Privacy Impact Assessment for the VA IT System called:
Salesforce: Attorney Fee Inventory Tracker (AFIT)
Office of Administrative Review
Veterans Benefits Administration

Date PIA submitted for review:
05/23/2022

System Contacts:

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Bertha L. Brown</td>
<td><a href="mailto:berth.a.brown@va.gov">berth.a.brown@va.gov</a></td>
<td>202-461-9740</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>
<td>215-842-2000 x4613</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>
<td>727-595-7291</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.

The Attorney Fee Inventory Tracker (AFIT) is a Salesforce Platform application that supports Office of Administrative Review (OAR) in streamlining its workload to track claims and/or appeals with a valid attorney fee agreement. This system that will serve as the primary source of communication between the Decision Review Operations Centers (DROC) and the Support Services Division (SSD) in regard to processing attorney fees claims.

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?

Attorney Fee Inventory Tracker (AFIT) is owned by Office of Administrative Review (OAR) which will be developed on the Salesforce platform. The Salesforce platform is owned by Office of Information Technology (OIT) as it is a Software as a Service (SaaS) system.
AFIT helps streamlining attorney fee workload, allowing stations and central office employees to track claims and/or appeals that have a valid attorney fee agreement between a Veteran/claimant and an accredited attorney/agent.

AFIT is a stand-alone system that will be utilized by approximately 300 VA employees serving as the primary source of communication and document sharing between the Agent and Attorney Fee Coordinators (AAFC) located within Decision Review Operations Centers (DROC) and Veterans Service Centers (VSC) and their local Support Services Divisions (SSD) regarding specific attorney fee cases. AFIT will allow for document sharing such as sharing system screen prints, award calculations, interoffice memos, and Veteran notification letters. Additionally, OAR employees and other central office entities will use AFIT for oversight, reporting, workload management and to respond to attorney fee inquiries.

Veterans can elect to represent themselves, work with a Veteran Service Officer free of charge or hire an accredited agent/attorney to represent them for a fee. Agents/attorneys can only charge an attorney fee for non-original claims. Once an AAFC determines that there is 1) a valid fee agreement associated with a non-original claim and 2) the Veteran is entitled to a past-due benefit they will input relevant information into AFIT to begin tracking the case until VA processes and sends out all appropriate payment.

Although AFIT data is stored in the Salesforce FedRAMP cloud, it remains the property of the VA and as such, the VA remains responsible for the security and privacy of this data. The VA enforces these protection requirements through the implementation of its cybersecurity policies and the Risk Management Framework (RMF) process. Under the RMF process, the system has a Data Security Categorization of Moderate, with the impacts of a data compromise being identified in the AFIT Data Security Categorization (DSC) memo. The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.

This PIA for AFIT will not
• Cause any business processes to change,
• Cause any technology changes, nor
• Affect the relevant SORN applicable for the system is Accreditation Records –VA. 01VA022(consolidated). The SORN covers all Personally Identifiable Information (PII) used in AFIT.

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 Account Information
- Health Insurance Beneficiary Numbers Account 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
- Integration Control Number (ICN)
- Military History/Service Connection
- Next of Kin
- Other Unique Identifying Information (list below)

Veteran File Number, Veteran benefit claim ID, Veteran date of claim, claim end product, Agent/Attorney’s First and Last name, agent/attorney business mailing address.

**PII Mapping of Components**

Attorney Fee Inventory Tracker (AFIT) consists of 0 key components (databases). If AFIT did contain components, then each component would have been analyzed to determine if any elements of that component collect PII. The type of PII collected by AFIT 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.

**PII Mapped to Components**

<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></td>
<td></td>
<td></td>
<td></td>
<td></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.*

The source of information is received through an Attorney Fee agreement. This is submitted to VA by the accredited agent/attorney who has signed a fee agreement with a Veteran in order to collect a fee in return for representing the Veteran on a VA claim. There is no prescribed form for the fee agreement, but the fee agreement is usually submitted with or after the attorney submits a complete VA Form 21-22a, Appointment of Individual as Claimant’s Representative.

DROC and VSC employees will enter Veteran and attorney information and SSD employees will review and add additional information for the DROC and VSC employees to review and act on. VA employees working within the VSCs and DROCs will enter information on the specifics of the attorney fee claim. OAR and other central office entities will have access to review, run reports and check the status on completed and pending cases entered in AFIT.

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.

Veteran claim request will be entered manually by VA employees and VA contractors into the AFIT tool which then will be utilized by OAR employees to track progress on each of these cases.

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 Veteran and identifying information associated with the Veteran will be validated with the Master Person Index (MPI) in real-time. Depending on the decision made by the DROC/VSC, the SSD employee will verify that the input information is correct and aligns with the award information submitted. OAR and other central office entities will review reports and complete spot checks to ensure pending and completed cases were input correctly.

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, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 38, United States Code, Sections 501(a), 5901, 5902, 5903 and 5904.
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 of exposure is associated with unauthorized users accessing the tool. The Veteran and the benefits information is at a risk of exposure. Based on FIPS categorization to the tool is categorized at a moderate impact.

**Mitigation:** Salesforce platform provides data and file encryption at rest and in transit. User access is based on role-hierarchy. Based on the role the VA employee, they can access the tool and authorize payment for Veteran’s attorney.

**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.

AFIT collects information of Veterans, VA Employees and Members of the Public data listed below:
• Veteran First and Last Name: identification of the veteran for benefit purposes
• Veteran File Number: identification of the Veteran for benefit purposes
• Social Security Number (SSN): identification of the Veteran for benefit purposes
• Benefit Claim ID: identification of the Veteran for benefit purposes
• Veteran Date of Claim: Identifies the date VA received the claim
• Claim End Product: Identifies the type of claim
• Employee Name: three different employee names are captured by the tool
  1. FAS Employee - identifies the VA employee who conducts the initial audit
  2. Authorizing FAS Employee - identifies the VA employee who authorizes the financial transaction
  3. AAFC Employee – identifies employee who determines the applicable financial fee allocation and provides what action needs to be taken by the finance.
• Attorney First and Last Name: Identifies agent/attorney for payment purposes
• Attorney Mailing Address: Identifies agent/attorney for payment purposes

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

Salesforce reporting dashboards are used for reporting metrics to leadership and to workload manage pending attorney fee cases. The tool will also allow for oversight and quality reviews of attorney fee cases.

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 PHI/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

AFIT system (Salesforce) is an encrypted secure system. Data in transit and at rest are protected by HTTPS site-to-site encryption. PII data is encrypted at rest and in transit with Salesforce Shield encryption. SSN is PII data, encrypted at rest with Salesforce Shield encryption.

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.

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA’s stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for Information Technology [the VA Authorizing Official (AO)]. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans’ information is used, stored, and protected.

Access Control:
Accessibility to data is granted based on the permission sets and role-based hierarchy applied based on FedRAMP Salesforce Gov Cloud Plus platform. Account creation is managed and offered through VA via two factor authentication (2FA) Personal Identity Verification (PIV) card and/or AccessVA. Single Sign On external (SSOe) is used to provide credential access to VA modules/communities residing in the Salesforce application, the determinant of access is organizational affiliation rather than personal identity. For some module(s) the required organizational e-mail confirmation and multi-factor authentication (MFA) will be enforced.

Version Date: October 1, 2021
Page 9 of 27
(IAL1), but no identity proofing (IAL2) and vice versa. The managers will reject any applications from individuals who do not work with them, do not require access, or are not using the correct e-mail address. IAM systems verify credential and collect audit logs based on access requested and may contain PII that might have been captured into order to authenticate to the resource.

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.

AFIT salesforce tool retains information of Veterans/ VA Employees/ Contractors/ Members of Public such as:
Veteran First and Last Name, Veteran File Number, SSN, Veteran Benefit Claim ID, Veteran date of claim, claim end product, VA Employee Name assigned to process case and agent/attorney First and Last Name, agent/attorney mailing address.

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.

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. OIT retains audit records for a defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and VA information retention requirements.

Appellate Litigation Files, Disposition instructions: Temporary. Close case file after completion of cases and receipt of last resolved motion or action. Cutoff closed files at the end of the fiscal
years. Maintain files on-site for one year and then transfer to closest Federal Records Center. Destroy 7 years after cutoff.

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 retention schedule for the Salesforce Development Platform (SFDP) is also applied to the AFIT Salesforce module.

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


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

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

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

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

AFIT does not use PII/live data of the Veterans, VA employees or members of the public information for research, testing or training. VA employees and VA contractors accessing the tool would have to undergo basic Privacy training such as, Privacy and Information Security Awareness and Rules of Behavior and information security training annually.

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:** Depending on the retention time, PII information of the Veteran or agent is at risk of exposure to unauthorized individuals. The information is retained in the system to process appeals and attorney payments that are initiated by Veteran when a claim is denied.

**Mitigation:** All data at rest within the SFGCP security boundary is encrypted in accordance with FIPS 140-2, as well as protected by FedRAMP certified “HIGH” security controls. Use of FedRAMP HIGH controls implemented under the FedRAMP ATO. Collectively, these controls within the SFGCP security boundary provide maximum protection to all VA Salesforce data. Only retro-active payments to the Veteran and agent are retained in the tool.

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>Master Person Index (MPI)</td>
<td>MPI is a Veteran database system, this will be utilized to validate the benefits of the Veteran to process their claim</td>
<td>Benefit ID, Veteran Name, SSN</td>
<td>Encrypted data transfer</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:** If appropriate safeguards are not in place, then Privacy information shared within the department may result in unauthorized data access.

**Mitigation:** Release of PII to unauthorized individuals is prohibited by the Privacy standards mandated to all VA employees, affiliates, trainees, volunteers, and contractors. Both contractor and VA employees are required to take Privacy, Health Insurance Portability and Accountability Act (HIPAA), and information security training annually. Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system. Encrypted site-to-site transcription. Data and files are encrypted both in transit and at rest. User specific, user access data configured for each role category and on least privilege base.

**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**
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:** Not applicable for this tool.

**Mitigation:** Not applicable to this tool.

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.

The SORNs defines the information collected from Veterans/ VA Employees/ Members of Public, use of the information, and how the information is accessed and stored.

Accreditation Records – VA. 01VA022(consolidated)
(https://www.oprm.va.gov/docs/sorn/SORN01VA22.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 SORN Accreditation Records – VA. 01VA022 provides individual their rights regarding opportunities to decline to provide information. This system does not collect information directly from individuals.

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 SORN Accreditation Records – VA. 01VA022 provides individual their rights regarding opportunities to decline to provide information. This is an internal tool utilized by OAR which does not collect information from the individuals directly.
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: There is a risk that Veterans may not know salesforce AFIT exists within the Department of Veterans Affairs which is utilized for tracking status of the claims and the retroactive payments.

Mitigation: The VA mitigates this risk by providing the public with one form of notice that the Salesforce AFIT exists through the Privacy Impact Assessment (PIA) which is posted for public access.

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.
Veterans may request access to Privacy Act records maintained by requesting a copy in writing. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VBA system of records, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted, and should be mailed to: FOIA/PA Officer (026G), Office of General Counsel, 810 Vermont Ave., NW., Washington, DC 20420. For requests concerning remote access program records, an individual should submit a written request to: FOIA/PA (20M33), Veterans Benefits Administration, 810 Vermont Ave., NW., Washington, DC 20420.

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.

Veterans have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA Regional Office that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager or designee for the concerned VBA system of records, and the facility Privacy Officer or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation [38 CFR 1.579](#).

Upon the receipt of amendment and approval by the System Manager, AAFCs and SSD employees can update inaccurate information in AFIT as identified.

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

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

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

The procedure for correcting information is outlined in this PIA, and SORN. Formal redress is provided. All information correction must be taken via the Amendment process.

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 ensure data accuracy.

Formal redress is provided in SORN. All information correction must be taken via the Amendment process. In addition, the individual may contact any Regional Office for guidance on how to gain access to his or her records and seek corrective action through the Amendment process.

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:** The individual may not be aware of how to access, redress or correct their information being captured in this tool.

**Mitigation:** The procedures to correct or amend information is included in the applicable SORN and this PIA.

Veterans have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA Regional Office that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager or designee for the concerned VBA system of records, and the facility Privacy Officer...
or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

Role-based Hierarchy is applied. Only assigned VA users can access this tool. Users must use Single Sign On (SSO) and two factor authentication to log into the AFIT platform. Access to the tool follows DTC standard of user access. Additionally, field audit trails and event monitoring provided by Salesforce platform assists in ensuring only assigned users have access to specific records within AFIT.

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.

Yes, VA contractors will be utilizing AFIT tool. Contracts are bound by the same privacy and security procedures and requirements as VA employees.
8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

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

General Training includes: VA Privacy and Information Security Awareness and Rules of Behavior, TMS 10203 - Privacy and Health Insurance Portability and Accountability Act (HIPPA), VA On-Boarding enterprise-wide training, and information security training annually.

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.

1. The Security Plan Status: Approved
2. The Security Plan Status Date: 02/24/2021
3. The Authorization Status: ATO
4. The Authorization Date: 03/18/2021
5. The Authorization Termination Date: 12/17/2023
6. The Risk Review Completion Date: 03/12/2021
7. The FIPS 199 classification of the system – Moderate (M, M, M – C/I/A)

Section 9 – Technology Usage
The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service
Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

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, AFIT system utilizes Salesforce Gov Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This is under the contract: “Salesforce Subscription Licenses, Maintenance and Support”, Contract Number: NNG15SD27B. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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 shared through the AFIT 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.

This is not applicable for AFIT tool. VA has full ownership over the data stored in the AFIT system.
9.4 NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

VA has full authority over data stored in Salesforce AFIT module.

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).

AFIT 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>AP</td>
<td>Authority and Purpose</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>AR</td>
<td>Accountability, Audit, and Risk Management</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>DI</td>
<td>Data Quality and Integrity</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>DM</td>
<td>Data Minimization and Retention</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>IP</td>
<td>Individual Participation and Redress</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>SE</td>
<td>Security</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>TR</td>
<td>Transparency</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>UL</td>
<td>Use Limitation</td>
</tr>
<tr>
<td>ID</td>
<td>Privacy Controls</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------</td>
</tr>
<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.

BERTHA BROWN

Privacy Officer, Bertha L. Brown

James C. Boring 149438

Information System Security Officer, James Boring

Michael S. Domanski 326889

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).

SORN: Accreditation Records – VA. 01VA022(consolidated)
https://www.oprm.va.gov/docs/sorn/SORN01VA22.PDF