained, and stored in the system.

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?

Access to the SF-VHARM system is requested by the employee's supervisor and approved by the system owner through Digital Transformation Center (DTC). All users will be required to authenticate to the system with a PIV card and will only have permissions to perform their assigned function. Based upon that function, each user will only have access to information on those participants which are assigned to them by their manager. The system will perform extensive logging to detail all actions taken by a user. Some of these actions are (but not limited to):

1) Logon / Logoff
2) Create Data
3) Update Data
4) Delete Data

2.4c Does access require manager approval?

Yes, supervisor/manager approval is required for accessing SF-VHARM application.

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

Yes, Profile-based setting available in Salesforce is leveraged for users access in SF-VHARM application. User have limited access to PII information captured in the tool and access is monitored using logging details available through Salesforce cloud technology.

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

SF-VHARM is accessed via a secured webpage utilizing SSO technology. SF-VHARM CRM is housed in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there. Accessibility to data is granted based on the permission sets and profile-based settings is 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. Single Sign On external (SSOe) is used to provide credential access to VA modules/communities residing in the Salesforce application, the determinant of access is organizational affiliation rather than personal identity. For some module(s) the required organizational e-mail confirmation and multi-factor authentication (MFA) will be enforced (IAL1), but no identity proofing (IAL2) and vice versa. The managers will reject any applications from individuals who do not work with them, do not require access, or are not using the correct e-mail address.

Additionally, The SF-VHARM Privacy Officer, Information System Security Officer, and Information System Owner will be responsible for maintaining all safeguards are put in place to protect PII and other sensitive information.

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*

VHA Recruitment Marketing CRM retains the following inform: Name, Personal Email Address, Veteran or Dependents Occupation, City, State, Area of Interest (location), Specialty, Employment Interest, Veteran Status. VA employee/VA Contractors username, login email, Members of the Public/Individual Occupation, City, State, Area of Interest (location), Specialty, Employment Interest, Veteran Status.

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.

1004.2 Temporary. Destroy no sooner than 6x years after the project, activity, or transaction is completed/superseded, but longer retention is authorized if needed for business use.

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

1. Item Number: 3010.5, Job Vacancy Case Files suggest Disposition Instruction: Temporary. Destroy 2 years after termination of register.
2. Item Number: 3050.13, Recruitment Records with Disposition Instruction: Temporary. Destroy when 1 year old, but longer retention is authorized if required for business use.
3. Item Number: 3015.13 Employee Drug Test Results with Disposition Instruction: Temporary. Destroy when employee leaves the agency or when 3 years old, whichever is later.

Alternately, the SORN also provides the same information, Records are retained in accordance with records retention standards approved by the Archivist of the United States, the National Archives and Records Administration, and published in VA Records Control Schedules. Records arising in connection with employee drug testing under Executive Order 12564 are generally retained for up to 2 years. Records are destroyed by shredding or burning.

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

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

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

Yes, the information in RCS 10-1 & NARA is adhered by application SF-VHARM. The retention schedule for the Salesforce Government Cloud Plus (SFGCP) also applied SF-VHARM module.

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

Following are the retention schedule information apply,
Per RCS 10-1,

1. Item Number: 3010.5, Job Vacancy Case Files suggest Disposition Instruction: Temporary. Destroy 2 years after termination of register. Disposition Authority: GRS 2.1, item 051 DAA-GRS-2014-0002-0007.

2. Item Number: 3050.13, Recruitment Records with Disposition Instruction: Temporary. Destroy when 1 year old, but longer retention is authorized if required for business use. Disposition Authority: GRS 2.1, item 180 DAA-GRS-2018-0008-0003.
3. Item Number: 3015.13 Employee Drug Test Results with Disposition Instruction: Temporary. Destroy when employee leaves the agency or when 3 years old, whichever is later. Disposition Authority: DAA-GRS-2017-0010-0019, item 130 and DAA-GRS 2017-0010 0020, item 131.

Per NARA,

1. Series# 207, Routine Administrative (Non-Mission) Records Common to All Offices. Disposition Instruction: Temporary DAA-0064-2015-0003 Item 1. Cut off at end of fiscal year in which the project/activity/transaction was completed or superseded. Destroy 7 years after cutoff. Disposition Authority: DAA-0064- 2015-0003-0001.

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

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.

Paper retention policy specific to department/ tool.

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

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training, and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

SF-VHARM does not use PII of the potential candidate information/ VA-Employee/ VA-Contractor information 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: Retaining data for extended periods in a SF CRM increases the likelihood of unauthorized access, data breaches, and compliance violations with privacy regulations. It can also lead to outdated or irrelevant information begin stored, potentially compromising data quality and integrity.

Mitigation: These risks underscore the importance of implementing a clear data retention policy that ensures PII is only kept for as long as necessary and deleted when no longer needed; policy will be to delete or destroy after six years.

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 Salesforce - VHA Recruitment Marketing CRM (SF-VHARM) consists of 2 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 Salesforce - VHA Recruitment Marketing CRM (SF-VHARM) consists 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 (SFGCP)	Yes	Yes	Name, Email, City, State, Occupation, Area of Interest (location), Specialty, Employment Interest, Veteran Status	Salesforce Government Cloud Plus (SFGCP) is a cloud platform, in which the system was built on and leverages the database to collect and store information.	Salesforce - VHA Recruitment Marketing CRM (SF-VHARM is a minor system hosted on the cloud SFGCP platform, which is FedRAMP certified and has security controls in place for safeguarding the data stored.
CRM-A	Yes	Yes	Candidate Users Name, Email, City, State Occupation, Area of Interest (location), Specialty, Employment Interest, Veteran Status	Collecting basic candidate information in CRMA facilitates efficient data analysis and reporting, which will help VHA exercise data-driven decision-making to continue improving their	Collecting basic candidate information in CRMA facilitates efficient data analysis and reporting, which will help VHA exercise data-driven decision-making to

				processes and campaigns over time	continue improving their processes and campaigns over time security training.

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.

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

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
N/A	N/A	N/A	N/A

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: Sharing information about data stored within a SF CRM, within the department can lead to unauthorized access and potential misuse of sensitive data, increasing the risk of privacy breaches and non-compliance with data protection regulations.

Mitigation: To mitigate these risks, we enforce strict access controls (role-based) ensuring that only authorized personnel can access specific data based on their job responsibilities. We also ensure data encryption, provide regular employee training on data privacy, and maintain detailed audit logs to monitor data access and sharing activities.

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: Sharing information with an external tool that will be sending emails to candidates based on triggers from the CRM, poses privacy risks. These risks include unauthorized access, data breaches, and potential misuse of email addresses by third parties, which can lead to phishing attacks, spam, and non-compliance with data protection regulations.

Mitigation: To mitigate the risk, we ensure that there are data sharing agreements in place with the external vendor, ensure the tool complies with strict data protection standards, implement end-to-end encryption for data transfers, and establish secure API connections. Additionally, we regularly audit the external tools security practices.

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.

Notice is provided to candidates in three ways:

1. *Disclaimer in the Interest Form filled by the candidate states* –
   "Thank you for your interest in a career with the U.S. Department of Veterans Affairs (VA)! By completing the registration form below, you will be added to VA's Candidate Relationship Manager (CRM), which may help VA match your job interests with VA opportunities. Please complete as much of the form as possible. Thank you again for your desire to serve our country's Veterans! DISCLAIMER: While registering in VA's CRM provides VA the ability to recruit you in the future, this process does not guarantee you will be contacted by VA or considered for future employment."

2. The SORNs defines the information collected from *Veterans or Dependents/ VA Employees/ Contractors/ Members of Public*, use of the information, and how the information is accessed and stored. *02VA135, Applicants for Employment Under Title 38 USC-VA*

3. *This Privacy Impact Assessment (PIA) also serves as a notice.*

6.1b If notice was not provided, explain why.

A notice is provided. See above 6.1a.

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

At the top of the interest form on the VHA website, before candidates click submit it states "Thank you for your interest in a career with the U.S. Department of Veterans Affairs (VA)! By completing the registration form below, you will be added to VA's Candidate Relationship Manager (CRM), which may help VA match your job interests with VA opportunities. Please complete as much of the form as possible. Thank you again for your desire to serve our country's Veterans! DISCLAIMER: While registering in VA's CRM provides VA the ability to recruit you in the future, this process does not guarantee you will be contacted by VA or considered for future employment."

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.

Candidates do not need to fill out the interest form if they do not want to. SF-VHARM is a CRM application aimed for VHA decision-making to continue improving their processes and campaigns over time. We have a checkbox on the interest form that candidates fill out asking them to review the VA privacy policy and it's a required field for submission of the interest form.

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.

Candidates are notified on the interest form that by completing the registration form, their information is added to the VA's Candidate Relationship Manager, which will help the VA match their job interests with VA opportunities. We have a checkbox on the interest form that candidates fill out asking them to review the VA privacy policy and it's a required field for submission of the interest form.

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: Insufficient notice to candidates regarding the scope of information collected when they fill out the interest form submitted to the CRM, poses risks of privacy infringement and non-

compliance. Candidates may feel their privacy is compromised, leading to distrust and potential legal implications if not adequately informed about the collection and use of their data.

Mitigation: We implement comprehensive privacy notices that clearly outline the scope of information collected, the purposes of collection, and how the data will be used and protected.

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.***

Candidates are not authenticated and thus cannot log-in to view the information on their contact record in SF-VHARM. An update to the candidate information is provided in a public-facing interest form page to correct/change their information after submission, but the candidate would have to refill out the entire form, so PII is not leaving the SF-VHARM CRM application onto a public-facing page. The candidate would need to update the entire form and resubmit because we are not taking PII out of the system and putting it on the public facing page for the candidate to see and update, since they are not authenticated and it's a public page.

Individuals wishing to inquire whether this system of records contains records on them should contact the local facility to which they applied or the Physician and Dentist Placement Service. Individuals submitting requests should furnish identifying information as required by VA for their records to be located and identified: (1) Full name, (2) date of birth, (3) social security number, (4) name and location of VA facility or Physician and Dentist Placement Service where application was submitted, (5) date of application, and (6) signature.

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)?

SF-VHARM is not exempt from the access provisions in the Privacy Act, not applicable.

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?

Refer to section 7.1a.

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.

A candidate may correct their information by completing the public-facing interest form. Because the candidates will not be authenticated users, there will not be a way for them to log into the platform and view their record.

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.

Candidates will receive instructions on how to update their information by completing the interest form. This will be at the end of each emails the candidates will receive.

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.

A formal redress is provided in each email a CRM candidate receives, which explains the process of updating their information by completing a new interest form.

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 absence of user authentication for direct information updates in the Salesforce CRM raises risks concerning access control, redress, and correction policies. Lacking robust redress and correction procedures may result in inaccuracies within candidate profiles, potentially impacting hiring decisions and undermining trust in our data management practices.

Mitigation: Establish clear and transparent guidance on how the candidates can update their information in the tool and provide the option on a recurring basis, and ensure timely response procedures for the candidates.

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?

New internal users must be provisioned with an individual license to access the system with discretion approval. (with PM/COR approval). User roles identify the information and applications a user can access. To receive access to the system, another user with appropriate permissions must sponsor them. The sponsor will describe which applications the user needs to access, the user's role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow field level control of the information and data. External users will not have access to the system.

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 will be no users from other agencies who will have access to SF-VHARM.

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.

Internal users have different personas identified SF-VHARM to include “Management Super User, Management, Sourcing, and Marketing” having varying degrees of access that is being further documented via CRUD matrix.

Role	**Access Type**
Management Super User	Create, Read, Edit or Read / View depending on the object
Management	Create, Read, Edit or Read / View depending on the object
Marketing	Create, Read, Edit or Read / View depending on the object
Sourcing	Create, Read, Edit or Read / View depending on the object

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

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

VA contract employee from DTC access is verified through the Contracting Officer’s Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system.

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

Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-

based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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

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

General Training include: VA Privacy Rules of Behavior, Privacy awareness training, HIPPA and VA on-boarding enterprise-wide training, in addition to a background check. 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 part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. System administrators are required to complete additional role-based training. All administrative users undergo mandated annual training, including privacy and HIPAA focused training and VA privacy and information security awareness training.

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:* 08/27/2024
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 09/09/2024
5. *The Authorization Termination Date:* 09/09/2026
6. *The Risk Review Completion Date:* 09/09/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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, Salesforce – VHA Recruitment Marketing CRM utilizes Salesforce Government Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce.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 Salesforce Gov Cloud Plus.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*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/PHI that will be shared through the Salesforce – VHA Recruitment Marketing CRM. Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

Ancillary data is not collected by Salesforce. VA has full ownership over the data stored in the SF-VHA RM application.

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

VA has full authority over data stored in SF- VHA Recruitment Marketing CRM.

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).

SF-VHA Recruitment Marketing CRM system does not utilize RPM.

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.

HARASH KATYAL

Digitally signed by HARASH KATYAL
Date: 2025.04.16 15:54:02 -04'00'

Privacy Officer, Harash Katyal

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2025.04.23 07:17:04 -04'00'

Information System Security Officer, Joseph Facciolli

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2025.04.21 12:11:58 -04'00'

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).

Notice is provided to candidates in three ways:

1. *Disclaimer in the Interest Form filled by the candidate states* –
   "Thank you for your interest in a career with the U.S. Department of Veterans Affairs (VA)! By completing the registration form below, you will be added to VA's Candidate Relationship Manager (CRM), which may help VA match your job interests with VA opportunities. Please complete as much of the form as possible. Thank you again for your desire to serve our country's Veterans! DISCLAIMER: While registering in VA's CRM provides VA the ability to recruit you in the future, this process does not guarantee you will be contacted by VA or considered for future employment."

2. The SORNs defines the information collected from *Veterans or Dependents/ VA Employees/ Contractors/ Members of Public*, use of the information, and how the information is accessed and stored. *02VA135, Applicants for Employment Under Title 38 USC-VA*

3. *This Privacy Impact Assessment (PIA) also serves as a notice.*

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

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