



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)

Date PIA submitted for review:

08/05/2022

System Contacts:

*System Contacts*

	Name	E-mail	Phone Number
Privacy Officer	Deea Lacey	Deea.Lacey@va.gov	512-386-2246
Information System Security Officer (ISSO)	Rito-Anthony Brisbane	Rito-Anthony.Brisbane@va.gov	512-460-5081
Information System Owner	Jonathan Lindow	Jonathan.Lindow@va.gov	512-981-4871

## Abstract

*The abstract provides the simplest explanation for “what does the system do?” and will be published online to accompany the PIA link.*

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 APIs 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:*

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

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

Version Date: October 1, 2021

Page 1 of 46

and applications. 347,464 users will use this application. FSC MuleSoft ESB (ESB2.0), owned by Financial Services Center (FSC) /Financial Technology Service (FTS). 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).

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.

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.

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.

System Name	Description/Function
Invoice Payment Processing System (IPPS)	Web application used by VA Staff to certify and process commercial Payments.
Customer Processing Management (CPM)/Customer Engagement Portal (CEP)	<p>The Customer Process Management (CPM) solution will allow technicians to manage, track and document and resolve customer calls through various inquiry methods, including phone calls, emails, tickets and customer generated self-service requests. The application will include built in workflows to assist technicians with inquiry resolution. The documentation of calls is necessary to track and report information, especially in instances of system issues, which must be elevated and resolved quickly. The CPM solution will include functionality to allow for communication between Tier 1 and Tier 2 Help Desks to escalate and resolve customer-initiated issues. It will also enable streamlined routing of work requirements to other work groups that support back-office work functions to track and manage work generated by incoming inquiries. The application will further enable tracking and reporting of issues received by Tier 2 staff directly.</p> <p>Customer Engagement Portal (CEP) is external facing portal which serves medical providers &amp; vendors doing business with VA to view reports related to Claims, Payments, Invoice &amp; Treasury Offsets. It replaced an</p>

	existing system called VIS with enhanced security features including two factor authentications.
Debt Management Center (DMC) Applications (includes Consolidated Patient Account Center (CPAC))	<p>Document Import and processing. The VA establishes debts, those debts are referred to DMC, who send the vet a letter they have a debt explaining their options, vets send in docs (correspondence) to manage their debts (repay plans, asking for a waiver, notice of disagreement- they believe their debt was generated in error) when received those docs were uploaded into DMC Pega application, and they are processed. At the end of the process the DMC sends a letter to the vet notifying them of the action taken.</p> <p>The Information Technology Services (ITS) division at the Financial Services Center (FSC) will retire the current Document Management System (DMS) as the FSC has procured a comprehensive Enterprise Content Management (ECM) solution. This solution includes, but is not limited to, the integration of Kofax, FileNet, and Pega. The ECM system will provide and fulfill existing document management capabilities for FSC. In addition, ECM will provide a solution to centralize and manage both FSC Records Management policies and guidelines. The FSC's ECM product suite will also provide the FSC the ability to scale and to meet expected demands for document management capabilities. Business process capabilities within the ECM solution will provide current and future needs for business process management.</p>
FSC Internal Applications	<p>The VA's security policy requires that a user may not have more than 3 concurrent sessions active in any given application. This solution will be implemented in a new service named the FSC Security Service which will soon bring the existing FSC Inactivity Service capability with greater robustness.</p> <p>The 1184 Payment Tracking &amp; Recertification System is designed to automate the inputting, processing, and tracking of claims for items entered via Standard Form 1184. The system is accessed via an Intranet connection from any Internet browser within the VA network.</p> <p>A Web Service that FSC apps call to verify if the user has used the app in the past 90 days, and if not, then the app will block the user from usage. The app passes to the service the login id of the user, and the id of the application they are trying to use, and the service sends back a result code informing if the user has used the app within the last 90 days. The Service tracks the datetime of the users and apps in it's own database.</p>

	<p>Web application used by FSC Staff as a tool for station cashiers to report it when they disburse money to individuals. It has a mechanism for reports to be reviewed and certified.</p> <p>The Change Management application provides the Change Manager with an interface to input and update change requests (CR) and run various reports (i.e., Open Change Requests, Requests by Developer, etc...). Information from this application has been used to complete SAS 70 audits of the Change Management process.</p> <p>The eClaims Payer manager (PayerSwitchDDE) is an internal web page that maintains the various Payer Tables for the eClaims PreProcessor.</p> <p>Combination website (administrative), service and console application- used on many of our servers, to watch for the receipt of files so they can be immediately processed. This is done instead of using a periodic process in order to ensure databases are updated as quickly as we receive the data. The web application portion is only used for the purpose of updating the even details.</p> <p>The Employee Information System was written for use by Fiscal Service Center (Austin, TX) employees, only. It is meant to capture essential identifying information about employees, including their address, phone and other contact information as well as vehicle identification (for security purposes) and division placement (used, for example, during fire drills at the FSC).</p> <p>FAS Accounting Training system is an application where FSC employees and contractors can register for training class and get updated with latest information on the trainings. This application maintains class attendance, class reminders, notification emails etc. for both instructors as well as participants. There are two user roles and based on authorization levels they can manage class and notifications.</p> <p>FASPAC is the Financial Accounting Service Payment and Collection System web portal available nationwide to Department of Veterans Affairs (VA) stations and Finance Services Center (FSC) personnel. It resides on the VA Intranet and was designed to automate the processing of Intra-governmental Payment and Collection (IPAC) documents. FASPAC provides an efficient and audit friendly method of collecting receivables and disbursing obligations.</p>
--	--

Web application used by FSC administrative staff to add/edit/remove GLAccount and update users' info. Proforma Transaction Lists are updated weekly (Mondays) from FMS. GL Accounts are not automatically updated from FMS. Allowed Staff can view proforma reports and GI Account reports. This application will allow VA Medical Centers the ability to enter veterans' EFT information into the VA's Financial Management System (FMS). Group Tool allows the user to look up information about a user account using either their Active Directory ID or their domain ID. It is meant to be a helpful tool for the FTS IT team when investigating account information in the various web applications supported at the FSC. The Individual Development Plan (IDP) application tracks employee goals, skills, and training classes. At the beginning of every fiscal year, employees should sit down with their supervisor to discuss their expectations for the upcoming fiscal year. These goals and skills should be submitted and approved within the application. The employees should also enter training class requests in the system, which follows a chain of approval before the training administrator registers the employee for the class. There are a set of reports available to help management, budget administrators, and training administrators track estimated and actual training costs, upcoming training classes, etc.

As part of the Economic Stimulus Plan, the Veterans Benefits Administration is authorized to make payments to certain Filipino World War II veterans beginning on April 1st, 2009. This is currently a onetime program with estimated total payments of \$198M and the volume is anticipated to be around 12,000 payments. There are currently 14,000 applications on file for this benefit and this program is a major priority in the Department of Veteran's Affairs.

NW Payroll application contains a record of all VA separated employees (back to circa 1992) who were covered by a retirement system at the time of their separation from the VA. It is also used to document retirement corrections cases and holds a record for every VA employee (again covered by retirement) who has now been converted over to DFAS payroll. It is used as an on-line tracking system to locate specific records for OPM inquiries and research, which eliminates paper and the use of microfiche and conserves on physical storage.

The OFMR application is intended to provide a web-based system for the retrieval of financial record reports. It will server pay information for all VA employees for every pay period since September 1999. It also serves as a research tool when processing audits, retro actions, etc. This web application will be used by PS Service employees and certified payroll technicians nationwide. It will reside on FSC Direct and will require SSL (https). The Online Form Submissions (OFS) has as part of its system a Windows Service application that runs C# code called “plugins” to perform tasks related to forms processing. The website is used to submit form requests for various level of access across VA FSC. Different kinds of access include Database, Remote access, new employee requests, permissions for servers, applications, share drives etc.

The ABC Project Portal application is used by the VAFSC to define and track project costs. Projects are created and assigned codes to internally identify them as well as track them. Employees/Users of the application are required to use the application to log their time on a daily basis and account for their time using ABC project codes hierarchically (Process -> ABC Activity). Users are granted access to specific areas of the application based on their role. The application provides extensive reporting capabilities as well as an array of administrative tasks which include user management, project management, system configuration, and maintenance functions.

The FOS Time Track is used to track time entered against projects, including meetings, Downtime, breaks, Scanning or any other Project Manager or Admin-defined tasks. Only FSC full time personnel use this application. An ABC report within this application summarizes the hours entered by the user for each pay period so they can enter the correct codes and hours into the ABC (AKA Project Portal) each period.

The Vendor Check web applications allows FSC internal users to access information about vendor status, full name, vendor code, duns number, address, and other information.

Web Application used by FSC staff to update Vendor Information - usually stored in the FSCDataDepot.VendorFile Table.

The VMS project will deliver an intranet web application for VHA agents to manage Veterans’ information via an Intranet Portal to FMS Vendor Table. The solution will

	Leverage existing FSC Vendor Service to publish the data from VHA to FMS.
VACHoice	The VA Choice program provides healthcare benefits for Veterans who meet one or more of the following criteria: are located more than 40 miles from a VA healthcare facility, need a specialist not available at nearby VA healthcare facility or are not able to obtain a medical appointment within 30 days at a nearby VA healthcare facility. The VA works with third party contractors to facilitate care for these Veterans and coordinates appointments with non-VA providers to ensure quality care is provided. Each contracted administrator uses different processes to provide Veteran Choice care and to provide authorization information to the VA.
Healthcare Claims Processing System (HCPS)/Referral Authorization System (RAS) Application	The HCPS project was initiated to deliver a claims processing system that will pay, adjudicate, and document all Fee Program claims for the VISN 11 hospitals, sites, civil hospitals, and non-VA Providers. This project is designed to support expedited payment of purchased care claims, as well as to assure proper payment to all third-party medical services providers.
Charge Card Portal (CCP)	The Charge Card Portal Application is intended to support the Government Charge Card Abuse Prevention Act of 2012 which mandates that federal agencies put new controls on government charge cards and enforce more stringent penalties for violations by federal employees. Currently, all agencies within the Department of Veterans Affairs (VA) issue three types of charge cards to their employees when necessary. These cards include travel, purchase cards, and fleet cards. The CCP product will send an automatic reminder notification to the cardholders requesting them to complete the forms. This will reduce the effort currently required of the A/OPCs to follow up with cardholders and program officials to ensure that the forms are completed on time. Further, CCP shortens the turnaround time between the cardholders and other officials who need to sign each form.
Equipment Lease Management System (ELMS)	This project is proposed for the Financial Services Center (FSC), partnering with the Office of Finance (OF), to provide tracking for VA-wide equipment lease management services (ELMS). This project is intended to help resolve findings from the VA Financial Statement Audit performed in Fiscal Year (FY) 2014. FSC lease management services shall include a user interface



	<p>capability for specified VA users to enter required accounting data, general information, supporting documentation for operating and capital leases as well as a search capability and a way to store all appropriate lease data. Additionally, reporting services will be provided as requested.</p> <p>This project supports the FSC's overall vision of providing high-quality financial services to our customers.</p>
Beneficiary Travel Self-Service System (BTSSS)	<p>The Beneficiary Travel Self-Service System (BTSSS) is a travel reimbursement solution providing a Veteran-focused experience for beneficiary travel reimbursements. The solution makes an intuitive interface available to Veterans and caregivers for submitting and tracking their beneficiary travel claims, relating to travel to and from VA health care or VA authorized non-VA health care service locations.</p>
Permanent Change of Station Portal (PCSP)	<p>The Permanent Change of Station (PCS) system is declared a Major Application hosted on the Financial Services Center's (FSC's) General Support System (GSS). The PCS system is a web Portal solution to manage folders, obligations, advances, claims, and payments. The portal is used daily to administrate forms 3918 ,3036, 1038 and 1012 for authorizing and approving employee moves, travel advances, travel authorizations, manage claims received from travelers, create obligations, advances, and payments that are submitted to FMS or IFAMs. Additionally, PCS reports payments to DFAS every two weeks.</p> <p>Information Technology (IT) services that support the PCS application include security and management features reside on the FSC Network. This includes but is not limited to local- and wide-area network (LAN/WAN) management, facilities for data warehousing, archival storage, fully supported electronic commerce/electronic data interchange, comprehensive disaster recovery programs, output preparation and distribution, full-service help desk, and user interfaces/support features.</p> <p>PCS Portal was designed to automate the whole process to relocate an employee to VA. The system interacts with all users in automated mode providing functionality to create and sign electronically all Forms required through the life cycle of the process.</p> <p>PCS provides manual and automated claims processes.</p>
Treasury Reconciliation (SF224)	<p>The FAS (Financial Accounting Services) Treasury Reconciliation Section researches and reconciles Treasury Statement of Differences related to the SF 224</p>

	reports and provide FASMatch cash reconciliation services for collections and disbursements.
Community Care Non-Network Claims (CCNNC)	Web application used by FSC staff to provide member, authorization and claim processing services for all program at the FSC. Initially, Non-Network claim and Dialysis claims will be processed. the other program type claims will be added later.
Defense Medical Logistics Standard Support (DMLSS)	DMLSS is an automated and integrated IT system. DMLSS serves the distinct role of providing integrated medical logistics support for the full spectrum of health care facilities business needs to support prevention and primary, secondary, and tertiary medical care. DMLSS brings together an integrated suite of logistics modules to support the continental United States and overseas MTFs. It provides functions such as Asset Management, Materiel Management, Equipment and Biomedical Maintenance Management, and Facility/Environment of Care Management. DMLSS has a robust acquisition capability and interfaces financial processes with all Service Components.
Provider Portal	Web application used by FSC staff and external providers to access EOB information for services previously rendered. The EOBs are made available in advance of the paper EOBs received by the vendors and allow them to reconcile services to payments. Staff portals have their own screens that allow them extended access to information for all providers so that they may provide phone help to the vendors.
Prior Year Recovery (PYR)	The PYR Project is to automate the Prior Year Recovery (PYR) process by extracting the relevant transactions from FMS, generate the appropriate corrections, and post them to FMS so that the FSC reduces audit exceptions. The corrections are aimed at reducing unnecessary over/understatement of the year end obligation balances.
Lockbox	The Lockbox Project is to automates receiving, storing, and sending data from a centralized location related to Debit Vouchers so that I may reconcile unmatched Veteran payments, provide data that creates the appropriate direct disbursement advance (DV) transactions in the centralized accounting system used by the VA, and provide data to the correct CPAC/Station so that the Veteran's account may be updated accordingly.
offSet	This database will contain payment information.
Kofax	This database will contain all scan and fax documents (for several applications such as ALAC, Retirement Suite, Travel, Vendorizing, OGA, DMC etc.) along with

	DLN, MetaData and document path. SOA/OSB services will pick data from this table and import into FileNet.
FSC Customer	This database stores CRM customer information.
ELMS	This database stores Enterprise lease management system information.
FSCDataDepot	We retrieve OBLH, PaymentHistory, Station, Vendor Details etc. from this database for several internal applications (such as BTSSS, ALAC etc.)
CCS	CCP retrieve cards and transaction information from CCS database.
CCP	This database stores 0242, user registration, charge card and transaction information.
HCPS	This database stores referrals, provider, member and authorization information
EPS Payment	We will retrieve payment details from this database (based on Checking Number, Routing Number, Agency Tracking Id etc.) for LockBox Application.
VAChoice	This database stores VA choice payment, remit and pit processing data related PCM TRIWEST application
PCM_VAChoice_TW	This database stores member, provider, referral and claims information related to TRIWEST application
PCM_VAChoice_HN	This database stores member, provider, referral and claims information related to HEALTHNET application
DashBAM	This database is used to store request and response payload's of OSB services. We will store request/responses for FileNet calls for internal applications (such as ALAC, Travel, Retirement Suite, PCS Portal, Vendorizing etc.).
Frontier	This database stores canceled check data.
DMS	N/A This Database does not exist.

The SORNS applicable to MuleSoft ESB is SORN 13VA047.

([https://www.oprm.va.gov/privacy/systems\\_of\\_records.aspx](https://www.oprm.va.gov/privacy/systems_of_records.aspx)).

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

- Nothing will be changed after the completion of this PIA in circumstances that require changes to business processes.
- 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.

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:

- |   |  |   |
|---|--|---|
| <input checked="" type="checkbox"/> Name  | <input type="checkbox"/> Mother's Maiden Name                              | <input checked="" type="checkbox"/> Personal Phone Numbers(s)                         |
| <input checked="" type="checkbox"/> Social Security Number  | <input checked="" type="checkbox"/> Personal Mailing Address               |   |
| <input checked="" type="checkbox"/> Date of Birth   |  |   |
| <input checked="" type="checkbox"/> Personal Fax Number   | <input checked="" type="checkbox"/> Vehicle License Plate Number           | <input type="checkbox"/> Military History/Service Connection                          |
| <input checked="" type="checkbox"/> Personal Email Address  | <input checked="" type="checkbox"/> Internet Protocol (IP) Address Numbers | <input type="checkbox"/> Next of Kin  |
| <input type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a different individual) | <input type="checkbox"/> Current Medications                               | <input checked="" type="checkbox"/> Other Unique Identifying Information (list below) |
| <input checked="" type="checkbox"/> Financial Account Information   | <input checked="" type="checkbox"/> Previous Medical Records               |   |
| <input type="checkbox"/> Health Insurance Beneficiary Numbers   | <input checked="" type="checkbox"/> Race/Ethnicity                         |   |
| <input type="checkbox"/> Account numbers  | <input checked="" type="checkbox"/> Tax Identification Number              |   |
| <input checked="" type="checkbox"/> Certificate/License numbers   | <input checked="" type="checkbox"/> Medical Record Number                  |   |
|   | <input type="checkbox"/> Gender  |   |
|   | <input type="checkbox"/> Integration Control Number (ICN)                  |   |

Version Date: October 1, 2021

Page 11 of 46

Additional Information Collected but Not Listed Above Here (For Example, A Personal Phone Number That Is Used as A Business Number)

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

MuleSoft FSC Enterprise Service Bus 2.0 (MuleSoft FSC ESB) consists of 15 key components (databases). 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 (MuleSoft FSC ESB) and the reasons for the collection of the PII are in the table below.

It 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 APIs 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.

PII is not directly involved in this system, but other systems are managed by access controls such as Multi-Factor Authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

### PII Mapped to Components

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

The first table of 3.9 in the PTA should be used to answer this question.

#### PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/Storage of PII	Safeguards
offSet Kofax FSC Customer ELMS FSCDataDepot CCS CCP HCPS EPS Payment VAChoice PCM_VAChoice_TW PCM_VAChoice_HN DashBAM Frontier DMS	<b>No (Only transports)</b>	<b>Yes</b>	<ul style="list-style-type: none"> <li>• <i>Name</i></li> <li>• <i>SSN</i></li> <li>• <i>Passport</i></li> <li>• <i>Driver's License</i></li> <li>• <i>Taxpayer ID</i></li> <li>• <i>Patient ID Number</i></li> <li>• <i>Credit Card Number</i></li> <li>• <i>Financial Account Number</i></li> <li>• <i>Address Information</i></li> <li>• <i>Asset Information</i></li> <li>• <i>Telephone Numbers</i></li> <li>• <i>Vehicle Registration Number</i></li> <li>• <i>Title Number</i></li> <li>• <i>Date of Birth</i></li> <li>• <i>Age</i></li> <li>• <i>Place of Birth</i></li> </ul>	<b>For Production Support</b>	Internal protection is managed by access controls such as Multi-Factor Authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

			<ul style="list-style-type: none"> <li>• <i>Race</i></li> <li>• <i>Religion</i></li> <li>• <i>Employment Information</i></li> <li>• <i>Security Clearance Information</i></li> <li>• <i>Medical Information</i></li> <li>• <i>Education Information</i></li> <li>• <i>Financial Information</i></li> <li>• <i>Drug Test results</i></li> <li>• <i>Criminal History</i></li> <li>• <i>Marital Status</i></li> <li>• <i>Family History</i></li> <li>• <i>Fax Number</i></li> <li>• <i>Account Numbers</i></li> <li>• <i>Email Address</i></li> <li>• <i>Date of Death</i></li> <li>• <i>Date of Admission</i></li> <li>• <i>Date of Discharge</i></li> <li>• <i>Vehicle and Serial Number</i></li> <li>• <i>Internet Protocol (IP) Address Numbers</i></li> <li>• <i>Device Identifiers</i></li> </ul>		
--	--	--	--	--	--

			<i>and serial Number</i> <ul style="list-style-type: none"> <li>• <i>Web URLs</i></li> <li>• <i>Medical Record Number</i></li> </ul>		
--	--	--	--	--	--

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

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

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

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

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 (CPAC))



FSC Internal Applications
VACHoice
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

### 1.3 How is the information collected?

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

*technologies or other technologies used in the storage or transmission of information in identifiable form?*

*If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.*

*This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

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.

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

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

*If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.*

*This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.*

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.

#### **1.5 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*

Version Date: October 1, 2021

Page 17 of 46

*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.*

*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:

Version Date: October 1, 2021

Page 18 of 46

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

## Section 2. Uses of the Information

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

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

*Identify and list each use (both internal and external to VA) of the information collected or maintained.*

*This question is related to privacy control AP-2, Purpose Specification.*

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

Name: used to identify a veteran.

Social Security Number: used to identify a veteran.

Date of Birth: used to identify a veteran.

Mother's Maiden Name: used to identify a veteran.

Personal Mailing Address: used to contact a veteran for mailing.

Personal Phone Number(s): used to contact a veteran.

Personal Fax Number: used to share documentation with the Veteran.

Personal Email Address: used to contact a veteran.

Financial Account Information: make payments to Vendors.

Account numbers: make payments to Vendors.

Certificate/License numbers:

Vehicle License Plate Number:

Internet Protocol (IP) Address Numbers: System IP

Previous Medical Records: used for a veteran.

Race/Ethnicity: veteran.

Tax Identification Number: Tax ID used as a vendor identifier.

Medical Record Number: for Veteran's records.

Driver's License

Patient ID Number: for Veteran's record

Credit Card Number: make payments to Vendors  
Asset Information: make payments to Vendors  
Drug Test results: used for a veteran  
Marital Status: used for a veteran  
Family History: used for a veteran  
Date of Death: used for a veteran  
Medical Record Number: used for a veteran  
Passport: used for a veteran  
Driver's License: used for a veteran  
Credit Card Number: make payments to Vendors  
Asset Information: used for a veteran  
Title Number: used for a veteran  
Place of Birth: veteran place of birth  
Religion: used for a veteran  
Employment Information: used for veteran  
Security Clearance Information: used for veteran  
Education Information: used for veteran  
Drug Test results: used for veteran  
Criminal History: used for veteran  
Marital Status: used for veteran  
Family History: used for veteran  
Account Numbers: used for veteran  
Date of Death: time of veteran  
Date of Admission: used for veteran  
Date of Discharge: used for veteran  
Device Identifiers and serial Number: used for veteran  
Web URLs: used for veteran

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

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

*If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the*

individual? If so, explain fully under which circumstances and by whom that information will be used.

*This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information*

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.

### **2.3 How is the information in the system secured?**

*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?*

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

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

### **2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?**

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

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

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

Principle of Use Limitation: *Is the use of information contained in the system relevant to the mission of the project?*

*This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.*

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.

## **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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?*

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

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

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

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

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:

[https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2016-0016\\_sf115.pdf?\\_ga=2.69375632.1057398564.1661111506-1381196282.1661111506](https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2016-0016_sf115.pdf?_ga=2.69375632.1057398564.1661111506-1381196282.1661111506)



### **3.4 What are the procedures for the elimination of SPI?**

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

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

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?*

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

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.*

*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.

**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

<b>List the Program Office or IT System information is shared/received with</b>	<b>List the purpose of the information being shared /received with the specified program office or IT system</b>	<b>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</b>	<b>Describe the method of transmittal</b>
IPPS	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• Name</li> <li>• SSN</li> <li>• Address Information</li> <li>• Date of Birth</li> <li>• Email Address</li> </ul>	Soap Services/Rest APIs
CPM/CEP	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• Name</li> <li>• SSN</li> <li>• Taxpayer ID</li> <li>• Patient ID Number</li> <li>• Financial Account Number</li> <li>• Address Information</li> <li>• Telephone Numbers</li> <li>• Date of Birth</li> <li>• Medical Information</li> <li>• Financial Information</li> <li>• Medical Record Number</li> </ul>	Soap Services/Rest APIs
DMS/DMC Applications (includes CPAC)	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• Name</li> <li>• SSN</li> <li>• Passport</li> <li>• Driver's License</li> <li>• Taxpayer ID</li> <li>• Patient ID Number</li> <li>• Credit Card Number</li> <li>• Financial Account Number</li> </ul>	Soap Services/Rest APIs

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
		<ul style="list-style-type: none"> <li>• Address Information</li> <li>• Asset Information</li> <li>• Telephone Numbers</li> <li>• Vehicle Registration Number</li> <li>• Title Number</li> <li>• Date of Birth</li> <li>• Age</li> <li>• Place of Birth</li> <li>• Race</li> <li>• Religion</li> <li>• Employment Information</li> <li>• Security Clearance Information</li> <li>• Medical Information</li> <li>• Education Information</li> <li>• Financial Information</li> <li>• Drug Test results</li> <li>• Criminal History</li> <li>• Marital Status</li> <li>• Family History</li> <li>• Fax Number</li> <li>• Account Numbers</li> <li>• Email Address</li> <li>• Date of Death</li> <li>• Date of Admission</li> <li>• Date of Discharge</li> <li>• Vehicle and Serial Number</li> <li>• Internet Protocol (IP) Address Numbers</li> <li>• Device Identifiers and serial Number</li> <li>• Web URLs</li> <li>• Medical Record Number</li> </ul>	
FSC Internal Applications	The purpose of information is to accomplish	<ul style="list-style-type: none"> <li>• Name</li> <li>• SSN</li> <li>• <i>Passport</i></li> </ul>	Soap Services/Rest APIs

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
	business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• <i>Taxpayer ID</i></li> <li>• <i>Credit Card Number</i></li> <li>• <i>Financial Account Number</i></li> <li>• <i>Address Information</i></li> <li>• <i>Telephone Numbers</i></li> <li>• <i>Date of Birth</i></li> <li>• <i>Security Clearance Information</i></li> <li>• <i>Financial Information</i></li> <li>• <i>Family History</i></li> <li>• <i>Fax Number</i></li> <li>• <i>Account Numbers</i></li> <li>• <i>Email Address</i></li> <li>• <i>Date of Death</i></li> </ul>	
VA Choice	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• <i>Name</i></li> <li>• <i>SSN</i></li> <li>• <i>Taxpayer ID</i></li> <li>• <i>Patient ID Number</i></li> <li>• <i>Financial Account Number</i></li> <li>• <i>Address Information</i></li> <li>• <i>Telephone Numbers</i></li> <li>• <i>Date of Birth</i></li> <li>• <i>Medical Information</i></li> <li>• <i>Financial Information</i></li> <li>• <i>Drug Test results</i></li> <li>• <i>Date of Admission</i></li> <li>• <i>Medical Record Number</i></li> </ul>	Soap Services/Rest APIs
HCPS/RAS Application	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• <i>Name</i></li> <li>• <i>SSN</i></li> <li>• <i>Taxpayer ID</i></li> <li>• <i>Patient ID Number</i></li> <li>• <i>Address Information</i></li> <li>• <i>Telephone Numbers</i></li> <li>• <i>Date of Birth</i></li> <li>• <i>Medical Information</i></li> <li>• <i>Financial Information</i></li> </ul>	Soap Services/Rest APIs

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
		<ul style="list-style-type: none"> <li>• <i>Drug Test results</i></li> <li>• <i>Date of Admission</i></li> <li>• <i>Medical Record Number</i></li> </ul>	
CCP	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• <i>Name</i></li> <li>• <i>Credit Card Number</i></li> <li>• <i>Financial Account Number</i></li> <li>• <i>Address Information</i></li> <li>• <i>Telephone Numbers</i></li> <li>• <i>Vehicle Registration Number</i></li> <li>• <i>Financial Information</i></li> <li>• <i>Account Numbers</i></li> <li>• <i>Email Address</i></li> </ul>	Soap Services/Rest APIs
ELMS	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• <i>Name</i></li> <li>• <i>Financial Account Number</i></li> <li>• <i>Address Information</i></li> <li>• <i>Asset Information</i></li> <li>• <i>Telephone Numbers</i></li> <li>• <i>Vehicle Registration Number</i></li> <li>• <i>Financial Information</i></li> <li>• <i>Account Numbers</i></li> <li>• <i>Email Address</i></li> <li>• <i>Vehicle and Serial Number</i></li> </ul>	Soap Services/Rest APIs
BTSSS	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• <i>Name</i></li> <li>• <i>SSN</i></li> <li>• <i>Driver's License</i></li> <li>• <i>Taxpayer ID</i></li> <li>• <i>Financial Account Number</i></li> <li>• <i>Address Information</i></li> <li>• <i>Telephone Numbers</i></li> <li>• <i>Financial Information</i></li> <li>• <i>Fax Number</i></li> <li>• <i>Account Numbers</i></li> <li>• <i>Email Address</i></li> </ul>	Soap Services/Rest APIs

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
PCS Portal	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• SSN</li> </ul>	Soap Services/Rest APIs
SF224	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• Name</li> <li>• <i>Financial Account Number</i></li> <li>• <i>Telephone Numbers</i></li> <li>• <i>Financial Information</i></li> <li>• <i>Account Numbers</i></li> <li>• Email Address</li> </ul>	Soap Services/Rest APIs
CCNNC	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• Name</li> <li>• SSN</li> <li>• <i>Taxpayer ID</i></li> <li>• <i>Patient ID Number</i></li> <li>• <i>Address Information</i></li> <li>• <i>Telephone Numbers</i></li> <li>• <i>Date of Birth</i></li> <li>• <i>Medical Information</i></li> <li>• <i>Financial Information</i></li> <li>• <i>Drug Test results</i></li> <li>• <i>Date of Admission</i></li> <li>• <i>Medical Record Number</i></li> </ul>	Soap Services/Rest APIs
DMLSS	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• Taxpayer ID</li> <li>• <i>Financial Account Number</i></li> <li>• Financial Information</li> </ul>	Soap Services/Rest APIs

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
Provider Portal	The purpose of information is to accomplish business functionality implemented by the Source System.	<ul style="list-style-type: none"> <li>• Name</li> <li>• Address Information</li> <li>• Telephone Numbers</li> <li>• Medical Information</li> <li>• Email Address</li> <li>• Web URLs</li> </ul>	Soap Services/Rest APIs
PYR	The purpose of information is to accomplish business functionality implemented by the Source System.	None	Soap Services/Rest APIs
Lockbox	The purpose of information is to accomplish business functionality implemented by the Source System.	None	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.*

*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.

Version Date: October 1, 2021

Page 31 of 46



**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*

<i>List External Program Office or IT System information is</i>	<i>List the purpose of information being shared / received /</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)</i>	<i>List the legal authority, binding agreement, SORN</i>	<i>List the method of transmission and the measures in</i>
---	--	---	--	--

Version Date: October 1, 2021

Page 32 of 46

<i>shared/received with</i>	<i>transmitted with the specified program office or IT system</i>	<i>with the Program or IT system</i>	<i>routine use, etc. that permit external sharing (can be more than one)</i>	<i>place to secure data</i>
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.*

*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:** If a user shares PII/PHI with external sources, violation of PII, PHI and HIPAA and privacy regulations would occur.

**Mitigation:** The MuleSoft ESB does not provide any PII or PHI that the user wouldn't already have access to, and the information is read only, upon request. Providers must register via ID.me and have SAM.gov affiliation. They must also know specific claim 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 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?**

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

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

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

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.
- Encryption data

**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 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.*

*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 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

## Section 7. Access, Redress, and Correction

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

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

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

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

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

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

### 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 by other processes specific to a program, system, or group of systems.*

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

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

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.

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?

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

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

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

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

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.

**8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?**

*If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.*

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

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.

**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?**

*If Yes, provide:*

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

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

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

No date for Initial Operating Capability (IOC) – Tentative date will be on October 01, 2022

## **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*

Version Date: October 1, 2021

*for the assessment to comply with VA Handbook 6517. Types of cloud models include Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).*

*This question is related to privacy control UL-1, Information Sharing with Third Parties.*

*Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.*

Yes, 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)**

*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*

<b>ID</b>	<b>Privacy Controls</b>
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice

Version Date: October 1, 2021

Page 43 of 46

<b>ID</b>	<b>Privacy Controls</b>
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

**Signature of Responsible Officials**

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

---

**Privacy Officer, Deea Lacey**

---

**Information System Security Officer, Rito-Anthony Brisbane**

---

**Information System 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).