Privacy Impact Assessment for the VA IT System called:

Salesforce - VA TrackForce

Office of Business Integration

Veterans Benefits Administration

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	James Boring	James.Boring@va.gov	215-842- 2000, Ext: 4613
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.

VA TrackForce is a tool used to perform two functionalities. First, it is used to keep track of workload tasks of different offices. Workload tasks by all offices are similar but may vary based on business need but do not contain PII/PHI other than the Employee name. Second, it is used to keep track of media inquiries or inquiries to VA from external sources. Media Inquiries will have name, phone, and email of external contact such as a reporter and one group will have listed an optional entry for Veteran Name with a Veteran File Number formula lookup. There are other sub-functions such as calendar tracking or customer relationship tracking that are not in use by any group.

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.*

The Salesforce - VA TrackForce / Office of Business Integration module was built in the Salesforce Government Cloud Plus. The data in the module is controlled by the Office of Business Integration, while the platform is managed by the Office of Information and Technology (OI&T). Each business line is a customer and approver of new users for each version of the tool.

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

The SalesForce - VA TrackForce module has two components: Task with Work Items and Media Inquiries. Both of these functions enable the VA employee(s) to create a record that is used to track a task, share the task with colleagues, upload documents against the record, and create reports and dashboards to track inventory and business line performance. Creating a record is necessary to accomplish the business needs of the VA Employee. Creating records under the Media Inquiry may contain a Veteran Full Name and file number/SSN. The Tasker and Work Item objects do not contain any sensitive or PII information.

The media inquiry and tasker functionalities are used by the below program offices.

Media Inquiries Functionality:
1. Office of Communications
2. National Cemetery Administration Office of Public Affairs

3. Office of Inspector General (OIG) Media Inquiry
4. Office of Research and Development (ORD) Media Inquiry.

Tasker and Work Item Functionality:
1. Office of Executive Review (OER) – includes calendar tracking
2. NCA Executive Review
3. Office of Communications (OC)
4. Program Initiatives and Integrity Control (PIICS)
5. Office of Strategic Support and Initiatives (OSSI)
6. Office of Financial Management (OFM) – Discretionary Budget Team
7. Office of Business Integration (OBI)
8. Education Service (EDU)
9. Office of Field Operations (OFO)
10. Office of Policy and Oversight (OPO)
11. Office of Mission Support (OMS)
12. Office of Transition and Economic Development (OTED)
13. Under Secretary for Benefits (USB) and Office of Principal Deputy Under Secretary for Benefits (PDUSB)
14. Taxonomy used by Change Control Board group in OBI

Customer Relationship – Not in Use
1. Office of Business Integration (OBI) Customer Virtual Profile (CVP)

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

Salesforce Government Cloud is hosted on a Salesforce Government Cloud Plus major platform, with an eMASS ID of 2010 for the minor Salesforce platform of VA TrackForce. Salesforce ownership is updated to reflect systems that are controlled by the VA, but not owned or operated by the VA.

The module is managed and maintained by the OI&T. Each business line is a customer and approver of new users for each version of the tool.

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 VA employees using the system currently is over 100 users.

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

File numbers, claim numbers, or Social Security Numbers are not used throughout the Tasks with Work Items. There is, however, a formula field on the Media Inquiry object that reflects the Veteran SSN from the Contact object using the related lookup field on the same page. Because this is a formula field on the Media Inquiry object, the SSN data is not actually stored in the VA TrackForce module, as it is stored in the Contact object. The related lookup field points to the Veteran's name only.

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

This system services nationwide and not a regional system. There are no integrations between this module and anything else internally in the Salesforce Platform or externally to any system.

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.*

While multiple sites in VA are able to utilize the module; the process for how the module is used is similar regardless of the site using the tool. The Tasker and Work Item objects do not contain any sensitive or PII information. Only the media inquiry functionality may contain PII information.

3. Legal Authority and SORN

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
38 U.S.C. 501.

75VA001B/87 FR 36584 ‘‘Case and Correspondence Management (CCM)–VA’’ (75VA001B).
https://www.govinfo.gov/content/pkg/FR-2022-06-17/pdf/2022-13066.pdf

58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

The system does use Salesforce Government Cloud Plus technology.

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?*

The system does use Salesforce Government cloud technology. The SORN does not require amendment or revision.

D. System Changes

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

There are no expected changes to the business process based on this PIA.

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

There are no expected changes to the technology based on this PIA.

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)

VA File Number/ Social Security Number

PII Mapping of Components (Servers/Database)

VA TrackForce consists of 0 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VA TrackForce 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	**N/A**	**N/A**	**N/A**	**N/A**	**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?

The source for information in the system is employee entered information regarding the tracking of tasks work items and media inquiries.

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.

For the Media Inquiry object, the SSN is displayed from the Contact object based upon the end user entering a Veteran Name into the Veteran Name related lookup field that points to the Contact Object. The Contact object resides inside Salesforce and is a shared standard object used by virtually all other Salesforce modules. This information is being entered by the VA Employee manually, there are no connections or integrations. The Contact object is a mutually shared object used by all Salesforce modules.

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

Salesforce

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 information is collected when an employee creates a Media Inquiry record and associates that record to a Veteran using the Veteran Name related lookup field that points to the Contact object. Completing this field is optional as not every record is relatable to a Veteran.

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 not collected on a form is not subjected to the Paperwork Reduction Act.

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.

The employee selects a Veteran's name from the related lookup on the Media Inquiry object that points to the Contact object. This related lookup enables the formula field to pull the File Number as it appears on the Contact object for that Veteran. Users of this module can create a new Veteran record if one does not exist, including adding a File Number.

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.

Ultimately, the enterprise Master Person Index initiative to match/synchronize Veterans on the Contact object will ensure that the information in the Contact object is accurate. This data is technically not retained by this module because it is derived from the Contact object. While the name appears on the Media Inquiry object, the SSN is a formula field that does not actually contain the data; the SSN is stored on the Contact object. VA TrackForce does not connect to or use the MPI solution because it only applies to the Contact object.

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 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 risk is similar to that of any other system in that if the wrong person gains access to the information, it can be used to obtain financial resources and negatively impact the lives of beneficiaries.

Mitigation: The Salesforce Government Cloud requires all access to utilize a PIV card while also logging 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 File Number 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.

Veteran Name: Used as an identifier
Veteran File Number/SSN: Used as an identifier.
Employee Name: used to identify workload task request
Reporter Name: used to identify and track media inquiry and reports
Reporter Email: used to identify, contact and track media inquiry and reports
Reporter Telephone: used to identify, contact and track media inquiry and reports

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.

VA TrackForce does not do analytics on individuals.

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.

A dashboard will be utilized to summarize the Media Inquiry records for the employee but will not include SSN or Veteran Name information.

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?

Salesforce Shield provides Shield Platform Encryption

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

SSN field is encrypted on the contact object.

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

Salesforce Shield provides Shield Platform Encryption which allows for natively encrypting sensitive data and protects sensitive data from unauthorized users.

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 VA TrackForce will have access. Access is determined by permission sets/rights approved by the VA TrackForce application owner. There are presently 8 business owners who act independently to approve individuals seeking access to the approved business line's iteration of VA TrackForce.

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

New users apply for access via the Digital Transformation Center (DTC). The DTC is the VA-appointed governing body for VA use of the Salesforce platform, and it decides what can and cannot go on the production platform. The DTC routes the request to personnel with admin access to the module, and access is given or denied based on the information provided by the user. The DTC is then notified of the permission or rejection, and the DTC acts on the request depending on the administrator's response. Salesforce keeps track of access requests, approvals, and denials. PII in Salesforce applications is encrypted, and every user with access to the Salesforce platform is required to adhere to the Privacy Information Security Agreement Rules of Behavior once a year, which govern how workers use/protect PII/PHI.

2.4c Does access require manager approval?

Yes, access is determined by permission sets/rights that are approved by the VA TrackForce application owner.

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

Audits can also be undertaken to track any misuse or unauthorized usage of PII/PHI. Salesforce keeps track of access requests, approvals, and denials. PII in Salesforce applications is encrypted, and every user with access to the Salesforce platform is required to adhere to the Privacy Information Security Agreement Rules of Behavior once a year, which govern how workers use/protect PII/PHI.

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

VA TrackForce application owner and Digital Transformation Center (DTC).

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*

Veteran Name
Veteran file number/SSN
Employee Name
Reporter Name
Reporter Email
Reporter Telephone

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.*

Retention of Records is expected to be 75 years. 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

3.3 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?

The below is the retention schedule for the Salesforce Developer Platform SFGCP and applies to the VA TrackForce module as well.

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

SFGCP 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 statutes, including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFGCP records are retained according to Record Control Schedule 10-1, Section 4 (Disposition of Records) (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf).

SFGCP completes a 90-day retention cycle for 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 SFGCP 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.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, Records Schedule Number DAA–0015–2018–0002. https://www.govinfo.gov/content/pkg/FR-2022-06-17/pdf/2022-13066.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.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. 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. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

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

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

The lower development environments for Salesforce do not allow the use of PII. For the VA TrackForce Media Inquiry 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 VA TrackForce 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 VA TrackForce 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 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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:

<u>Privacy Risk:</u> VA TrackForce is not currently sharing PII with any other VA IT systems.

<u>Mitigation:</u> VA TrackForce is not currently sharing PII with any other VA IT systems.

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***	***List the method of transmission and the measures in place to secure data***

			more than one)	
N/A	N/A	N/A	N/A	N/A

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

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

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

Follow the format below:

<u>Privacy Risk:</u> Information from Salesforce - VA TrackForce is not shared externally.

<u>Mitigation:</u> Information from Salesforce - VA TrackForce is not shared externally.

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.

(https://www.oprm.va.gov/privacy/systems_of_records.aspx).
75VA001B/87 FR 36584 ‘‘Case and Correspondence Management (CCM)–VA’’ (75VA001B).
https://www.govinfo.gov/content/pkg/FR-2022-06-17/pdf/2022-13066.pdf

58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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

Notice has been provided in the following SORNs.
75VA001B/87 FR 36584 ‘‘Case and Correspondence Management (CCM)–VA’’ (75VA001B).
https://www.govinfo.gov/content/pkg/FR-2022-06-17/pdf/2022-13066.pdf

58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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.

The notice was provided in the publishing of the following SORNs.

75VA001B/87 FR 36584 ‘‘Case and Correspondence Management (CCM)–VA’’ (75VA001B).
https://www.govinfo.gov/content/pkg/FR-2022-06-17/pdf/2022-13066.pdf

58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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.

The information in VA TrackForce is shared in the Salesforce Contact Object and is already part of Salesforce. No new information is being solicited or provided by individuals. Therefore, no penalty or denial of service is required.

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.

The information in VA TrackForce is shared in the Salesforce Contact Object and is already part of Salesforce. No new information is being solicited or provided by individuals. The PIA for MPI which is where the Contact Object obtains its data should cover any instance under 6.3.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

Mitigation: This PIA acts as a means of notification to individuals that Salesforce - VA TrackForce is retaining PII Data. VA TrackForce uses Veteran name and file number from the Contact Object which pulls its information from MPI. Further information can be found in the PIA for MPI. Additionally, SORNs 75VA001B and 58VA21/22/2886 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 VA TrackForce.

The VA FOIA website: https://department.va.gov/foia/

The SORNs website:

75VA001B/87 FR 36584 ''Case and Correspondence Management (CCM)–VA'' (75VA001B).
https://www.govinfo.gov/content/pkg/FR-2022-06-17/pdf/2022-13066.pdf

58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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 not exempt from the privacy act.

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

For an individual to obtain access to their information the FOIA process for VA would need to be followed, as the system is not exempt from the privacy act.

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 Media Inquiry record, that employee would have the ability to edit the Full Name field to make any corrections as necessary because it was manually entered.

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.

VA TrackForce uses Veteran name and file number/SSN from the Contact Object which pulls its information from MPI. Further information can be found in the PIA for MPI.

The employees can correct the Veteran referenced records if necessary. 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 on the Veteran referenced record.

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 tracking media inquiries by VA Central Office employees, in which occasionally a Veteran may be referenced in the media inquiry.

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.

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 VA TrackForce.

The VA FOIA website: https://department.va.gov/foia/

The SORNs website:

75VA001B/87 FR 36584 ''Case and Correspondence Management (CCM)–VA'' (75VA001B).
https://www.govinfo.gov/content/pkg/FR-2022-06-17/pdf/2022-13066.pdf

58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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 be unaware of how they can access or correct their information in the system.

Mitigation: Individuals can submit a FOIA or Privacy Act Request to obtain a copy of their information in the system. However, because the data in VA TrackForce is from the Contact object, which is provided by the MPI, the PIA for the MPI should provide additional mitigation strategies.

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 the 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 VA have access to Salesforce - VA TrackForce within the Salesforce platform in the production environment.

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.

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.

8.2 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 is 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 VA TrackForce. All users are required to have the standard VA Privacy Awareness and Cyber Security training within the Talent Management System (TMS).

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

Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 09/13/2022
3. *The Authorization Status:* Active
4. *The Authorization Date:* 09/30/2021
5. *The Authorization Termination Date:* 08/07/2023
6. *The Risk Review Completion Date:* 09/23/2021
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.***

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 TrackForce system utilizes Salesforce Gov Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The SalesforceGovernment Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that ishosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services(AWS) GovCloud West. Under the contract

"Salesforce Subscription Licenses, Maintenance, and Support", Contract Number: NNG15SD27B. This software utilizes the PaaS Service of Salesforce Gov Cloud.

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 VA TrackForce platform. Contract agreement "Salesforce Subscription Licenses, Maintenance, and Support", Contract Number: NNG15SD27B.

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

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

This question is related to privacy control DI-1, Data Quality.

No ancillary data is being collected by this 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, as VA is utilizing Salesforce Gov Cloud Plus. 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).

VA TrackForce 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**

ID	Privacy Controls
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 provided in this Privacy Impact Assessment is true and accurate.

JEAN-CLAUDE WICKS

Digitally signed by JEAN-CLAUDE WICKS
Date: 2023.08.01 10:46:07 -06'00'

Privacy Officer, Jean-Claude Wicks

JAMES BORING

Digitally signed by JAMES BORING
Date: 2023.08.01 17:27:43 -04'00'

Information Systems Security Officer, James Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2023.08.01 14:15:51 -04'00'

Information Systems 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).

SORN’s applicable for the system:

75VA001B/87 FR 36584 ‘‘Case and Correspondence Management (CCM)–VA’’ (75VA001B).
https://www.govinfo.gov/content/pkg/FR-2022-06-17/pdf/2022-13066.pdf

58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.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