Privacy Impact Assessment for the VA IT System called:

Salesforce - Contract Manager

Veterans Benefits Administration

Office of Business Integration (OBI)

Date PIA submitted for review:

7/25/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jean-Claude Wicks	Jean-Claude.Wicks@va.gov	202-502-0084
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000 X4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

Contract Manager is a Salesforce Module that is available for use by Contracting Officer Representatives (CORs) and those that the COR designates to manage VA Contracts. With this module, the COR can manage, track, and report on the various components of an actively awarded contract. This includes onboarding and offboarding activity, deliverables, communications, budget and invoices and other general contract related tasks. The module is internal to the VA and is not public facing.

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. The IT system name and the name of the program office that owns the IT system.

Contract Manager – Owned by Office of Business Integration

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

The Contract Manager module has been built in the Salesforce Government Cloud. The module is managed by the Office of Business Integration (OBI) and the platform is managed by the Office of Information and Technology (OI&T). Each business line is a customer and approver of new users into each version of the tool. The Contract Manager module has several features in which the COR can use to manage the content and various components of a VA Contract. These features include onboarding and offboarding activities, managing deliverables, recording communications, and tracking invoice payments and budgets and approver of new users into each version of the tool. The onboarding feature of the tool contains a file related list that is encrypted in which background investigation documents can be attached for helping the COR keep track of onboarding contractors.

C. Indicate the ownership or control of the IT system or project.

Office of Business Integration

2. Information Collection and Sharing

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

The total number of contractors whose information will be stored in Contract Manager is not calculable however it will range in the hundreds to thousands potentially in the first year. Also, it is anticipated that upwards to 100 hundred users may use this tool within the first year and that these

users will consist of VA Employees and Contractors. The Onboarding object contains a field to enter the name of a contractor and has no other PII fields in that object. However, the Files related list can be used to upload background investigation documents for contractors only that do contain PII or sensitive information.

E. A general description of the information in the IT system and the purpose for collecting this information.

Contract Manager can store information about contractors, contracts, deliverables, projects budgets, and invoices. The purpose of collecting this information is so that the COR can use the tool as a cloud-based COR file for managing contracts. Information collected includes contractor name, other names, DOB, place of birth, SSN, phone number, email, current and former address, resume, criminal history, financial standing and credit report, medication and drugs, fingerprint location, race, height, weight, hair and eye color, citizenship and passport information, gender, military service, selective service registration and education/work history.

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

There is no information sharing conducted by this system other than the fact that the information itself is being stored in the Salesforce government cloud.

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

This system services nationwide and not a regional system as it operates on the VA instance/org of Salesforce. While it can be used simultaneously by multiple users at different sites, the system is set up to operate the same way for individuals.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The legal authority to operate the system is The Privacy Act of 1974 (5 U.S.C. 552a(e)(4)) and the SORNs 145VA005Q3, 146VA005Q3, and 199VA10.

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?

This is not applicable.

D. System Changes

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

No

K. Whether 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.

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*
- ☐ 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)

Place of Birth
Other Names
Former Address
Resume
Criminal History

Financial Standing and Credit Report	Gender
Fingerprint Location	Military Service
Race	Selective Service Registration
Height and Weight	Prior Employer Information
Hair and Eye Color	Education History
Citizenship and Passport Information	

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

PII Mapping of Components (Servers/Database)

Contract manager consists of 0 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Contract Manager 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A					

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?

Contractors are providing this information directly to VA for Contract Onboarding purposes.

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.

Not applicable.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

Contract Manager is the source of the information, however not all PII listed is reportable only Full Name and VA Email Address are reportable.

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?

The data is manually entered and/or uploaded by the COR on the Onboarding object and is not created via electronic transmission from another system or created by the system itself.

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

The information is collected when an employee creates an Onboarding record and associates that record to a Contractor using the Full Name field and uploads any associated background investigation documents. All records must be created by the user and the background investigation documents provided by the contract serve as the source of information for what is input into the Contract Manager.

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.

No systemic accuracy checking is in place for this tool and depends on manual entry by the user or COR. The User or COR is responsible for ensuring the accuracy of the information entered.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Not applicable.

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

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

The Privacy Act of 1974 (5 U.S.C. 552a(e)(4)), is the legal authority to collect the information listed in question 1.1. The authority for maintenance of the system is Section 501(a), (b), and chapter 55 of Title 38, United States Code.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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 risk is similar with any other systems that if the wrong person were to have access to the information, it could be used to obtain financial resources and negatively impact a beneficiaries' lives.

Mitigation: The Salesforce Government Cloud requires all access utilize a PIV card while also logged onto the VA network through secure sites essentially a 2-factor authentication process. All VA employees accessing the system have had full background checks. Additionally, no external users will have access to this Salesforce module. Finally, the Full Name field will be encrypted per Digital Transformation Center (DTC) Security Requirements.

Section 2. Uses of the Information

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

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

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

Onboarding Object Information collected includes:
Contractor name: Used as an identifier.
Other names: Used as an identifier.
DOB: Used to identify age and confirm identity.
Place of birth: Used to confirm identity.
SSN: Used as an identifier.
Phone number: Used to contact individual.
Email: Used to contact individual.
Current and former address: Used to confirm identity and/or contact individual.
Resume: Used to determine employment suitability.
Criminal history: Used to determine employment suitability.
Financial standing and credit report: Used to determine employment suitability.
Medication and drugs: Used to determine employment suitability.
Fingerprint location: Used in PIV/badge issuance purposes.
Race, height, weight, hair and eye color: Used in PIV/badge issuance purposes.
Citizenship and passport information: Used to confirm identity.
Gender: Used to confirm identity.
Military service: Used to determine employment suitability.
Selective service registration: Used to determine employment suitability.
Education/work history: Used to determine employment suitability.

This information is part of attached documents to a record representing the onboarding contractor and is all used as part of the background investigation process for identification, contact purposes, and/or suitability for contract employment.

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.

Contract Manager does not do analytics on individuals. A dashboard will be utilized to summarize the Onboarding records for the employee but will not include PII information.

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.

Not applicable as the records created in this system are for the COR's reference and do not create new information about individuals.

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?

Documents containing PII are manually uploaded to Contract Manager behind VA Firewall to the Files Related List which is encrypted.

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

Documents containing PII (including SSN) are manually uploaded to Contract Manager behind VA Firewall to the Files Related List which is encrypted.

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

Documents containing PII (including SSN) are manually uploaded to Contract Manager behind VA Firewall to the Files Related List which is encrypted.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

VA Employees and authorized Contractors assigned to Contract Manager will have access. Access is determined by permission sets/rights that are approved by the application owner which is the Office of Business Integration.

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

Yes, a user only has access if provided permissions by Digital Transformation Center (DTC) but approved by OBI. Additionally, the COR must assign a user to a contract within the tool. This is documented with the technical design document and the user setup instructions that are maintained by DTC.

2.4c Does access require manager approval?

Access requires the approval of the business owner, OBI.

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

Yes, users that have access to PII in Contract Manager will have permission sets listed in their profile and a historic review of cases completed whereby access is granted is also being kept.

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

All users are responsible for assuring safeguards for PII per their Privacy Act training and by signing the Rules of Behavior agreement.

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*

Contractor name, other names, DOB, place of birth, SSN, phone number, email, current and former address, resume, criminal history, financial standing and credit report, medication and drugs, fingerprint location, race, height, weight, hair and eye color, citizenship and passport information, gender, military service, selective service registration and education/work history.

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.*

The below is the retention schedule for the Salesforce Developer Platform SFDP and applies to the Contract Manager module as well. 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).SFDP completes a 90-day retention cycle of all data including deletion. Active Data stays on disk until the data is deleted or changed. Customer-deleted data is temporarily available (15 days) from the Recycle Bin. Backups are rotated every 90 days, therefore changed or deleted data older than 90 days is unrecoverable. VA can export the data stored on the SFDP and retain it locally in order to meet

VA/NARA retention requirements. All data upon completion or termination of a contract will be turned over to VA and disposed of as soon as notice of the termination or completion is given.

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). SFDP completes a 90-day retention cycle of all data including deletion. Active Data stays on disk until the data is deleted or changed. Customer-deleted data is temporarily available (15 days) from the Recycle Bin. Backups are rotated every 90 days, therefore changed or deleted data older than 90 days is unrecoverable. VA can export the data stored on the SFDP and retain it locally in order to meet VA/NARA retention requirements. All data upon completion or termination of a contract will be turned over to VA and disposed of as soon as notice of the termination or completion is given notion period.

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

Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B)

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.

For data to be deleted from any Salesforce module object, a ticket must be created with the Digital Transformation Center (DTC) that outlines the data to be deleted. The module owner must approve of such records for deletion prior to DTC deleting. DTC is the administrative body that safeguards and manages the Salesforce platform.

SFDP completes a 90-day retention cycle of all data including deletion. Active Data stays on disk until the data is deleted or changed. Customer-deleted data is temporarily available (15 days) from the Recycle Bin. Backups are rotated every 90 days, therefore changed or deleted data older

than 90 days is unrecoverable. VA can export the data stored on the SFDP and retain it locally in order to meet VA/NARA retention requirements.

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.

The lower development environments for Salesforce do not allow the use of PII. For the Contract Manager Onboarding component, test data is utilized/created. Because the configuration of the component does not have any validation against other VA systems of record, real Veteran data is not required to test the functionality of the system. Training for users is done in the lower environments and test data is used.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System 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:

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

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

Follow the format below:

Privacy Risk: The risk to maintaining data within Contract Manager is the longer time frame information is kept, the greater the risk that information possibly will be compromised or breached.

Mitigation: To mitigate the risk posed by information retention, the Contract Manager Module adheres to the VA RCS 10-1. All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500.

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

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the 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: Although Contract Manager is not currently sharing PII with any other VA IT systems, the internal risk is that a user may see information related to an onboarding contractor for a contract the user is not assigned to as a COR.

Mitigation: This risk is mitigated in several ways. First, the COR of a contract determines who these records can be shared with. The system wide default for onboarding records is set to private meaning no one can see those records unless those records are shared with them which is controlled by the COR of a contract. Second, a user has to request access and be approved to use the application. Simply being a user of the application does not grant access to view records. Third, the COR has to assign a user to a specific role in the application and there are only a few roles that allow for viewing of onboarding records. Lastly, because the application is internal only users have signed the Rules of Behavior agreement and completed all privacy training and are responsible for the safekeeping of any PII/PHI.

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				

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.

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

Follow the format below:

Privacy Risk: There is a risk that information could be accessed by unauthorized individuals when sharing externally.

Mitigation: Information in Contract Manager should not be shared with unauthorized individuals. All Contract Manager users must undergo annual training and certification of the Privacy Information Security Act Rules of Behavior training. The certification ensures the end user understands the rules regarding sharing sensitive information with the correct individuals and on a need to know basis. Violations of this rule can be traced back to the individual which would require an audit of all systems accessed and actions completed by the end user to determine when, how, what, and why sensitive information was shared. Salesforce audit logs can assist in this effort. All user in the Salesforce VA organization have Single Sign On (SSO) which is only valid so long as they are up to date with the rules of behavior that are currently listed in our VA Network.

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.

This is covered by SORN 145VA005Q3, 146VA005Q3, and 199VA10/86 with the links below.

145VA005Q3/73 FR 15852 Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA

https://www.govinfo.gov/content/pkg/FR-2022-07-01/pdf/2022-14118.pdf

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

https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf

199VA10/86 FR 28928 VA Employee Whole Health Program Records-VA

https://www.govinfo.gov/content/pkg/FR-2021-05-28/pdf/2021-11316.pdf

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

Not applicable

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.

Not applicable

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.

Contractors must provide the information collected by Contract Manager in order to work for the VA. If they decline to provide the information they would not be allowed to work on the contract and for the VA.

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.

Contractors must provide the information collected by Contract Manager in order to work for the VA. If they decline to provide any part of the information they would not be allowed to work on the contract and for the VA.

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?

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

Privacy Risk: There is a risk that individuals may not be aware of this system and that it is collecting PII data.

Mitigation: This PIA acts as a means of notification to individuals that Contract Manager is retaining PII Data. Additionally, SORN 145VA005Q3, 146VA005Q3, and 199VA10/86 act as a form of notice.

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.***

The data collected within the Production component is not exempt from FOIA/Privacy Act requests and would be handled by the centralized group processing VBA FOIA/Privacy Act requests. Individuals would need to submit a FOIA or Privacy Act request in order to obtain copies of the information stored in Contract Manager.

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).

System is not exempt from Privacy Act.

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

For an individual to obtain access to their information, the FOIA process for VA would need to be followed.

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.

If a wrong Full Name is entered by an employee on the Onboarding record, that employee would have the ability to edit the Full Name field to make any corrections as necessary. Because the Contractor being onboarded will not use this module, they would not know if any values, fields, or forms have errors. The COR or end user managing the Onboarding record would reach out to the Contractor or POC the works on behalf of the Contractor to obtain correct values, fields, or forms to enter into the Onboarding record. know if any values, fields, or forms have errors. The COR or end user managing the Onboarding record would reach out to the Contractor or POC the works on behalf of the Contractor to obtain correct values, fields, or forms to enter into the Onboarding record.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The employees can correct their own records if needed. If the record is selected for a quality review, then the quality reviewer can potentially notify the employee to correct the Full Name. The employee's supervisor would be able to notify the employee as well if a Full Name needs to be corrected.
The individual to whom the data or PII pertains would not be notified of any corrections as this system is internal to VA for the use of CORs to manage their contracts. If there are corrections needed the COR or Contract Manager user would reach out separately to the affected Contractor to obtain correct information to update the record in the module.

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.

This is not applicable to Contract Manager.

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 individuals will not know how to access or correct information in the system.

Mitigation: Individuals can submit a FOIA request to obtain copies of their information in the system. The COR will also contact the individual directly if any information needs to be corrected.

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.

New users submit a request for access through the Digital Transformation Center (DTC). The DTC then assigns the request to the individuals who have admin access to the module and the access is then granted or denied based on the information the user provided. The DTC is then notified of the approval/disapproval and DTC acts on the request based on the admin's response.

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?

No users from agencies outside VBA have access to Contract Manager within the Salesforce platform in the production environment. The VBA employees are able to edit entries that were part of the original submission as well as other items needed for case management and workload reporting.

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

Roles can be established in Contract Manager for read only or edit access. Typically, read only is provided to users who need to see entries but show not be allowed to make changes.

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.

VA contractors from the DTC and possibly from the Contract being managed by the COR will have access to the production environment. VA Contractors are required to complete the Privacy and Information Security Agreement yearly, also known as the Rules of Behavior. Signing the Rules of Behavior ensures proper conduct and management of sensitive information.

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

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

No additional system specific privacy training is provided for end users of Contract Manager. All users are required to have the standard VA Privacy Awareness and Cyber Security training within the Talent Management System (TMS). General Training includes VA Privacy and Information Security Awareness and Rules of Behavior, TMS 10203 - Privacy and Health Insurance Portability and Accountability Act (HIPPA), VA On-Boarding enterprise-wide training, and annual information security training. After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained

via electronic acknowledgment and is tracked through the TMS system. After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the privacy and security awareness training.

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:* Please provide response here09/13/2022
3. *The Authorization Status:* Active
4. *The Authorization Date:* Please provide response here09/30/2021
5. *The Authorization Termination Date:* Please provide response here08/07/2023
6. *The Risk Review Completion Date:* Please provide response here09/23/2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* FIPS 199 Classification is a Moderate System.

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.***

Not applicable for the application

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

9.2 Does the contract with the 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/PHI that will be shared through the Salesforce – Office of Inspector General (OIG) Legal Case Management System. Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD7B.7B.

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.

Please provide response here Ancillary data is not collected by Salesforce. VA has full ownership over the data stored in the Contract Manager application.

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

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

VA has full authority over data stored in Contract Manager.

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).

Contract Manager 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**

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

Signature of Responsible Officials

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

JEAN-CLAUDE WICKS

Digitally signed by JEAN-CLAUDE WICKS
Date: 2023.08.04 07:36:41 -06'00'

Privacy Officer, Jean-Claude Wicks

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2023.08.08 11:45:25 -04'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2023.08.07 08:12:58 -04'00'

Information System Owner,Michael Domanski

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

145VA005Q3/73 FR 15852 Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA

https://www.govinfo.gov/content/pkg/FR-2022-07-01/pdf/2022-14118.pdf

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

https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf

199VA10/86 FR 28928 VA Employee Whole Health Program Records-VA

https://www.govinfo.gov/content/pkg/FR-2021-05-28/pdf/2021-11316.pdf

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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