Privacy Impact Assessment for the VA IT System called:

SALESFORCE- CONSOLIDATED INTERNSHIP SOLUTION

VA Corporate Office

HUMAN CAPITAL SERVICES CENTER (HCSC)

2042

Date PIA submitted for review:

March 04, 2024

System Contacts:

System Contacts

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

Abstract

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

Salesforce- Consolidated Internship Solution (CIS) is a solution to administer and monitor Human Capital Services Center's (HCSC) various development programs including support for operations, communications, feedback mechanisms and participant management. This solution provides a digitized automated solution to consolidate programs, streamline processes and optimize workflow which provides improved visibility and metrics. Within the HCSC and under the Stakeholder's purview there are currently three distinct programs:

A.) Pathways Program is designed and marketed towards students and recent graduates of all ages and backgrounds. Pathways consists of three distinct sub-programs:

(i) Presidential Management Fellows (PMF) Program

(ii) Internship Program

(iii) Recent Graduates Program

B.) Workforce Recruitment Program (WRP) is a government-wide program participated by the VA and co-sponsored by the Department of Defense and the Department of Labor. The goal of the program is to increase the representation of individuals with disabilities, especially severe disabilities, in the Federal and private workforce.

C.) National Diversity Internship Program (NDIP) provides internship opportunities to diverse undergraduate and graduate students who are currently enrolled, full-time or part-time, in a degree-seeking program, at an accredited post-secondary institution.

The goal for this initiative is to manage and track the Pathways, WRP and NDIP programs in a centralized system to eliminate information silos and provide visibility into which participants are part of each program. Additionally, the solution will be user friendly and provide automation in order for HCSC to reach their full participation potential. The CIS application will (1) Provide a single source of truth for the management of all the internship programs (2) Allow potential business offices to complete the intern application and upload necessary documentation (3) Ability to complete and track agreements (4) Support the Intake, Selection (Review and Approval), Onboarding, and Program & Project Management processes (5) have Built-in dashboards and reporting capabilities.

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:

1. General Description

A. *What is the IT system name and the name of the program office that owns the IT system?*

The IT System name is Consolidated Internship Solutions (CIS) and it is owned by Human Capital Services Center (HCSC).

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

CIS Goals:

- Developing a centralized management system for tracking the program participant lifecycle across the Pathways Program (Interns & Recent Graduates (I&RG) and Presidential Management Fellows (PMF) and Workforce Recruitment Program (WRP)
- Providing improved visibility and metrics into the respective internship programs

Implementing a foundation for:

- Providing future automations to support HCSC in achieving their full participation potential
- Enriching the module to onboard the National Diversity Intern Program (NDIP)

The purpose of the IT system is to allow business lines and IT to deliver faster more secure solutions by building on a commercially available Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) product called Salesforce. Salesforce allows the configuration of a graphical user interface (GUI) to provide data entry, workflows, reporting and dashboards.

Consolidated Internship Solution (CIS) is a solution to administer and monitor Human Capital Services Center's (HCSC) various development programs including support for operations, communications, feedback mechanisms and participant management. Within the HCSC and under the Stakeholder's purview there are currently three distinct programs: A.) Pathways Program is designed and marketed towards students and recent graduates of all ages and backgrounds. Pathways consists of three distinct sub-programs: (i) Presidential Management Fellows (PMF) Program, (ii) Internship Program, (iii) Recent Graduates Program. B.) Workforce Recruitment Program (WRP) is a government-wide program participated by the VA and co-sponsored by the Department of Defense and the Department of Labor. The goal of the program is to increase the representation of individuals with disabilities, especially severe disabilities, in the Federal and private workforce. C.) National Diversity Internship Program (NDIP) provides internship opportunities to diverse undergraduate and graduate students who are currently enrolled, full-time or part-time, in a degree-seeking program, at an accredited post-secondary institution. The goal for this initiative is to manage and track the Pathways, WRP and NDIP programs in a centralized system to eliminate information silos and provide visibility into which participants are part of each program. Additionally, the solution will be user friendly and provide automation in order for HCSC to reach their full participation potential.

The stakeholder has a legacy solution (SharePoint) that has been decommissioned and is no longer maintained. Additionally, HCSC continues to acquire more internship programs and has redefined internal processes.

C. *Who is the owner or control of the IT system or project?*

Office of Information Technology (OI&T), Enterprise Program Management Office (ePMO). The IT system name is Consolidated Internship Solution (CIS) and it is owned by Human Capital Services Center (HCSC).

2. Information Collection and Sharing

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

Projected 1-Year record additions in Salesforce: 52,416

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

CIS information used would include Name, Date of Birth, address, phone numbers, email ID, Demographic information including race/ethnicity/gender/age, disability status, Veteran status, employment and educational history, and resumes.

The CIS application will (1) Provide a single source of truth for the management of all the internship programs (2) Allow potential business offices to complete the intern application and upload necessary documentation (3) Ability to complete and track agreements (4) Support the Intake, Selection (Review and Approval), Onboarding, and Program & Project Management processes (5) have Built-in dashboards and reporting capabilities.

The purpose of the IT system is to allow business lines and IT to deliver faster more secure solutions by building on a commercially available Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) product called Salesforce. Salesforce allows the configuration of a graphical user interface (GUI) to provide data entry, workflows, reporting and dashboards. This IT system is categorized as minor and augments a Major Application Salesforce Development Platform (SFDP) VA.

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

Demographic information including race/ethnicity/gender/age, disability status, veteran status, employment, and educational history, resumes, name and contact information such as phone numbers, addresses and emails.

The CIS Salesforce module is being implemented in two Phases with the combination of these two phases helping to support and provide critical business impacts and metrics on the following Stakeholder Consolidated Internship processes: Pre-Application & Requisitions Application Intake & Review Onboarding & Training Management & Performance Offboarding & Future Engagements. Specifically, Phase I will address the features and capabilities for two of the three subsystems (programs) Internship Programs: Pathways (Interns, Recent Graduates and PMF) and WRP. Phase II will include NDIP, integrations, data migration and analytics for the Consolidated Internship Solution.

G. Is 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?

No.

3. Legal Authority and SORN

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

The following is a full list of related laws, regulations and policies and the legal authorities:

Executive Order 14035 Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce

Issues guidance to increase the availability of paid internships, fellowships, and apprenticeships; reduce reliance on unpaid internships and similar programs; and improve outreach to and recruitment of individuals from underserved communities.

Executive Order 13583 Establishing a Coordinated Government-wide Initiative to Promote Diversity and Inclusion in the Federal Workforce.

Wherever possible, the Federal Government must also seek to consolidate compliance efforts established through related or overlapping statutory mandates, directions from Executive Orders, and regulatory requirements. By this order, I am directing executive departments and agencies (agencies) to develop and implement a more comprehensive, integrated, and strategic focus on diversity and inclusion as a key component of their human resources strategies. This approach should include a continuing effort to identify and adopt best practices, implemented in an integrated manner, to promote diversity and remove barriers to equal employment opportunity, consistent with merit system principles and applicable law.

Executive Order 13562 Recruiting and Hiring Students and Recent Graduates.

The Office of Personnel Management (OPM) is issued final regulations implementing the Pathways Programs established by E.O. 13562, signed December 27, 2010. As directed by the President, the Pathways Programs provide clear paths to Federal internships and potential careers in Government for students and recent graduates. The Pathways Programs consist of the Internship Program, the Recent Graduates Program and the Presidential Management Fellows Program. Positions in the Pathways Programs are excepted from the competitive service. Participants in these Programs are appointed under the newly created Schedule D of the excepted service.

The Code of Federal Regulations, 5 CFR Parts 213, 302, 315, 330, 334, 362, 531, 536, 537, 550, 575, and 890

Executive Order 13548, Increasing Federal Employment of Individuals with Disabilities

The Workforce Recruitment Program (WRP) is a recruitment and referral program that connects federal and private sector employers nationwide with highly motivated college students and recent graduates with disabilities who are eager to prove their abilities in the workplace through summer or permanent jobs. WRP is the number one source to identify pre-screened college students and recent graduates with disabilities for opportunities within the federal government. In 2011, the Office of Personnel Management (OPM) highlighted the WRP as a model strategy in its guidance to federal agencies regarding the recruitment and hiring of people with disabilities in response to Executive Order 13548, Increasing Federal Employment of Individuals with Disabilities.

171VA056A/78 FR 63311-Human Resources Information Systems Shared Service Center (HRIS SSC)—VA (Oct 23, 2013)
https://www.govinfo.gov/content/pkg/FR-2013-10-23/pdf/2013-24830.pdf

Information from SORN: Human Resource Information System Shared Service Center (HRIS SSC)- VA 171VA056A/ 78 FR 63311

- To produce and maintain the official personnel records, including reports and statistical data, of VA employees for use by Federal, State and local agencies and organizations authorized by law or regulation to have access to such information. These records may be disclosed as part of an ongoing matching program to accomplish these purposes. This routine use does not authorize the disclosure of information that must be disclosed under the criteria contained in 5 U.S.C. 552a (b) (7), (8), and (11). The Code of Federal Regulations, 5 CFR Parts 213, 302, 315, 330, 334, 362, 531, 536, 537, 550, 575, and 890.

Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317

5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended by Public Law No.104---231, 110 Stat. 3048

- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- E-Government Act of 2002 § 208
- Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites
- OMB Memo M---99---18, Privacy Policies on Federal Web Sites
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- OMB Circular A-130, Appendix III, “Security of Federal Automated Information Systems”
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002

OMB M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

- VA Directive and Handbook 6502, Privacy Program
- State Privacy Laws

The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397.

Salesforce Government Cloud was granted a full ATO by Deputy CIO Service Delivery and Engineering (SD&E), for all applications that sit on the platform. The IT System name is Salesforce Development Platform (SFDP) VA; it is owned by the Office of Information Technology (OI&T), Enterprise Program Management Office (ePMO).

I. *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?*

N/A, the system is not in the process of being modified at this time. CIS will not modify an existing SORN.

Salesforce Government Cloud is maintaining underlying physical infrastructure. Additional ISA/MOUs are required between the VA and VA designated contractors/vendors that own the data that is stored or processed within Salesforce Development Platform VA. The vendor-specific agreements will describe the data ownership and storage requirements. The parties agree that transmission, storage, and management of VA sensitive information residing in the Salesforce Development Platform VA is the sole responsibility of VA employees or designated contractors/vendors assigned to manage the system. At no time will Salesforce Government Cloud have any access to VA data residing within the Salesforce Development Platform VA. Thus, all agreements on data and system responsibilities shall not be covered in this base agreement (MOU). However, Salesforce Government Cloud shall provide the tools to allow VA to properly secure all systems and data hosted in the Salesforce Development Platform VA.

4. System Changes

J. *Will the completion of this PIA will result in circumstances that require changes to business processes?*

No.

K. *Will the completion of this PIA could potentially result in technology changes?*

No.

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. 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
□ Social Security Number
☒ Date of Birth
□ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)

□ Personal Fax Number
☒ Personal Email Address
□ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
□ Financial Information
□ Health Insurance Beneficiary Numbers Account numbers
□ Certificate/License numbers[1]
□ Vehicle License Plate Number
□ Internet Protocol (IP) Address Numbers
□ Medications
□ Medical Records
☒ Race/Ethnicity
□ Tax Identification Number
□ Medical Record Number
☒ Gender
□ Integrated Control Number (ICN)
☒Military History/Service Connection
□ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Demographic information including race/ethnicity/gender/age, disability status, Veteran status, employment history, resumes, name and contact information such as phone numbers, addresses and emails. At this juncture a combination of contact information is considered the External User ID.

PII Mapping of Components (Servers/Database)

Consolidated Internship Solutions, a Salesforce application, consists of **one** key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **CIS** 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 3.9 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
HR Smart PeopleSoft Database (Oracle PeopleSoft Human Capital Management)	Yes	Yes	Date of Birth (DOB) Disability Status Resume	To facilitate recruitment and management of our program participants	Licenses with further access governed by roles.

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

			Employment History External User ID Gender Race Ethnicity Name Personal Contact Number Personal Email Address Personal Mailing Address	throughout their life cycle.	

1.2 What are 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?

Those providing information include VA Personnel (Supervisor, Hiring Manager, HR Professional, HCSC Program Manager, HCSC Directors and Chief Learning Officer) or the interested candidate.

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.

Future-state would include integration with HR-Smart which would automate most of the manual input and lower redundant requests.

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

CIS has the capability to produce reports and dashboards based on the participant records that exist in the database.

1.3 How is the information collected?

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?*

Information may be collected directly from the individual or other VA personnel (Supervisor, Hiring Manager, HR Professional, HCSC Program Manager, HCSC Directors and Chief Learning Officer) before they are hired via written or verbal communication with a VA employee. HR Professional/ Program Manager will gather the data from the USA JOBS portal. The data collected will be manually entered in Salesforce by the HR Professional/ Program Manager. Once onboarded, the employee may edit their profile in the system. In a future state information may be collected through other VA systems such as TMS or HR Smart. All intakes and records are facilitated electronically.

The information and data will be collected through validation of the data provided to the team by IAM.

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?

All intakes and records are facilitated electronically.

1.4 How will the information be checked for accuracy? 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.

Information is validated when initially stored and ad hoc whenever VA personnel have validity concerns. There are opportunities for the Supervisor, Hiring Manager, HR Professional, HCSC Program Manager, HCSC Directors, or Chief Learning Officer to adjudicate a record as well as the candidate his or herself. In the future state information may be collected through other VA systems such as TMS or HR Smart.

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?

Information is validated when initially stored and ad hoc whenever VA personnel have validity concerns. There are opportunities for the Supervisor, Hiring Manager, HR Professional, HCSC Program Manager, HCSC Directors, or Chief Learning Officer to adjudicate a record as well as the candidate his or herself. In the future state information may be collected through other VA systems such as TMS or HR Smart.

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 following is a full list of related laws, regulations and policies and the legal authorities:

Executive Order 13562 Recruiting and Hiring Students and Recent Graduates

The Office of Personnel Management (OPM) is issued final regulations implementing the Pathways Programs established by E.O. 13562, signed December 27, 2010. As directed by the President, the Pathways Programs provide clear paths to Federal internships and potential careers in Government for students and recent graduates. The Pathways Programs consist of the Internship Program, the Recent Graduates Program, and the Presidential Management Fellows Program. Positions in the Pathways Programs are excepted from the competitive service. Participants in these Programs are appointed under the newly created Schedule D of the excepted service.

Executive Order 14035 Diversity, Equity, Inclusion, and Accessibility (DEIA) in the Federal Government

This Executive Order aims to cultivate a workforce that draws from the full diversity of the Nation. The EO states that the Federal Government must be a model for diversity, equity, inclusion, and accessibility (DEIA) and must strengthen its ability to recruit, hire, develop, promote and retain our Nation's talent and remove barriers to equal opportunity. The EO establishes that DEIA are priorities and outlines procedures to advance these priorities across the federal workforce.

The Code of Federal Regulations, 5 CFR Parts 213, 302, 315, 330, 334, 362, 531, 536, 537, 550, 575, and 890

Executive Order 13548, Increasing Federal Employment of Individuals with Disabilities

The Workforce Recruitment Program (WRP) is a recruitment and referral program that connects federal and private sector employers nationwide with highly motivated college students and recent graduates with disabilities who are eager to prove their abilities in the workplace through summer or permanent jobs. WRP is the number one source to identify pre-screened college students and recent graduates with disabilities for opportunities within the federal government. In 2011, the Office of Personnel Management (OPM) highlighted the WRP as a model strategy in its guidance to federal agencies regarding the recruitment and hiring of people with disabilities in response to Executive Order 13548, Increasing Federal Employment of Individuals with Disabilities.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The individual data elements are not personally identifiable however, if combined, may be associated with the individual. All information collected is consistent with what would be requested when a candidate applies to the VA. Sensitive Personal Information (SPI) including personal contact information, SSN and medical information may be at risk to exposure via HR Smart, which would be a concern via HR Smart through system integration, not the SalesForce module itself. Data breach may occur at the facility level or network level.

Mitigation: Only directly relevant and necessary information is collected. Not all fields are required. Information collection and use is subject to the VA privacy policies. Depending on level of authority granted to the respective user by their home department via the VA, each user will have sensitivity level of access to veteran data based on profile-based permissions. The profiles will be reviewed on a regular basis to ensure that appropriate information is shared with appropriate users. All employees with access to Veteran's information are required to complete the VA Privacy Information Security Awareness training and Rules of Behavior annually. SFDP protects data by ensuring that only authorized users can access the SPI of veterans with strict password security policy. Each of the passwords are stored in the form of Secure Hash Algorithm (ex: 256 one-way hash format). All data is encrypted in transfer. To ensure the utmost privacy and security at the facility level, authorized personnel must pass through multiple levels of biometric and/or badge scanning to reach the salesforce system rooms/cages. All buildings are anonymous with silent alarms installed at all exterior entrances which notify the law enforcement in an event of suspected intrusion. Data is backed up. Backups do not physically leave the data center. Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only https traffic on ports 80 and 443, along with Internet Control Message Protocol (ICMP) traffic. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry.

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
External User ID	File identification purposes/program reporting	Not used
Name	File identification purposes/program reporting	Not used
Date of Birth	File identification purposes/program reporting	Not used
Phone Number	File identification purposes/program reporting	Not used
Email Address	File identification purposes/program reporting	Not used
Mailing Address	File identification purposes/program reporting	Not used
Race/Ethnicity	File identification purposes/program reporting	Not used
Gender/Age	File identification purposes/program reporting	Not used
Disability Status	File identification purposes/program reporting	Not used
Veteran Status	File identification purposes/program reporting	Not used
Employment	File identification purposes/program reporting	Not used
Educational History	File identification purposes/program reporting	Not used
Resumes	Program Management	Not used

2.2 What types of tools are 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 would be used to run reports or dashboards which would aid in reporting to upper management and improving HCSC's internship and development programs.

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.
The system does not create or make available new or previously unutilized information about an individual. No action or determinations will be taken against or for the individual identified because of the newly derived data and the record would only be accessible by the subject of the record, their Supervisor, Hiring Manager, HR Professional, HCSC Program Manager, HCSC Directors and Chief Learning Officer).

2.3 How is the information in the system 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?
After logging in, a user establishes a session with the platform. Session security also limits the risk of internal attacks, such as when one employee tries to use another employee's session. The default session timeout is two hours of inactivity. When the session timeout is reached, users are prompted with a dialog that allows them to log out or continue working. If they don't respond to this prompt, they're logged out.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
N/A: The tool doesn't collect, process, or retain SSN of the individual.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
Security is achieved using access credentials via login credentials along with integrating the PIV card and eToken security fobs and role-based access and licenses. After logging in, a user establishes a session with the platform. Session security also limits the risk of internal attacks, such as when one employee tries to use another employee's session. The default session timeout is two hours of inactivity. When the session timeout is reached, users are prompted with a dialog that allows them to log out or continue working. If they don't respond to this prompt, they're logged out.

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

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

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

<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.

2.4a How is access to the PII determined?

Users must submit a request for access to the Business Owner. Business owner adjudicates the request and determines the level of access based upon user roles. Business owner will forward approved requests for access to DTC for access.

Information is only accessible to those with a license and further access is determined on a role by role basis. HCSC's Development Services team will determine who may acquire a license which will be awarded through the Digital Transformation Center (DTC). All information collected is relevant to the mission of the project which is to manage existing operations of our Intern and Career Development Programs. All information collected is consistent with what would be requested when a candidate applies to the VA.

All users are issued licenses to access system. In order to access CIS, potential users request access and is routed to the system owner for verification, adjudication and determination for the appropriate level of access prior to routing to the DTC.

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

Salesforce Government Cloud is maintaining underlying physical infrastructure. Additional ISA/MOUs are required between the VA and VA designated contractors/vendors that own the data that is stored or processed within Salesforce Development Platform VA. The vendor-specific agreements will describe the data ownership and storage requirements. The parties agree that transmission, storage, and management of VA sensitive information residing in the Salesforce Development Platform VA is the sole responsibility of VA employees or designated contractors/vendors assigned to manage the system. At no time will Salesforce Government Cloud have any access to VA data residing within the Salesforce Development Platform VA. Thus, all agreements on data and system responsibilities shall not be covered in this base agreement (MOU). However, Salesforce Government Cloud shall provide the tools to allow VA to properly secure all systems and data hosted in the Salesforce Development Platform VA.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

User roles and personas are documented in the CIS User Guide and users only are assigned the level of access needed to perform their roles. Systematic reviews are conducted and once individuals complete program requirements their access is removed unless a continued need is documented.

2.4c Does access require manager approval?

Program Manager/HR Specialist and Executive require manager designation and/or approval.

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

There are two types of users that can manage CIS data: (1) the authorized module users and based on their permissions they can either create or update the data and (2) VA Salesforce platform Digital Transformation Center team.

2.4e Who is responsible for assuring safeguards for the PII?

The SFDP uses two VA Identity and Access Management (IAM) services to validate user login information. The validation of VA employees is done through Active Directory Federated Services (ADFS) and Veterans' information is validated using Access VA and their internal resources. Salesforce is hosted in a Salesforce environment within a FedRAMP government certified cloud.

ADFS: All VA employees use their PIV to sign into SFDP using ADFS. This IAM VA service checks the presented A credentials from their PIV card against VA's Active Directory. If an employee is not a user in Active Directory, then they will not have access to SFDP.

AccessVA: AccessVA is utilized in the credential validation process as well as assisting in the creation of a Single Sign-On external capability. Applications using IAM's AccessVA allow a Veteran to sign up, access, and use the application via accepted AccessVA credentials.
CIS system connects to HR Smart PeopleSoft Database (Oracle PeopleSoft Human Capital Management) for validating the individual identity for participation in the program throughout the lifecycle.

The SORN Applicable for CIS is Human Recourses Information Systems Shared Service Center (HRIS SSC)-VA, SORN 171VA056A/ 78 FR 63311. This SORN covers all the PII information applicable to the tool.

Section 3. Retention of Information

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

3.1 What information is retained?

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

Name
Date of Birth
Phone Number
Email Address
Mailing Address
Race/Ethnicity

Gender/Age
Disability Status
Veteran Status
Employment History
Educational History
Resumes
External User ID

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

All information input is retained by the system either in an active or archived state for 75 years in accordance with 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.

3.3 Has the retention schedule been 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. 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. Please work with the system Privacy Officer and 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?

SFDP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. 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). SFDP records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records) (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf).

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

Retention of Records is expected to be 75 years. Records are kept in archived status indefinitely. 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

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.

Records are electronic and are not destroyed, they are archived.

Active Data stays on disk until the VA deletes or changes it. Data on backups is retained for 90 days until the backups are overwritten. Log data is retained by Salesforce for a year. VA exports data and retain it to meet VA/NARA retention requirements and dispose of the exported data at the end of the retention period.

When hard drives and backup tapes are at their end of life, the media is sanitized based on Salesforce’s Media Disposal Policy. Hard drives are overwritten using a multiple---pass write of complementary and random values. If it wipes successfully, we will return the disk or array to the vendor. If it fails during the wiping process we retain and destroy (i.e., degauss, shred, or incinerate). Backup tapes are degaussed prior to disposal. Specifics on the sanitization process are below.

Salesforce has an established process to sanitize production backup disks and hard drives prior to disposal, release out of salesforce’s control, or release to the vendor for reuse. Production backup disks and hard drives are sanitized or destroyed in accordance with salesforce’s Media Handling Process. All data is handled and located in VA own Salesforce’s servers in Herndon, VA and Chicago, IL in the Salesforce Government Cloud server classification. Said information is handled with proper authority and scrutiny. Hard drives are sanitized within the data center facility using a software utility to perform a seven---pass overwrite of complementary and random values. If the drives wipe successfully, the hardware will be returned to the lessor. If the drive fails during the wiping process the drives are retained within a locked container within the salesforce data center facilities until onsite media destruction takes place. Leasing equipment provides salesforce with the opportunity to use the latest equipment available from vendors.

Periodically, a third-party destruction vendor is brought on---site to perform physical destruction of any hard drives that failed overwrite. A certificate of destruction is issued once the media is physically destroyed. Electronic data and files of any type, including PII, Sensitive Personal Information (SPI), and more are destroyed in accordance with the Department of Veterans’ Affairs VA Directive 6500 (January 24, 2019), (https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf).

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. The OIT Chief/CIO will be responsible for identifying and training OIT staff on VA media sanitization policy and procedures. The ISO will coordinate and audit this process and document the audit on an annual basis to ensure compliance with national media sanitization policy.

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.

N/A: PII is not used for research, testing or training – rather a "scrubbed" subset of data or "dummy" data.

<u>3.6 PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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 ISSO to complete all Privacy Risk questions inside the document this section).

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

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

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u> The risk to maintaining data within the SFDP is that longer retention times increase the risk that information can be compromised or breached.

<u>Mitigation:</u> To mitigate the risk posed by information retention, the SFDP adheres to the VA RCS schedule for data it maintains. When the retention data is reached for a record, the team will carefully dispose of the data by the determined method as described in question 3.4. All electronic storage media used to store, process, or access VA records will be disposed of in adherence with the latest version of VA Handbook 6500.1, Electronic Media Sanitization.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

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

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VA Time and Attendance VATAS	Profile information of interested parties, applicants and participants is recorded as part of current activities to manage HCSC's internship and development programs.	Veteran Name Veteran status Date of Birth (DOB) Disability Status Resume Employment history External User ID Gender Race Ethnicity Name Personal contact number	Site to site connection using VA internal network using SFTP

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
		Personal Email address Personal Mailing address	
VA Office of Inspector General OIG	Profile information of interested parties, applicants and participants is recorded as part of current activities to manage HCSC's internship and development programs.	Date of Birth (DOB) Disability Status Resume Employment history External User ID Gender Race Ethnicity Name Personal contact number Personal Email address Personal Mailing address	Interconnection is Unidirectional using SFTP
VA Learning University Education Data Repository VALU EDR	Profile information of interested parties, applicants and participants is recorded as part of current activities to manage HCSC's internship and development programs.	Date of Birth (DOB) Disability Status Resume Employment history External User ID Gender Race Ethnicity Name Personal contact number Personal Email address Personal Mailing address	Interconnection is Unidirectional using SFTP
VA Hospital Administration Leadership & Workforce Development System VHA LWD	Profile information of interested parties, applicants and participants is recorded as part of current activities to manage HCSC's internship and development programs.	Date of Birth (DOB) Disability Status Resume Employment history External User ID Gender Race Ethnicity Name Personal contact number Personal Email address Personal Mailing address	Interconnection is Unidirectional using SFTP
Department of Veterans Affairs (VA) Identity and	Profile information of interested parties, applicants and participants is recorded	Date of Birth (DOB) Disability Status Resume Employment history	Interconnection is Unidirectional using SFTP

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Security Services (ISS)	as part of current activities to manage HCSC's internship and development programs.	External User ID Gender Race Ethnicity Name Personal contact number Personal Email address Personal Mailing address	
Identity and Access Management (IAM) - Active Directory Federated Service (ADFS)	IAM ADFS Provisioning Service provides self-service options for internal VA users for centralized creation, modification, deletion and suspension for user accounts based on business processes and interactions defined by applications or systems.	Veteran Name Veteran status Date of Birth (DOB) Disability Status Resume Employment history External User ID Gender Race Ethnicity Name Personal contact number Personal Email address Personal Mailing address	The ADFS servers pass a token to the SFDP that validates a VA internal user, via their federated ID, as a current credentialed user of VA systems. Access credentials via login credentials along with integrating the PIV card and eToken security fobs.
Office of Resolution Management Diversity and Inclusion (ORMDI)	Profile information of interested parties, applicants and participants is recorded as part of current activities to manage HCSC's internship and development programs.	Date of Birth (DOB) Disability Status Resume Employment history External User ID Gender Race Ethnicity Name Personal contact number Personal Email address Personal Mailing address	Email

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Secretary	Profile information of interested parties, applicants and participants is recorded as part of current activities to manage HCSC's internship and development programs.	Date of Birth (DOB) Disability Status Resume Employment history External User ID Gender Race Ethnicity Name Personal contact number Personal Email address Personal Mailing address	Email
Deputy Secretary	Profile information of interested parties, applicants and participants is recorded as part of current activities to manage HCSC's internship and development programs.	Date of Birth (DOB) Disability Status Resume Employment history External User ID Gender Race Ethnicity Name Personal contact number Personal Email address Personal Mailing address	Email
Office of Chief Human Capital Officer (CHCO)	Profile information of interested parties, applicants and participants is recorded as part of current activities to manage HCSC's internship and development programs.	Date of Birth (DOB) Disability Status Resume Employment history External User ID Gender Race Ethnicity Name Personal contact number Personal Email address Personal Mailing address	Email
Booze Allen Hamilton	Access to maintain and edit system.	Date of Birth (DOB) Disability Status Resume Employment history External User ID Gender	Access credentials via login credentials along with

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
		Race Ethnicity Name Personal contact number Personal Email address Personal Mailing address	integrating the PIV card and eToken security fobs.
Digital Transformation Center (DTC)	Access to maintain and edit system.	Date of Birth (DOB) Disability Status Resume Employment history External User ID Gender Race Ethnicity Name Personal contact number Personal Email address Personal Mailing address	Access credentials via login credentials along with integrating the PIV card and eToken security fobs.

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

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: Profile information of interested parties, applicants and participants is recorded as part of current activities to manage HCSC’s internship and development programs. Potential threats include accidental disclosure, theft, and hacking. The information collected through CIS coupled with other information could lead to identifying the individual leading to adverse effect on the integrity of VA and in turn for the HCSC program.

Mitigation: Users of the system will all have undergone VA Privacy and Information Security Awareness and Rules of Behavior Training as well as the Annual Government Ethics Report Requirement, Government Ethics - The Essentials, offered through TMS. Role-based security to access the tool using their email ID with prior approval from Program Officer/ Manager.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
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: Profile information of interested parties, applicants and participants is recorded as part of current activities to manage HCSC's internship and development programs. Potential threats include accidental disclosure, theft, and hacking. The information collected through CIS coupled with other information could lead to identifying the individual leading to adverse effect on the integrity of VA and in turn for the HCSC program.

If there is data being shared outside of the department in the future, access controls will be implemented based on MOUs, contracts, or agreements.

Mitigation: Users of the system will all have undergone VA Privacy and Information Security Awareness and Rules of Behavior Training as well as the Annual Government Ethics Report Requirement, Government Ethics - The Essentials, offered through TMS. Role-based security to access the tool using their email ID with prior approval from Program Officer/ Manager.

VA has contracted Salesforce Inc. to deliver services that include maintaining VA data. A contract is in place that clearly articulates Salesforce's roles and responsibilities. Authorized Salesforce personnel access user level data to provision and provide the Salesforce service. Access is controlled by authentication and is restricted to authorized individuals. Salesforce's security policies address the required security controls that must be followed in order to protect PII. Salesforce Development Platform VA will be connected to Equinix for data transfer purposes. Equinix will provide details of the security event, the potential risk to VA owned sensitive information, and the actions that have been or are being taken to remediate the issue. Activities that will be reported include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Equinix will also provide VA with a written closing action report once the security event or incident has been resolved. VA will follow this same notification process should a security event occur within the VA boundary involving Equinix's provided data. Designated POCs will follow established incident response and reporting procedures, determine whether the incident warrants escalation, and comply with established escalation requirement for responding to security incidents.

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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (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?

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 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, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

All information collected is consistent with what would be requested when a candidate applies to the VA. Notice is provided upon applying for the position via USA Jobs and upon acceptance of the position via USA Staffing.

Privacy Act Notice (PL 93-579): We use this information to determine qualifications for employment. This is authorized under Title 5 U.S.C. 3302 and 3361.

USA Staffing® is an Official U.S. Government System for authorized use only. Unauthorized use of this system or the information on this system could result in criminal prosecution. Signing into USA Staffing® indicates you have read and accepted the Full Terms and Conditions of Use and you consent to security testing and monitoring.

Full Terms and Conditions of Use

USA Staffing® is a U.S. Government information system to be used by authorized users only. Information from this system resides on computer systems funded by the government.

The data and documents on this system include Federal records that contain sensitive information protected by various Federal statutes, including the Privacy Act, 5 U.S.C. § 552a. The use of personally owned devices to process, store, or transmit USA Staffing® Personally Identifiable Information (PII) is prohibited.

All access or use of this system constitutes user understanding and acceptance of these terms and constitutes unconditional consent to review, monitor, record, audit, and take action by all authorized government and law enforcement personnel.

Unauthorized user attempts or acts to (1) access, view, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, (4) accrue resources for unauthorized use, or (5) otherwise misuse this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties.

Additional notice is available through the existing SORN from the OPRM site (https://www.oprm.va.gov/docs/Current_SORN_List_09_21_2021.pdf).
The SORN applicable for the system is Human Resources Information Systems Shared Service Center (HRIS SSC)—VA (https://www.govinfo.gov/content/pkg/FR-2013-10-23/pdf/2013-24830.pdf) 171VA056A/ 78 FR 63311

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

All information collected is consistent with what would be requested when a candidate applies to the VA. Notice is provided upon applying for the position via USA Jobs and upon acceptance of the position via USA Staffing. Privacy Act Notice (PL 93-579): We use this information to determine qualifications for employment. This is authorized under Title 5 U.S.C. 3302 and 3361.USA Staffing® is an Official U.S. Government System for authorized use only. Unauthorized use of this system or the information on this system could result in criminal prosecution. Signing into USA Staffing® indicates you have read and accepted the Full Terms and Conditions of Use and you consent to security testing and monitoring. Full Terms and Conditions of Use USA Staffing® is a U.S. Government information system to be used by authorized users only. Information from this system resides on computer systems funded by the government. The data and documents on this system include Federal records that contain sensitive information protected by various Federal statutes, including the Privacy Act, 5 U.S.C. § 552a. The use of personally owned devices to process, store, or transmit USA Staffing® Personally Identifiable Information (PII) is prohibited. All access or use of this system constitutes user understanding and acceptance of these terms and constitutes unconditional consent to review, monitor, record, audit, and take action by all authorized government and law enforcement personnel. Unauthorized user attempts or acts to (1) access, view, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, (4) accrue resources for unauthorized use, or (5) otherwise misuse this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties. Additional notice is available through the existing SORN from the OPRM site (https://www.oprm.va.gov/docs/Current_SORN_List_09_21_2021.pdf). The SORN applicable for the system is Human Resources Information Systems Shared Service Center (HRIS SSC)—VA (https://www.govinfo.gov/content/pkg/FR-2013-10-23/pdf/2013-24830.pdf) 171VA056A/ 78 FR 63311

6.1c 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.

Profile information of interested parties, applicants and participants is recorded as part of current activities to manage HCSC’s internship and development programs. All information collected is consistent with what would be requested when a candidate applies to the VA.

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.

Yes, the individual has the right to decline to provide their demographic information, disability status and resumes. The application will still be processed without sharing their demographic information. However, if the candidate doesn't provide the required information such as name, contact information; the recruitment process cannot proceed. Their basic contact information is necessary to account for everyone enrolled in the program.

As per USA JOBS Privacy Policy, USA JOBS will collect PII (Name, email address, other unique identifier) only if specifically provided by the applicant.

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.

As per USA JOBS Privacy Policy if the individual chooses to send an email or forms requests, there is only sharing of information with another government agency if their inquiry relates to that agency, or as otherwise required by law.

The applicant provides user level data, which may contain PII, for provisioning and providing the salesforce service, and the Customer continues to have access to such information.

VA does not otherwise share this information with Salesforce except if required by law to do so. VA has sole ownership of the information and data located in Salesforce's Data Center. VA is the only entity that has access to that said data.

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that VA employees and Veterans will not know that applications built on the SFDP collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation: The tool mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the methods discussed in question 6.1. The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and the SORN.

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?

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 http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Once a participant is onboarded to the VA, they have access to their record for the duration of the program. If individuals were never onboarded then they will not be able to access the system and therefore, their information is not stored in the system.

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)?

The system is covered under the following SORN (https://www.oprm.va.gov/privacy/systems_of_records.aspx) and 171 VA056A/78 FR 63311-Human Resources Information Systems Shared Service Center (HRIS SSC)—VA (Oct 23, 2013)

https://www.govinfo.gov/content/pkg/FR-2013-10-23/pdf/2013-24830.pdf

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?

the system is covered under the privacy act system of records as noted above.

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.

Any party with access to the record can correct immature or erroneous information based on their role permissions.

Users who become part of the VA will have direct access to their information. Those who did not transition to the Participant phase may contact the Hiring Manager, HR Professional or HCSC Program Manager they spoke with.

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.

During training individuals will be notified of the option to correct inaccuracies based on role permissions. Users who become part of the VA will have direct access to their information. Those who did not transition to the Participant phase may contact the Hiring Manager, HR Professional or HCSC Program Manager they spoke with.

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.

Users who become part of the VA will have direct access to their information. Those who did not transition to the Participant phase may contact the Hiring Manager, HR Professional or HCSC Program Manager they spoke with.

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 System ISSO to complete all Privacy Risk questions inside the document this section).*

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: There is a risk that Users whose records contain incorrect information may not receive notification of any changes.

Mitigation: SFDP mitigates the risk of incorrect information in an individual's records by authenticating information and validating data accuracy using the resources discussed in question 1.5. Furthermore, Users will have access to their own individual online records using a username and password credentials. Privileged users will access online records other than their own, consistent with their authority and organizational affiliations using PIV.

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?

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?
Users receive access via license granted via the DTC utilizing a link to a request form.

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?
Roles that would have access are limited to the VA and would include Participants, Supervisors, Hiring Managers, HR Professionals, HCSC Program Manager, HCSC Directors and Chief Learning Officer. Parameters were established by system designers.

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.
Read-Only and Editable functionality depends on the role. Parameters were established by system designers.

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.

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's Talent Management System (TMS). The Office of Contract Review operates under a reimbursable agreement with VA's Office of Acquisition, Logistics and Construction (OALC) to provide pre-award, post-award, and other requested reviews of vendors' proposals and contracts. Contractually all contractors are required to sign the VA Form 0752 NDA.

System Owner and Contracting Officer Representative (COR) is the individual to accept and amend any incoming or outgoing contracts involving Salesforce Development Platform VA.

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.

Initial and annual Security Awareness Training includes security best practices, threat recognition, privacy, compliance and policy requirements, and reporting obligations. Upon completion of training, personnel must complete a security and privacy quiz with a passing score. All required VA privacy training must be completed in TMS prior to the user being provisioned.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 02/24/2021
3. *The Authorization Status:* ATO
4. *The Authorization Date:* 7/6/23
5. *The Authorization Termination Date:* 7/6/26
6. *The Risk Review Completion Date:* 03/12/2021
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 No or In Process, provide your ***Initial Operating Capability (IOC) date.*** N/A

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.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes, CIS system utilizes Salesforce Gov Cloud+. Under the contract: Salesforce Subscription Licenses, Maintenance and Support, Contract Number: NNG15SD27B.

This software utilizes the PaaS Service of Salesforce GovCloud+.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes, VA has full ownership of the PII that will be used by the Consolidated Internship Solution (CIS) platform.

Contract between VA and 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.

No ancillary data is shared or collected by the CIS tool.

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.

Yes, it is, as the VA is utilizing Salesforce GovCloud+. Information is only shared internally.

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).

The Consolidated Internship Solution (CIS) does not utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2024.04.10 11:48:11 -06'00'

Privacy Officer, Julie Drake

JAMES BORING Digitally signed by JAMES BORING
Date: 2024.04.09 11:25:11 -04'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI Digitally signed by MICHAEL DOMANSKI
Date: 2024.04.09 10:30:44 -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).

USA JOBS- Privacy Policy: https://www.usajobs.gov/help/privacy/

OPRM Site: https://www.oprm.va.gov/docs/Current_SORN_List_09_21_2021.pdf
SORN applicable to CIS: Human Resources Information Systems Shared Service Center (HRIS SSC)—VA (171VA056A/ 78 FR 63311).

HELPFUL LINKS:

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 Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices