Privacy Impact Assessment for the VA IT System called:

VA TrackForce

Office of Business Process Integration
Veterans Benefits Administration

Date PIA submitted for review:
2/25/2022

System Contacts:

<table>
<thead>
<tr>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Simon K. Caines</td>
<td><a href="mailto:Simon.caines@va.gov">Simon.caines@va.gov</a></td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>James Boring</td>
<td><a href="mailto:James.Boring@va.gov">James.Boring@va.gov</a></td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Michael Domanski</td>
<td><a href="mailto:Michael.Domanski@va.gov">Michael.Domanski@va.gov</a></td>
</tr>
</tbody>
</table>
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 Salesforce Module that is used by various business lines mostly in the VA Central Office for Veterans Benefits Administration (VBA) to track tasks and work items related to business line work. The end users are using this tool to create records that are used to track the status/progress of a task that they are assigned. The end user also uses that record to associate documents and collaborate between other staff members. Reports and Dashboards are used to track and analyze staff work and performance, inventory and status of tasks and works items. The end users are VBA Employees and represent business lines such as Office of Executive Review (OER), Office of Strategic Engagement (OSE) and others. At the time of this PIA there are a total of 8 business lines and over 100 users that have access to use this Salesforce Module. Each business line has their own version of the tool and users are grouped by business line and are only able to see tasks and work items that pertain to their business line and are not able to see tasks and work items in other business lines. Included in VA TrackForce is the ability to track Media Inquiries which is used exclusively by the Office of Strategic Engagement.

Overview

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

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?
The VA TrackForce module has been built in the Salesforce Government Cloud. The module is managed by the Office of Business Process Integration, 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 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.

The total number of VA employees using the system currently is over 100 users. 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 name only.

This system services nationwide and not a regional system.

The Tasker and Work Item objects do not contain any sensitive or PII information.

There are no integrations between this module and anything else internally in the Salesforce Platform or externally to any system.

To gain access to VA TrackForce users must use of Single Sign On (SSO) service using a Personal Identification Verification (PIV) card and associated credentials.

VA TrackForce is covered by the Salesforce Authority to operate (ATO).

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

The SORN 121VA10P2 covers the data used in VA TrackForce.

The system does use Salesforce Government cloud technology.

Ownership rights to PII data should be covered in the Salesforce contract and VA has ownership of the data as it persists on the Salesforce Government Cloud.

Per NIST 800-144, it is understood that the organization (VA) is ultimately accountable for security and privacy of data held by Salesforce on our behalf.

The magnitude of harm if PII was disclosed would have a negative impact on both the Cloud Service Provider (CSP) and VA. While there is limited data in the system through the Production component, that data could be used to negatively impact individuals’ credit, jobs, and other areas sensitive
information can be used inappropriately. This could leave the CSP and VA open to litigation. The Privacy Act of 1974 is the legal authority to operate.

**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://www.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
- [x] Personal Phone Number(s)
- [ ] Personal Fax Number
- [x] Personal Email Address
- [ ] Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- [ ] Financial Account Information
- [ ] Health Insurance Beneficiary Numbers
- [ ] Certificate/License numbers
- [ ] Vehicle License Plate Number
- [ ] Internet Protocol (IP) Address Numbers
- [ ] Current Medications
- [ ] Previous Medical Records
- [ ] Race/Ethnicity
- [ ] Tax Identification Number
- [ ] Medical Record Number
- [ ] Gender
- [ ] Integration Control Number (ICN)
- [ ] Military History/Service Connection
- [ ] Next of Kin
- [ ] Other Unique Identifying Information (list below)
PII Mapping of Components

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.

PII Mapped to Components

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

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

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

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

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

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

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.
1.3 How is the information collected?

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

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

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.

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

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

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

The 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 to include adding a File Number. Ultimately, the enterprise Master Person Index initiative to match/synchronize Veterans on the Contact object will ensure that information in the Contact object is accurate. This module does not technically retain this data as it relies on the Contact object as the source of data. While the name appears on the Media Inquiry object, the SSN is a formula field that doesn’t actually store the data, the Contact object is where the SSN is stored. VA TrackForce does not connect to or utilize the MPI solution as that relates only 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.

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 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 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 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
SSN: Used as an identifier

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

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

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

VA TrackForce does not do analytics on individuals. 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?

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

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

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

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. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

VA Employees and authorized Contractors assigned to VA TrackForce will have access. Access is determined by permission sets/rights that are approved by the VA TrackForce application owner. There are currently 8 business owners that act independently to approve individuals seeking access to the approving business line’s iteration of VA TrackForce.

New users submit a request for access through the Digital Transformation Center (DTC). Digital Transformation Center (DTC) is the VA appointed governing body over VA use of the Salesforce platform and determine what is allowed or not allowed to go onto the production platform. The DTC 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 takes action on the request based on the admin’s response. Requests, approvals, and denials of access are recorded within Salesforce. PII in Salesforce applications is encrypted and each user that has access to the Salesforce platform has to agree to the Privacy Information Security Agreement Rules of Behavior once a year that dictates how employees use/safeguard PII/PHI. Additionally, audits can be performed to track misuse or any prohibited use of PII/PHI.
Any disciplinary actions for misuse of the information would be covered in VBA’s privacy policy and by governing regulations.

The use of the information is critical to the success of the mission and fully supports the USB’s current priorities.

**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

**3.2 How long is information retained?**

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

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

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](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)? If so please indicate the name of the records retention schedule.**

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

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

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

SFGCP 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 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.

3.4 What are the procedures for the elimination of SPI?

*Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?*

This question is related to privacy control DM-2, Data Retention and Disposal

All records will be electronic, and the details of their disposal will be documented within the SORN that covers the Master Person Index (MPI) and should also be recorded as part of the Software as a Service (SAAS) documentation/contract. The SORN 121VA10P2 covers the PII in VA TrackForce.

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.

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

*Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what*
controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

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.

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**

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

4.2 **PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

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

**Privacy Risk:** NA – VA TrackForce is not currently sharing PII with any other VA IT systems.

**Mitigation:** NA – 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*

| List External Program Office or IT System information is shared/received with | List the purpose of information being shared / received | 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 | List the method of transmission and the measures in place |}

---

Version Date: October 1, 2021

Page 14 of 27
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 VA TrackForce should not be shared with unauthorized individuals. All VA TrackForce 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 notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

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

External users do not use VA TrackForce so there is no privacy policy. 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. The SORN 121VA10P2 covers the PII in VA TrackForce.

https://www.oprm.va.gov/docs/CurrentSORNList_4_29_20.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.

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: Information stored in the shared Salesforce object contains PII.

Mitigation: This PIA acts as a means of notification to individuals that 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.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

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

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

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

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.

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 is 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 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.

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

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

This is not applicable to VA TrackForce.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.

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

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

Follow the format below:
**Privacy Risk:** There is a risk that information is individuals are 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 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?**

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

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

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

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

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.

No users from agencies outside VBA have access to VA TrackForce 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.

8.2 **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 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?

If Yes, provide:

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

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

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

In Process: Initial Operating Capability (IOC) date has passed and this application is currently in use. “Assess only” eMASS package is in progress.

Version Date: October 1, 2021
Page 21 of 27
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).

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.

Yes, TrackForce system utilizes Salesforce Gov Cloud. Under the contract: “Salesforce
Subscription Licenses, Maintenance and Support”, Contract Number: NNG15SD27B. This
software utilizes the PaaS Service of Salesforce 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)

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 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**

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

Version Date: October 1, 2021

Page 24 of 27
<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
Signature of Responsible Officials

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

Simon K. Caines
3430973
Digitally signed by Simon K. Caines 3430973
Date: 2022.03.31 13:25:28 -04'00'

Privacy Officer, Simon K. Caines

James C. Boring
149438
Digitally signed by James C. Boring 149438
Date: 2022.03.31 14:37:21 -04'00'

Information System Security Officer, James Boring

Michael S. Domanski
326889
Digitally signed by Michael S. Domanski 326889
Date: 2022.03.31 13:45:43 -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).

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