Privacy Impact Assessment for the VA IT System called:

Salesforce – VA Privacy Service Customer Support (SF-VAPSCS)

Veterans Affairs Central Office

Office of Information & Technology

eMASS ID# 2458

Date PIA submitted for review:

03/24/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	Gina.siefert@va.gov oitprivacy@va.gov	224-558-1584
Information System Security Officer (ISSO)	Joseph Facciolli	Joseph.Facciolli@va.gov	215-842-2000 x2012
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

The Department of Veterans Affairs (VA) Privacy Service operates the Salesforce – VA Privacy Service Customer Support (SF-VAPSCS) module. SF-VAPSCS is a correspondence workflow management system that assists the VA Privacy Service in responding to complaints, comments, and requests for redress from the public, other government agencies, and the private sector. VA Privacy Service conducted this privacy impact assessment because SF-VAPSCS collects and uses personally identifiable information (PII).

Overview

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

1 General Description

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

VA Privacy Service receives numerous complaints, comments, and requests for redress of privacy issues throughout the year. The correspondence requires analysis, storage, categorization, and coordinated response. The SF-VAPSCS, a Software as a Service (SaaS), is a workflow system that Office of Information and Technology (OIT) – VA Privacy Service personnel utilize to respond effectively to inquiries from Veterans, the public and other government, and private-sector agencies. SF-VAPSCS allows users to manage correspondence tracking with pre-defined routing inside workflow templates.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

Salesforce Government Cloud Plus (SFGCP) is a cloud platform. Data in the platform is controlled by VA but non-VA owned and operated.

Office of Information and Technology (OIT) – VA Privacy Service is the business owner and sole user of SF-VAPSCS and as such is primarily responsible for the system. SF-VAPSCS utilizes the cloud platform called Salesforce Government Cloud Plus (SFGCP) which is controlled by VA, but non-VA owned and operated.

2. Information Collection and Sharing

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

SF-VAPSCS contains data from individuals who submit inquiries or complaints to OIT – VA Privacy Service, either directly or by authorized representatives, or whose inquiries or complaints are referred from other offices. SF-VAPSCS is expected to store information on approximately 1500 individuals/annually.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☒	VA Employees
☐	Clinical Trainees
☒	VA Contractors
☒	Members of the Public/Individuals
☐	Volunteers

D. What is a general description of the information in the IT system and the purpose for collecting this information?
Information collected in SF-VAPSCS is derived from the written and electronic correspondence received from VA components, the public, other government agencies, and the private sector. This information may include the name and home address of the individual sending the correspondence or initiating a telephone call to the agency. Other information that may be obtained but is not required, includes the email address, telephone number, business or organizational address, or the Social Security Number of the individual. The SF-VAPSCS record, created by the receipt of this correspondence, will also include the subject matter of the correspondence. If an individual submits paper-based correspondence, personnel from the VA Privacy Service scan the document(s) and an image of the correspondence is maintained in a case file.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.
SF-VAPSCS shares information internally with VA Privacy Service customer support representatives and managers including contractors.

F. Are the modules/subsystems only applicable if information is shared?
Yes. SF-VAPSCS shares information internally with VA Privacy Service customer support representatives and managers including contractors.

G. Is the system operated in more than one site to include primary and secondary 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?
SF-VAPSCS is not operated at multiple sites.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority and SORN to operate the IT system?
The collection of documents within SF-VAPSCS is governed by 5 U.S.C. § 301 (general agency powers for recordkeeping), the Privacy Act of 1974, as amended (5 U.S.C. § 552a),

and Executive Order 13719 (providing for appointment of a Privacy Officer to assure, in part, that personal information contained in Privacy Act system of records is handled in full compliance with fair information practices). Pursuant to 5 U.S.C. § 301, VA is authorized to implement Departmental regulations that manage VA's day-to-day operations. These operations include regulating employees, managing agency business, and controlling agency papers and property.

I. *What is the SORN?*
75VA001B / 87 FR 36584, *Case and Correspondence Management-VA (CCM)* (6/17/2022)
https://www.govinfo.gov/content/pkg/FR-2022-06-17/pdf/2022-13066.pdf

J. *SORN revisions/modification* The SORN does not require revision and/or modification.

K. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*
The system is not in the process of being modified.

4. System Changes

L. *Will the business processes change due to the information collection and sharing?*

☐ *Yes*
☒ *No*

M. *Will the technology changes impact information collection and sharing?*

☐ *Yes*
☒ *No*

Section 1. Characterization of the Information

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

1.1 Information collected, used, disseminated, created, or maintained in the system.

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ **Full** Social Security Number
- ☐ **Partial** Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account Numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☒ Tax Identification Number
- ☐ Medical Record Number
- ☒ Sex
- ☐ Integrated Control Number (ICN)
- ☒ Military History/Service Connection
- ☐ Next of Kin
- ☐ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI)
- ☒ Other Data Elements (list below)

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

Other PII/PHI data elements: Claim/File Number, Place of Birth, Business Email, Business Phone, Business Address, Residential Address, Human Resource information pertaining to claims or Equal Employment Opportunity (EEO).

1.2 List the sources of the information in the system
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?
The sources of the information are the original incoming correspondence sent by the original requestor, and any related correspondence received back from assigned responder by way of phone calls, mail, and electronic mail.
The requests can also be received from various sources including but not limited to:

- Internal VA Components
- The White House
- State and local governments
- U.S. and foreign corporations
- Other federal agencies
- Congressional offices
- Non-government organizations
- The public

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.
Information can also be received from sources other than the individual as these sources may be referring the individual to the OIT – VA Privacy Service for assistance with their inquiry or these sources may have previously corresponded or interacted with the individual.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
SF-VAPSCS is not a source of information. Request information is added to the system using the information provided by the requestor.

1.3 Methods of information collection
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?
System users enter information into SF-VAPSCS by:
• typing the information received verbally into the SF-VAPSCS record;
• typing the information received via mail into the SF-VAPSCS record;

• scanning original documents into the SF-VAPSCS record as an Adobe PDF file;
• copying information received electronically and pasting them into the appropriate fields in an electronic form which comprises a portion of the SF-VAPSCS record.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?
SF-VAPSCS is not subject to the requirements of the Paperwork Reduction Act as there is no information collection from individuals as defined in VA Directive 6309, Collections of Information.

1.4 Information checks for accuracy, and how often will it be checked.

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.
Office of Information and Technology (OIT) – VA Privacy Service checks the information for accuracy by comparing the information entered into the SF-VAPSCS record to the source of the information. These sources include phone calls, mail, and electronic mail from the individual.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?
Data accuracy is not checked using a commercial aggregator because the data is sourced directly from the person making the inquiry.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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 collection of documents within SF-VAPSCS is governed by 5 U.S.C. § 301 (general agency powers for recordkeeping), the Privacy Act of 1974, as amended (5 U.S.C. § 552a), and Executive Order 13719 (providing for appointment of a Privacy Officer to assure, in part, that personal information contained in Privacy Act system of records is handled in full compliance with fair information practices). Pursuant to 5 U.S.C. § 301, VA is authorized to implement Departmental regulations that manage VA's day-to-day operations. These operations include regulating employees, managing agency business, and controlling agency papers and property.

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

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

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

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

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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 scope of the information collected in VAPSCS is limited to the amount of data necessary to act upon the request, correspondence, or other possible action item received by VA. Although each correspondence is very likely to collect the full name of a correspondent, the date of birth, for example, is only collected if it is voluntarily given and relevant to the request or correspondence. If individuals provide information that is not relevant, it is not documented (e.g., information taken by phone and is not written down) in the system.

Mitigation:
The risk is mitigated by safeguarding the information collected in accordance with applicable privacy laws and policies including all applicable VA automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is stored. Access to the system containing the information in this system is limited to those individuals who have been granted system access rights, and those who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Claim / File Number (Could be the same as SSN)	Assist in the agency response to complaints, comments and requests for redress.	Not used
SSN	Assist in the agency response to complaints, comments and requests for redress.	Not used
Tax ID	Assist in the agency response to complaints, comments and requests for redress.	Not used
Name	Assist in the agency response to complaints, comments and requests for redress.	Not used
Date of Birth	Assist in the agency response to complaints, comments and requests for redress.	Not used
Place of Birth	Assist in the agency response to complaints, comments and requests for redress.	Not used
Sex	Assist in the agency response to complaints, comments and requests for redress.	Not used
Personal and/or Business Email	Assist in the agency response to complaints, comments and requests for redress.	Not used
Personal and/or Business Phone	Assist in the agency response to complaints, comments and requests for redress.	Not used

Business, Mailing and/or Residential Address	Assist in the agency response to complaints, comments, and requests for redress.	Not used
Mother's Maiden Name	Assist in the agency response to complaints, comments and requests for redress.	Not used
Military Status/Service Connection	Assist in the agency response to complaints, comments and requests for redress.	Not used
Human Resource information pertaining to claims or Equal Employment Opportunity (EEO)	Assist in the agency response to complaints, comments and requests for redress.	Not used

2.2 Describe the types of tools used to analyze data and what type of data may be produced.
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?
SF-VAPSCS has customized reporting features built into the system. These reports allow the OIT-VA Privacy Service to report on the number of privacy complaints, the categories of complaints, and the disposition of complaints. Reports will also include the component from which the complaint originated.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
SF-VAPSCS does not create or make available new or previously unutilized information about an individual.

2.3 How the information in the system is secured.
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?
SF-VAPSCS is accessed via a secured webpage utilizing Single Sign-On (SSO) technology. SF-VAPSCS is housed in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there. The data exchange will be through a site-to-site encryption having Transmission Layer Security. Salesforce Shield Platform provides FIPS 140-2 certified encryption.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).
There are no additional protections in place aside from Salesforce Shield Platform which provides FIPS 140-2 certified encryption. (All data and content stored in Salesforce Government Cloud Plus (SFGCP) is encrypted.)

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
Salesforce Shield Platform provides FIPS 140-2 certified encryption, and all data and content stored in Salesforce Government Cloud Plus (SFGCP) is encrypted. SF-VAPSCS is accessed via a secured webpage utilizing SSO technology. SF-VAPSCS is implemented with the 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. VA Privacy Service customer support representatives have each undergone extensive background checks and have taken the required annual privacy training, as well as signed off on Rules of Behavior document.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?
OIT– VA Privacy Service requires that access to the information within SF-VAPSCS be limited to authorized personnel by restricting access to employees and contractors who are assigned to review, process, track, and respond to the inquiries.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

The following controls ensure that information is handled in accordance with the described uses above:

- Implemented mandatory personnel security policies and procedures that require all personnel to be the subject of a favorable background investigation prior to being granted access to sensitive information systems;
- Required the completion of appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access;
- Employed a formal sanctions process for personnel failing to comply with established information security and privacy policies and procedures;
- Required that access to the information within SF-VAPSCS be limited to authorized personnel; and
- Provided initial and follow-on security and privacy awareness education for each individual with access to SF-VAPSCS.

2.4c Does access require manager approval?
Access to the information within SF-VAPSCS is limited to authorized personnel who are assigned to review, process, track, and respond to the inquiries
.
2.4d Is access to the PII being monitored, tracked, or recorded?
Yes, SF-VAPSCS tracks user activity in the system to include data accessed in accordance with security policies and procedures.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?
SF-VAPSCS is accessed via a secured webpage utilizing Single Sign-On (SSO) technology. SF-VAPSCS is housed in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there. Accessibility to data is granted based on the permission sets and profile-based settings is 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 Access VA.

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*

The following data is retained by SF-VAPSCS:

- Name
- Full Social Security Number
- Date of Birth
- Mother's Maiden Name
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Email Address
- Tax Identification Number
- Sex
- Military History/Service Connection
- Claim File Number
- Place of Birth
- Business Email Address
- Business Phone Number
- Business Address
- Residential Address
- Human Resource Information

SF-VAPSCS also maintains a record of correspondence between OIT- VA Privacy Service and the complainant.

3.2 How long is information retained?

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

Privacy complaint records are retained for three years after resolution or referral in accordance with National Archives and Records Administration General Records Schedule 4.2. Information Access and Protection Records, series Item 065, Privacy Complaint Files, and disposition authority DAA-GRS-2019 0001-0004.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. Please work with the system VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.
3.3a Are all records stored within the system of record indicated on an approved disposition authority?
Yes, all records are stored within the system of record indicated on an approved disposition authority.

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

- General Records Schedule 4.2, Information Access and Protection Records, series Item 065, Privacy Complaint Files, and disposition authority DAA-GRS-2019 0001-0004. https://www.archives.gov/files/records-mgmt/grs/grs04-2.pdf

3.4 What are the procedures for the elimination or transfer of SPI?
Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.
All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500 and 6300. https://www.va.gov/vapubs/search_action.cfm?dType=1 SF-VAPSCS tool adheres to the National Archives and Records Administration General Records Schedule 4.2. 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). No paper form is used for tracking inquiries in the system. SF-VAPSCS 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).

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?
Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training, and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.
SF-VAPSCS does not use PII for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

Consider the following FIPPs below to assist in providing a response:
Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.
Principle of Data Quality and Integrity: The PIA should describe 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: There is a risk that information maintained by the system could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released, breached, or exploited.

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. Basic information and email correspondence about the submitted helpdesk ticket is retained.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a **SF-VAPSCS** consists of **zero** key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **SF-VAPSCS** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A	N/A	N/A	N/A	N/A	N/A

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
VA Privacy Service customer support representatives and managers including contractors	Performing duties as assigned.	Name Full Social Security Number Date of Birth Mother's Maiden Name Personal Mailing Address Personal Phone Number(s) Personal Email Address Tax Identification Number Sex Military History/Service Connection Claim File Number Place of Birth Business Email Address Business Phone Number Business Address Residential Address Human Resource Information	Granted permissions to program and via email

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).

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

Follow the format below:
Privacy Risk: There is a risk that SF-VAPSCS data may be shared with unauthorized individual(s), or that authorized users may share it with other unauthorized individuals. The risk might include end users who do not log out of SF-VAPSCS when away from their computers.

Mitigation: The VA requires single-sign-on (SSO) or two-factor authentication (2FA) in order to access SF-VAPSCS. The following security control families are applicable (in addition to all NIST applicable RMF families):

- Audit and Accountability
- Awareness Training
- Security Assessment and Authorization
- Incident Response Personnel Security
- Identification and Authentication

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

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

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

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

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

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

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

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Follow the format below:

Privacy Risk: SF-VAPSCS does not share or disclose information externally; therefore, there is no privacy risk.

Mitigation: A mitigation is not needed because there is no external sharing or disclosing of information.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.
Notice is provided to individuals before collection of information with publication in the Federal Registrar of 75VA001B / 87 FR 36584, *Case and Correspondence Management-VA (CCM)* SORN and this publicly available Privacy Impact Assessment (PIA) for the system. In addition, VA Privacy Service also posts a Privacy Policy (https://www.va.gov/privacy-policy) on the bottom of the webpage with its contact information.

6.1b If notice was not provided, explain why.
Notice was provided.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.
Notice is provided to individuals before collection of information with publication in the Federal Registrar of 75VA001B / 87 FR 36584, *Case and Correspondence Management-VA (CCM)* SORN and this publicly available Privacy Impact Assessment (PIA) for the system. In addition, VA Privacy Service also posts a Privacy Policy (https://www.va.gov/privacy-policy) on the bottom of the webpage with its contact information.

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.
Individuals are not obligated in any way to submit correspondence to VA. Individuals have an inherent right to decline sending information to the OIT- VA Privacy Service.

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.
An individual's right to consent to particular uses of the information is inherent in the nature of SF-VAPSCS. An individual's inquiry is tracked and answered. The information provided is not disclosed beyond those personnel inside of VA with a valid need to know to respond to the individual's complaint, comment, or request for redress. An individual's correspondence topic is provided to VA leadership as a matter of information on volume and current issues.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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 an individual is unaware that their information is being collected by the system.

Mitigation: The VA provides notice to individuals before collection of information with publication in the Federal Registrar of 75VA001B / 87 FR 36584, *Case and Correspondence Management-VA (CCM)* SORN and this publicly available Privacy Impact Assessment (PIA) for the system. In addition, VA Privacy Service also posts a Privacy Policy (https://www.va.gov/privacy-policy) on the bottom of the webpage with its contact information.

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 The procedures that allow individuals to gain access to their information.

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing at VA Privacy Service, US Department of Veterans Affairs, 810 Vermont Avenue NW Washington, DC 20420. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

This system is not exempt from the Privacy Act.

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

Individuals may gain access to their own information by submitting a Freedom of Information Act (FOIA) request (https://department.va.gov/foia/). Individuals may also contact the VA Privacy Serve with SF-VAPSCS requests at the following: VA Privacy Service, US Department of Veterans Affairs, 810 Vermont Avenue 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.

Should an inaccuracy be discovered during the resolution of the case file, the organization tasked with resolving the case file may contact the originating submitter. Mistakes in the spelling of the writer's name, prefix, and/or suffix, etc. can be corrected inside of SF-VAPSCS by any authorized user. Manual requests for corrections can be submitted to VA Privacy Service, US Department of Veterans Affairs, 810 Vermont Avenue NW Washington, DC 20420.

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.
Individuals seeking to contest or amend records within SF-VAPSCS pertaining to them should contact the system manager in writing as indicated above. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
Redress is provided.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.
Principle of Individual Participation: If access and/or correction is denied, then is the individual must be provided notice as to why the denial was made and how to challenge such a denial.
Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.
This question is related to privacy control IP-3, Redress.
Follow the format below:
Privacy Risk: There is a risk that individuals may not know the procedures on how to request access, correction or redress of information in the SF-VAPSCS.
Mitigation: Any risk that the individual may not correct their information is mitigated by allowing individuals to request access or amendment of their records at any time. Individuals may access their information by using the PA/FOIA process outlined on the VA web site at www.va.gov/privacy or by contacting OIT-VA Privacy Service directly at VA Privacy Service, US Department of Veterans Affairs, 810 Vermont Avenue NW Washington, DC 20420.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?
Only a limited number of OIT-VA Privacy Service personnel have access to the database. This access is limited to employees and contractors who are assigned to review, process, track, and respond to the inquiries. These individuals will be assigned and granted access through the System Owner after receiving approval from the SF-VAPSCS Business Owner. The System Owner and the OIT-VA Privacy Service maintain and manage a list of authorized SF-VAPSCS users.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?
No users from other agencies have access to the system.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.
Access to SF-VAPSCS is limited to employees and contractors who are assigned to review, process, track, and respond to the inquiries. These users have read, write and edit access to SF-VAPSCS.

8.2a. Will VA contractors have access to the system and the PII?
Yes, VA Privacy Service contractors will have access to SF-VAPSCS.

8.2b. What involvement will contractors have with the design and maintenance of the system?
Contractors will be involved in the design, development, and maintenance of the system.

8.2c. Does the contractor have a signed confidentiality agreement?
All contractors who will utilize SF-VAPSCS have signed NDAs.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?
No, the contractor does not have an implemented Business Associate Agreement.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
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.

All contractors who will utilize SF-VAPSCS have signed NDAs.

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 Rules of Behavior
- Privacy awareness training
- HIPPA and VA on-boarding enterprise-wide training

Users must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via VA's Talent Management System 2.0 (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS 2.0 system.

8.4 The Authorization and Accreditation (A&A) completed for the system.
8.4a If Yes, provide:

1. *The Security Plan Status:* Not yet approved
2. *The System Security Plan Status Date:* 12/14/2023
3. *The Authorization Status:* Approved (ATO) Authority to Operate
4. *The Authorization Date:* 12/14/2023
5. *The Authorization Termination Date:* 12/14/2026
6. *The Risk Review Completion Date:* 12/14/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
The Initial Operating Capability date for SF-VAPSCS is January 4, 2024.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

Yes, SF-VAPSCS utilizes the Salesforce Government Cloud Plus (SFGCP) Platform. SFGCP is hosted in the Amazon Web Services (AWS) GovCloud. The SFGCP is built on the underlying Salesforce.com platform that is hosted in a FedRAMP Certified FISMA High environment which is in the AWS GovCloud West. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). ***(Refer to question 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes, VA has full ownership of the PII that will be used by the SF-VAPSCS module. 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.

Ancillary data is not collected by Salesforce. VA has full ownership over the data stored in SF-VAPSCS.

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 SF-VAPS

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).

No robotic process automation (RPA) is used in this system.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2025.06.05 12:49:42 -05'00'

Privacy Officer, Gina Siefert

JOSEPH FACCIOLLI Digitally signed by JOSEPH FACCIOLLI
Date: 2025.06.05 11:43:03 -04'00'

Information Systems Security Officer, Joseph Facciolli

MICHAEL DOMANSKI Digitally signed by MICHAEL DOMANSKI
Date: 2025.06.05 10:42:32 -04'00'

Information Systems Owner, Michael Domanski

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

- Privacy, Policies, And Legal Information | Veterans Affairs

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)