Privacy Impact Assessment for the VA IT System called:

MuleSoft FSC Enterprise Service Bus 2.0 (ESB)

Financial Services Center (FSC)

Veterans Affairs Central Office (VACO)

eMASS ID #2154

Date PIA submitted for review:

05/29/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Pamela M. Smith*	*Pamela.Smith6@va.gov*	*512-937-4824*
Information System Security Officer (ISSO)	*Ronald Murray*	*Ronald.Murray2@va.gov*	*512-460-5081*
Information System Owner	*Jonathan Lindow*	*Jonathan.Lindow@va.gov*	*512-568-0626*

Abstract

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

MuleSoft FSC Enterprise Service Bus 2.0 (ESB) will be replacing the existing Oracle ESB and will help Customer Applications retrieve, process data from the back-end systems, Databases and Services. The MuleSoft Application Programming Interfaces (API) will process the data coming in on the Request from Client Applications and Users do not interact with this system directly as it does not have a User Interface.

Overview

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

FSC MuleSoft ESB (ESB2.0), owned by Financial Services Center (FSC) /Financial Technology Service (FTS).

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

MuleSoft is an Application Programming Interface (API) lifecycle management Solution, which is Lightweight, stateless Java-Based enterprise service bus (ESB) Integration platform that provides a way to interface with wide variety of systems such as Databases, Messaging systems, File Systems, Software as a Service (SaaS) etc. This Platform in general provides a seamless way to enable the exchange of data between different systems and applications.

C. Who is the owner or control of the IT system or project?

The MuleSoft ESB system is VA Owned and VA Operated. The APIs/Services created in this platform are hosted on Microsoft Azure Gov Cloud (MAG) within the boundary of VA Enterprise Cloud (VAEC) and controlled by Financial Technology Services (FTS)

2. Information Collection and Sharing

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

347,464 users will use this application.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

This System does not collect the sensitive information directly from the Individual users but receives the data in the request from the Client Applications. The Client Applications that call the Mule APIs have their own business function and reasons for collecting/using the sensitive information.

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

The information coming in on the request is being passed through to the back-end systems/ services and based on what is requested, Mule APIs send to, retrieve from, or store the data in, the backend systems/existing databases.

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

This System acts as a messenger between the Client Systems and Back-end Systems/Databases. The Mule APIs is used by the Client/Source Systems to send and retrieve information from the back-end Systems.

3. Legal Authority and SORN

H. *What is the citation of the legal authority to operate the IT system?*

The SORNS applicable to MuleSoft ESB is SORN 13VA047. (https://www.oprm.va.gov/privacy/systems_of_records.aspx). Individuals Submitting Invoices/Vouchers for Payment and Accounting Transactional Data-VA (13VA047)

"AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 31 U.S. Code 3512- Executive Agency Accounting and other Financial Management Reports and Plans; Federal Managers' Financial Integrity Act section 2 of 1982; Federal Financial Management Improvement Act of 1996; E-Government Act of 2002 title III., Federal Information Security Modernization Act (FISMA) of 2014; Clinger Cohen Act of 1996; 38 CFR part 17 17.120–17.132; OMB Circular A–123, Management's Responsibility for Internal Control.

2023-18807.pdf (govinfo.gov)

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

SORN is still active and does not need amendment or revision. This SORN covers cloud usage and storage.

4. System Changes

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

No. Completion of this PIA will not result in circumstances that requires changes to the business processes.

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

This PIA could not potentially result in technology changes.

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. 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
- ☒ 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
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements:

•Passport
•Driver's License
•Credit Card Number
•Asset Information
•Title Number
•Place of Birth

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

•Religion
•Employment Information
•Security Clearance Information
•Education Information
•Drug Test results
•Criminal History
•Marital Status
•Family History
•Account Numbers
•Date of Death
•Date of Admission
•Date of Discharge
•Vehicle and Serial Number
•Device Identifiers and serial Number
•Web URLs

PII Mapping of Components (Servers/Database)

< **MuleSoft FSC Enterprise Service Bus 2.0** > consists of <**15**> 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 < **MuleSoft FSC Enterprise Service Bus 2.0** > 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 3.9 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**
offSet Kofax FSC Customer ELMS FSCDataDepot CCS CCP HCPS EPS Payment VAChoice PCM_VAChoice_TW PCM_VAChoice_HN DashBAM	No (Only transports)			•Name •SSN •Passport •Driver'sLicense •TaxpayerID •Patient IDNumber •Credit CardNumber •FinancialAccountNumber •AddressInformation •AssetInformation •TelephoneNumbers •VehicleRegistrationNumber •TitleNumber	Internal protection is managed by access controls such as Multi-Factor Authentication, awareness and training, auditing, and internal network controls.

Frontier DMS				•Date of Birth •Age •Place of Birth •Race •Religion •EmploymentInformation •SecurityClearanceInformation •MedicalInformation •EducationInformation •FinancialInformation •Drug Testresults •CriminalHistory •MaritalStatus •FamilyHistory •FaxNumber •AccountNumbers •EmailAddress •Date ofDeath •Date ofAdmission •Date ofDischarge •Vehicle andSerialNumber •InternetProtocol(IP)AddressNumbers •DeviceIdentifiers and serial Number •Web URLs •MedicalRecordNumber	Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

This System is a service bus and does not collect any data from the individuals. It only transports data from the systems listed below to back-end Systems and web services.

Invoice Payment Processing System (IPPS)
Customer Processing Management (CPM)/Customer Engagement Portal (CEP)
Debt Management Center (DMC) Applications (includes Consolidated Patient Account Center (CPA
FSC Internal Applications
VA Choice
Healthcare Claims Processing System (HCPS)/Referral Authorization System (RAS) Application
Charge Card Portal (CCP)
Equipment Lease Management System (ELMS)
Beneficiary Travel Self-Service System (BTSSS)
Permanent Change of Station Portal (PCSP)
Treasury Reconciliation (SF224)
Community Care Non-Network Claims (CCNNC)
Defense Medical Logistics Standard Support (DMLSS)
Provider Portal
Prior Year Recovery (PYR)
Lockbox

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.

This System is a service bus and does not collect any data from the individuals. It only transports data from the systems listed below to back-end Systems and web services.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

This System does not create the information but only transports the data.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

This System is a service bus and does not collect any data from the individuals. It only transports data from the systems listed below to back-end Systems and web services. The Client Systems calling MuleSoft APIs will be the data source systems and MuleSoft APIs do not collect information from the individuals directly.

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?

This System is a service bus and does not collect any data from the individuals. It only transports data from the systems listed below to back-end Systems and web services.

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

MuleSoft ESB does not check for accuracy and this responsibility lies with the Source Systems invoking MuleSoft APIs as this system only transports data through. The Client Systems calling MuleSoft APIs will be the data source systems and MuleSoft APIs do not collect information from the individuals directly, hence, do not have the control to check accuracy.

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?

MuleSoft ESB does not check for accuracy and this responsibility lies with the Source Systems invoking MuleSoft APIs as this system only transports data through.

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

Legal authority: Budget and Accounting Act of 1950; General Accounting Office Title 8, Chapter #3; Authorized under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. CFR › Title 38 › Chapter I › Part 3 › Subpart A › Section 3.216 - Mandatory disclosure of social security numbers. CFR › Title 38 › Chapter I › Part 1 › 38 CFR 1.575 - Social security numbers in veterans' benefits matters. U.S. Code › Title 38 › Part IV › Chapter 51 › Subchapter I › § 5101 38 U.S. Code § 5101 - Claims and forms CFR › Title 32 › Subtitle A › Chapter VII › Subchapter A › Part 806b › Subpart C › Section 806b.12 32 CFR 806b.12 - Requesting the Social Security Number Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules

• 13VA047/ 85 FR 22788 Individuals Submitting Invoices-Vouchers for Payment-VA

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: This System receives PII/PHI data from the Source Systems and does not collect the data directly from the individuals.

Sensitive personal information may be released to unauthorized individuals.
Mitigation: The Source Systems would have to be reviewed with in place processes to make sure the information is relevant, accurate and securely collected and there is a mitigation plan implemented. Both contractors and VA Employees are required to take privacy, HIPAA, and information security training annually.

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.

This System only transports the data from the Source Systems to Back-end systems and does not collect, use, or store.

PII/PHI Data Element	Internal Use	External Use
Name	used to identify a veteran.	Not used
Social Security Number	used to identify a veteran.	Not used
Date of Birth	used to identify a veteran.	Not used
Mother's Maiden Name	used to identify a veteran.	Not used
Personal Mailing Address	used to contact a veteran for mailing.	Not used
Personal Phone Number(s)	used to contact a veteran.	Not used
Personal Fax Number	used to share documentation with the Veteran.	Not used
Personal Email Address	used to contact a veteran.	Not used
Financial Account Information	make payments to Vendors.	Not used
Account numbers	make payments to Vendors.	Not used
Certificate/License numbers		Not used
Vehicle License Plate Number		Not used
Internet Protocol (IP) Address Numbers	System IP	Not used
Previous Medical Records	used for a veteran.	Not used
Race/Ethnicity	veteran.	Not used
Tax Identification Number	Tax ID used as a vendor identifier.	Not used
Medical Record Number	for Veteran's records.	Not used
Driver's License		Not used
Patient ID Number	for Veteran's record	Not used
Credit Card Number	make payments to Vendors	Not used
Asset Information	make payments to Vendors	Not used
Drug Test results	used for a veteran	Not used

Marital Status	used for a veteran	Not used
Family History	used for a veteran	Not used
Date of Death	used for a veteran	Not used
Medical Record Number	used for a veteran	Not used
Passport	used for a veteran	Not used
Driver's License	used for a veteran	Not used
Credit Card Number	make payments to Vendors	Not used
Asset Information	used for a veteran	Not used
Title Number	used for a veteran	Not used
Place of Birth	veteran place of birth	Not used
Religion	used for a veteran	Not used
Employment Information	used for veteran	Not used
Security Clearance Information	used for veteran	Not used
Education Information	used for veteran	Not used
Drug Test results	used for veteran	Not used
Criminal History	used for veteran	Not used
Marital Status	used for veteran	Not used
Family History	used for veteran	Not used
Account Numbers	used for veteran	Not used
Date of Death	time of veteran	Not used
Date of Admission	used for veteran	Not used
Date of Discharge	used for veteran	Not used
Device Identifiers and serial Number	used for veteran	Not used
Web URLs	used for veteran	Not used

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

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

This System does not use any tools to analyze the data as this System does not control the data being produced and only transports the data from the Source Systems to Back-end systems.

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.

This System does not control the data being produced and only transports the data from the Source Systems to Back-end systems.

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

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

The Data is encrypted 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?

The SSNs are sent over SSL during transmission and only accessible to the Application.

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

FSC performs annual reviews in accordance with VA guidelines for all the VA systems it supports.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

<u>Principle of Use Limitation:</u> 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?

Access to MuleSoft control plane can only be requested by submitting 9957 and having access to this control plane does NOT give users access or visibility into any PII/PHI data because the PII/PHI data flows through on Runtime plane hosted within Azure gov cloud.

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

Yes

2.4c Does access require manager approval?

Yes

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

Yes

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

Data Administrator and Security

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*

Request Data is retained in the backend database for troubleshooting and production support purposes.

Name
Social Security Number
Date of Birth
Mother's Maiden Name
Personal Mailing Address
Personal Phone Number(s)
Personal Fax Number
Personal Email Address
Financial Account Information
Account numbers
Certificate/License numbers
Vehicle License Plate Number
Internet Protocol (IP) Address Numbers
Previous Medical Records
Race/Ethnicity
Tax Identification Number
Medical Record Number

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

Request Data is retained for 30 days to assist production support to troubleshoot.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes, the retention schedule has been approved by VA and each Source System should have the schedule in place.

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

Example CRM/CEP Source System Schedule: Yes, GRS Schedule 1.1, Item #10, Disposition Authority DAA-GRS-2013-0003-0001 Governed by General Accounting Office Regulations which require retention for records created prior to July 2,1975: 7 years after the period of the account; records created on and after July 2, 1975: Link to retention schedule:

rcs10-1.pdf (va.gov)

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Electronic records are retained if required (GRS Schedule 1.1, Item #10), and are destroyed in accordance with NARA disposition instructions. [Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.] We are also finalizing procedures to automate the destruction of media at the appropriate time based on published NARA and VA instructions (nightly job that removes data outside of retention period

deletes / destroys metadata and image to re-use file storage). Internal Management ensures these procedures are enforced IAW FSC Directive 6300 and VA 6300.1 (Records Management).

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.

This system does not use PII for any Testing, Training, or research as it does not control the data. Only test data is used for the system testing.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: The request data retained in the back-end systems could contain PII information. If information is retained longer than specified, privacy information may be released to unauthorized individuals.
Mitigation: Real data is only stored in Production database and the access is restricted to Data Base Administrator (DBA) and allowed members.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Invoice Payment Processing System (IPPS)	The purpose of information is to accomplish business functionality implemented by the Source System.	•Name •SSN •Address Information •Date of Birth •Email Address	Soap Services/Rest APIs
Customer Processing Management (CPM)/Customer Engagement Portal (CEP)	The purpose of information is to accomplish business functionality implemented by the Source System.	•Name •SSN •Taxpayer ID •Patient ID Number •Financial Account Number •Address Information •Telephone Numbers •Date of Birth •Medical Information •Financial Information •Medical Record Number	Soap Services/Rest APIs

Debt Management Center (DMC) Applications (includes Consolidated Patient Account Center (CPA	The purpose of information is to accomplish business functionality implemented by the Source System.	•Name •SSN •Passport •Driver's License •Taxpayer ID •Patient ID Number •Credit Card Number •Financial Account Number •Address Information •Asset Information •Telephone Numbers •Vehicle Registration Number •Title Number •Date of Birth •Age •Place of Birth •Race •Religion •Employment Information •Security Clearance Information •Medical Information •Education Information •Financial Information •Drug Test results •Criminal History •Marital Status •Family History •Fax Number •Account Numbers •Email Address •Date of Death •Date of Admission •Date of Discharge •Vehicle and Serial Number •Internet Protocol (IP)Address Numbers •Device Identifiers and serial Number •Web URLs	Soap Services/Rest APIs

		•Medical Record Number	
FSC Internal Applications	The purpose of information is to accomplish business functionality implemented by the Source System.	•Name •SSN •Passport •Taxpayer ID •Credit Card Number •Financial Account Number •Address Information •Telephone Numbers •Date of Birth •Security Clearance Information •Financial Information •Family History •Fax Number •Account Numbers •Email Address •Date of Death	Soap Services/Rest APIs
VA Choice	The purpose of information is to accomplish business functionality implemented by the Source System.	•Name •SSN •Taxpayer ID •Patient ID Number •Financial Account Number •Address Information •Telephone Numbers •Date of Birth •Medical Information •Financial Information •Drug Test results •Date of Admission •Medical Record Number	Soap Services/Rest APIs

Healthcare Claims Processing System (HCPS)/Referral Authorization System (RAS) Application	The purpose of information is to accomplish business functionality implemented by the Source System.	•Name •SSN •Taxpayer ID •Patient ID Number •Address Information •Telephone Numbers •Date of Birth •Medical Information •Financial Information •Drug Test results •Date of Admission •Medical Record Number	Soap Services/Rest APIs
Charge Card Portal (CCP)	The purpose of information is to accomplish business functionality implemented by the Source System.	•Name •Credit Card Number •Financial Account Number •Address Information •Telephone Numbers •*Vehicle Registration Number* •Financial Information •Account Numbers •Email Address	Soap Services/Rest APIs
Equipment Lease Management System (ELMS)	The purpose of information is to accomplish business functionality implemented by the Source System.	•Name •Financial Account Number •Address Information •Asset Information •Telephone Numbers •*Vehicle Registration Number* •Financial Information •Account Numbers •Email Address •Vehicle and Serial Number	Soap Services/Rest APIs

Beneficiary Travel Self-Service System (BTSSS)	The purpose of information is to accomplish business functionality implemented by the Source System.	•Name •SSN •Driver's License •Taxpayer ID •Financial Account Number •Address Information •Telephone Numbers •Financial Information •Fax Number •Account Numbers •Email Address	Soap Services/Rest APIs
Permanent Change of Station Portal (PCSP)	The purpose of information is to accomplish business functionality implemented by the Source System.	•SSN	Soap Services/Rest APIs
Treasury Reconciliation (SF224)	The purpose of information is to accomplish business functionality implemented by the Source System.	•Name •Financial Account Number •Telephone Numbers •Financial Information •Account Numbers •Email Address	Soap Services/Rest APIs
Community Care Non-Network Claims (CCNNC)	The purpose of information is to accomplish business functionality implemented by the Source System.	•Name •SSN •Taxpayer ID •Patient ID Number •Address Information •Telephone Numbers •Date of Birth •Medical Information •Financial Information •Drug Test results •Date of Admission •Medical Record Number	Soap Services/Rest APIs
Defense Medical Logistics Standard Support (DMLSS)	The purpose of information is to accomplish business functionality implemented by the Source System.	•Taxpayer ID •Financial Account Number •Financial Information	Soap Services/Rest APIs

Provider Portal	The purpose of information is to accomplish business functionality implemented by the Source System.	•Name •Address Information •Telephone Numbers •Medical Information •Email Address •Web URLs	Soap Services/Rest APIs

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The Application uses two factor authentications from IAM SSOi to protect data, along with that there are authorization mechanisms defined to determine what level of data to expose. Data in rest at the CRM database is encrypted, and Data will be transmitted over ESB with https protocol so the transmission itself is secure. If a bad internal actor accesses CCNNC Provider Portal information, then they could use the limited PII/PHI to support identity theft activities.

Mitigation: The Information is sent over SSL transmission and only accessible to the Application. Use of masking, challenge questions, ID.me registration, Security Account Manager (SAM) registration and knowledge of specific claim information combined with manual approval process are used to mitigate risk of a bad actor accessing PII/PHI.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	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: .
No privacy risk as information is not shared externally.

Mitigation: No Mitigation is necessary.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Individuals upon are request are referred to the source system owner or sponsor, etc. Information will not be obtained prior to written notice being provided to everyone. This System does not collect the information from the individuals directly and the Source Systems should be taking the measures needed: •All access requests are logged and recorded.
•Encryption data

https://www.oprm.va.gov/privacy/systems_of_records.aspx.

Individuals Submitting Invoices/Vouchers for Payment and Accounting Transactional Data-VA (13VA047).

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

SORN is provided to the public

https://www.oprm.va.gov/privacy/systems_of_records.aspx.

Individuals Submitting Invoices/Vouchers for Payment and Accounting Transactional Data-VA (13VA047).

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used

appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

The provided SORN explains the reason, purpose, authority, and routine uses of the collected information is adequate to inform those affected by the system that their information has been collected and is being used appropriately.

https://www.oprm.va.gov/privacy/systems_of_records.aspx.

Individuals Submitting Invoices/Vouchers for Payment and Accounting Transactional Data-VA (13VA047).

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.

This System does not collect the information from the individuals directly and the Source Systems should be taking the measures needed. Example CRM/CEP Source System measures: No, as we do not require them to provide any information.

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.

This System does not collect the information from the individuals directly and the Source Systems would have a process in place. >Example CRM/CEP Source System measures: No, as we do not require them to provide any information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: Has sufficient notice been provided to the individual?

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

Privacy Risk: Veterans and members of the public may not know VA maintains, collects and store data in this software.

Mitigation: Individuals upon request, are referred to the source system owner or sponsor, etc. Information will not be obtained prior to written notice being provided to everyone.
This System does not collect the information from the individuals directly and the Source Systems should be taking the measures needed:
•All access requests are logged and recorded.
•Data is encrypted.

Section 7. Access, Redress, and Correction

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

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

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

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

This System does not collect the information from the individuals directly and the Source Systems should be taking the measures needed.

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)?

MuleSoft is not exempt from the access provisions of 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?

MuleSoft is a Privacy Act System

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.

This System does not collect the information from the individuals directly and the Source Systems should be taking the measures needed. Example CRM/CEP Source Systems measures: Corrections are handled at the respective Call Centers that are external to CEP. User submits a fresh new form to overwrite the previous incorrect info.

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.

This System does not collect the information from the individuals directly and the Source Systems should be taking the measures needed. Example CEP Source System measures: Corrections are handled at the respective Call Centers that are external to CEP. Financial Services Center, Help Desk at (512) 460-5700.

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

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

This System does not collect the information from the individuals directly and the Source Systems should be taking the measures needed. Example CEP Source System measures: Corrections are handled at the respective Call Centers that are external to CEP. Financial Services Center, Help Desk at (512) 460-5700.

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

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: Inaccurate data may be used to process individual privacy information.

Mitigation: This System does not collect the information from the individuals directly and the Source Systems should be taking the measures needed:

•Individuals upon request, are referred to the source system owner or sponsor, etc.
•Information will not be obtained prior to written notice being provided to everyone.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

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

8.1a Describe the process by which an individual receives access to the system?

Access to MuleSoft control plane can only be requested by submitting 9957 and having access to this control plane does NOT give users access or visibility into any PII/PHI data. Only internal VA users are given the access to the Control plane via 9957 requests. Developer role gives access to creation of API and publishing/Deploying the API in Dev environment. Admin role gives access to deploying and managing the configurations of the platform in higher environments.

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?

MuleSoft System is Internal only.

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.

Separation of duties matrix is used to identify user's role and determine their level of access:
•User: read only •System admin: read and write •Database admin: read and write •Application

Admin: read and write •VA Cloud Broker: read and write •Managers: read and write •Approvers: read and write.

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 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, Contractors can request access to MuleSoft control plane by submitting 9957 and having access to this control plane does NOT give them access or visibility into any PII/PHI data. Only internal VA users are given the access to the Control plane via 9957 requests. Developer role gives access to creation of API and publishing/Deploying the API in Dev environment. Admin role gives access to deploying and managing the configurations of the platform in higher environments.
All Contractors complete and acknowledge the VA Rules of Behavior which outlines the NDA requirements.

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.

Mandatory Privacy training is provided to all VA users both generic and specific to their roles. Privacy and Information Security Awareness and Rules of Behavior (Talent Management System course #10176) is required for all Federal and Contractor personnel that require access to the VA Network. Annual training compliance is closely monitored. Other required Talent Management System courses monitored for compliance: •VA 10203: Privacy and HIPAA Training •VA 3812493: Annual Government Ethics

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* 08/30/2022
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 04/22/2024

5. *The Authorization Termination Date:* 04/22/2026
6. *The Risk Review Completion Date:* 04/17/2024
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.***

N/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), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes, The cloud model is Platform as a Service (PaaS)

The environments where this System's control plane and runtime plane are hosted have a FedRAMP authorization (Yes, VAEC Azure).

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

VAEC Azure Contract number NNG15SD27B 36C10B19F0460 P00007

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

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

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

No

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.

Azure is under contract as Cloud Provider in VAEC

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

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.

PAMELA SMITH

Digitally signed by PAMELA SMITH
Date: 2024.06.11 15:39:25 -05'00'

Privacy Officer, Pamela M. Smith

RONALD MURRAY

Digitally signed by RONALD MURRAY
Date: 2024.06.12 07:03:20 -05'00'

Information Systems Security Officer, Ronald Murray

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2024.06.12 08:31:38 -05'00'

Information Systems Owner, Jonathan Lindow

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).

HELPFUL LINKS:

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 Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices