Privacy Impact Assessment for the VA IT System called:

Data Management Interface
Austin Information Technology Center (AITC)
VA Central Office (VACO)

Date PIA submitted for review:

05/09/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov	202-632-8431
Information System Security Officer (ISSO)	Joseph Facciolli	Joseph.Facciolli@va.gov	215-983-5299
Information System Owner	Mark S. Kelley	Mark.Kelley2@va.gov	512-326-6331

Abstract

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

The Data Management Interface (DMI) is an interface engine on the Austin Information Technology Center (AITC) Enterprise Server Mainframe developed at the AITC. DMI receives and stores data from VA Medical Centers and Clinics in the form of messages for subsequent use by applications that process at the AITC. DMI also receives and stores data from applications in the form of reports, error messages or transactions for database update and transmits these items to the Medical Centers.

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. The IT system name and the name of the program office that owns the IT system.

Data Management Interface (DMI) Austin Information Technology Center (AITC)

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

The Data Management Interface (DMI) is owned by Austin Information Technology Center (AITC) DMI is an interface engine or "message broker" on the AITC Enterprise Server Mainframe developed at the AITC. DMI receives and stores data from VA Medical Centers and Clinics in the form of messages for subsequent use by applications that process at the AITC. DMI also receives and stores data from applications (reports, error messages or transactions for database update) and transmits it to the Medical Centers. No data is shared outside of the owning applications. This is thru 'bleed' and 'xmit; functions that run from the owning applications.

DMI acknowledges receipt of messages from the Medical Centers and receives delivery confirmation for successful transmission of messages to the Medical Centers. DMI saves the messages for a specific period for retransmission to stations, or re-extract for applications as necessary. DMI also contains a file transfer capability for data exchange with entities outside of the VA.

C. Indicate the ownership or control of the IT system or project.

The Data Management Interface (DMI) is owned by Austin Information Technology Center (AITC)

2. Information Collection and Sharing

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

DMI Has 35,000 on average in input messages daily. These are records of veterans, dependents, and VA employees. In all, an estimated 6.8 million individuals will have their Personally Identifiable Information (PII) stored in DMI.

E. *A general description of the information in the IT system and the purpose for collecting this information.*

DMI passes information/data received from Defense Logistics Agency (DLA) and then transmitted to other VA systems. DMI stores the information in the database and provide this to all the applications that are running on the mainframe.

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

DMI passes information/data received from Defense Logistics Agency (DLA) and then transmitted to other VA systems. DMI stores the information in the database and provide this to all the applications that are running on the mainframe.

G. *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.*

DMI operates at only one site.

3. Legal Authority and SORN

H. *A citation of the legal authority to operate the IT system.*

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled" Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31,United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

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?*

Data in DMI is not retrieved by personal identifier therefore a SORN is not required.

4. System Changes

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

The completion of this PIA will not result in business process changes.

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

The completion of this PIA will not result in any 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:

☒ 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*
☒ 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)

PII Mapping of Components (Servers/Database)

Data Management Interface consists of 1 key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Data Management Interface 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

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
EO Enterprise Infrastructure Support-Mainframe (EIS-M)	Yes	No	Name, Social Security Number (SSN), Date of Birth (DOB), Mother's Maiden Name, Mailing address, Phone Number(s), Fax Number, Email Address, Emergency Contact, Financial Information, Health Insurance Beneficiary Numbers Account numbers, Vehicle License Plate Number, Current Medications, and Previous Medical Records, Race/Ethnicity	Receive and Transmission	TCIP / Transmitted via secure electronic data exchange

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?

The information sources for DMI system are provided by VA Medical Centers, VA systems and the Defense Logistics Agency (DLA) of the Department of Defense (DOD). DMI receives the information and passes it to the application that processes it. Some source systems collect data directly from the veteran. Source systems include:

Credit Card System (CCS)
Computer Assisted Payment Processing System (CAP)
Electronic Data Interchange – Procurement (EDP)
Electronic Data Interchange – FSC (EDF)

Financial Management System (FMS)
LOG Procurement History and Cataloging (ISM)
National Item File (NIF)

Sources of information include the following VHA systems:

Automated Safety Incident Surveillance and Tracking System (AST)
Consolidated Co-Payments Processing Center (CCP)
Central FEE (FEE)
Debt Management System (DM2)
Decision Support System (DSS)
Data Translation (DT1)
Emerging Pathogens Initiative (EPI)
Functional Status Outcomes Database (FIM)
Hospital Laboratory (LAB)
Home Based Primary Care (HBC)
First Party Lockbox (LBX)
Logistics (LOG)
Non- VA Hospital System (NVH)
Patient Treatment File (PTF)
Treasury Offset Process (TOP)

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.

The information sources for DMI system are provided by VA Medical Centers, VA systems and the Defense Logistics Agency (DLA) of the Department of Defense (DOD).

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

DMI does not create any new information.

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?

All DMI system information is derived from other data source systems in the form of data transfers and messages. The information from the Medical Centers is transmitted to DMI via Vista Mailman. Information from the DLA is transmitted by Secure File Transfer Protocol (SFTP).

1.3b 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.

DMI does not perform system checks for accuracy using a commercial aggregator.

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.

DMI does not examine the data in the message for content. DMI only verifies that the data is formatted correctly, i.e., contains a valid application code in the header, has an end of message indicator, and does not exceed the allowable message length. Any checking for completeness is performed by the data owning application.

1.4b 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.

DMI does not perform system checks for accuracy using a commercial aggregator.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31,United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

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

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

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

Principle of Purpose Specification: 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: DMI may receive data in the incorrect format and DMI would not be able to ingest or process the data.

Mitigation: DMI verifies that the data is formatted correctly and rejects and sends data back if it's not formatted correctly.

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.

DMI acts as an interface between Mailman server at AITC and 22 other applications. All the information that medical centers send should go through DMI to an application since applications don't have an ability to receive the data directly from the medical centers. DMI receives and stores data from VA Medical Centers and Clinics (VAMC) in the form of messages for subsequent use by applications that process at the AITC. DMI also receives and stores data from applications (reports, error messages or transactions for database update) and transmits it to stations. DMI acknowledges data receipt and successful transmissions and saves the data for a specific period for retransmission to stations, or re-extract for applications as necessary.

The information in the system, messages, is used for the express purpose of passing it to the processing application or transmission to the Medical Centers.

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.

DMI does not analyze data.

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.

DMI does not create new data.

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?

Data in transit uses Secure File Transfer Protocol and Data at rest uses FIPs 199.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

All the information collected by DMI is encrypted on the storage device.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?(see document in chat)

The PII/PHI is encrypted both at the disk storage and visual tape storage.

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:

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

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

2.4a How is access to the PII determined?

The DMI system programmer.

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

The Supervisor based on the job description/role has to put in a request to the YourIT or Service Now department to grant access to the system.

2.4c Does access require manager approval?

Yes

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

No.

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

The DMI System Owner

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

Name, Social Security Number (SSN), Date of Birth (DOB), Mother's Maiden Name, Mailing address, Zip Code, Phone Number(s), Fax Number, Email Address, Emergency Contact, Financial

Information, Health Insurance Beneficiary Numbers Account numbers, Vehicle License Plate Number, Current Medications, and Previous Medical Records, Race/Ethnicity.

3.2 How long is information retained?

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

Two years in archived files unless the source systems identify specific messages/data transfers that are associated with a litigation hold process. The data associated with a litigation hold will be retained for the duration of the process in accordance with VA Directive 6311 and VA Office of General Council Litigation Hold Policy.

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.

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

VHA records controls schedule 10-1. Item 6000.2 (b) 2) Interim Electronic Source Information. Electronic version of source information obtained from other electronic databases, optical disk, or other magnetic media not considered as part of the consolidated patient medical record. May include information generated electronically by medical equipment. Temporary. Destroy/delete after migration of information to another electronic medium. Destruction of interim version of information is not to occur until it has been determined that the migrated information represents an exact duplicate of the previous version of the migrated information. N1-15-02-3, item 2.

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.*

Data is automatically deleted from the message archive store at the end of the 2 year retention period unless a court order/litigation hold procedure requires that it be kept for a longer period. Electronic media sanitization when the records are authorized for destruction (or upon system decommission) will be carried out in accordance with OIT-OIS SOP MP-6- Electronic Media Sanitization and VA Directive 6371-Destruction of Temporary Paper Records.

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

While the messages in DMI may contain PII, we never reference the data contained in the messages. Through the mainframe security package, CA Top-secret, only the DMI admins have access to the database and files that may contain PII or the IT support people whose data it belongs to. DMI is not used as a testing, training or research system.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u>

The risk for information maintained in DMI could be retained longer than necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation:
The system automatically deletes files when the retention period ends at two years.

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***
Veterans' Health Information System & Technology Architecture	Personnel Action Processing • Benefits Management • Compensation	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mother's Maiden Name	Transmitted via secure electronic data exchange from mailman messaging in

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***
(VistA)	Management • Data transfer for end use applications and programs	• Mailing address • Zip Code • Phone Number(s) • Fax Number • Email Address • Emergency Contact • Financial Information • Health Insurance Beneficiary Numbers Account numbers • Vehicle License Plate Number • Current Medications • Previous Medical Records • Race/Ethnicity	VISTA
Automated Safety Incident Surveillance and Tracking Systems (AST)	• Personnel Action Processing • Benefits Management • Compensation Management • Data transfer for end use application	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mailing address • Zip Code • Phone Number(s) • Race/Ethnicity	Transmitted via secure electronic data exchange
Consolidated Co-Payments Processing Center (CCP)	• Benefits Management • Benefits Management • Compensation Management • Data transfer for end use applications and programs	• Name • Social Security Number (SSN) • Mailing address • Zip Code • Current Medications • Previous Medical Records	Transmitted via secure electronic data exchange
Debt Management System (DM2)	• Data transfer for end use applications and programs	Name • Social Security Number (SSN) • Mailing address • Zip Code	Transmitted via secure electronic data exchange
Decision Support System (DSS)	• Benefits Management • Compensation	• Name • Social Security Number (SSN)	Transmitted via secure electronic data exchange

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***
	Management • Data transfer for end use applications and programs	• Date of Birth • Zip Code	
Data Translation (DT1)	• Benefits Management • Compensation Management • Data transfer for end use applications and programs	• No PII or PHI	Transmitted via secure electronic data exchange
Emerging Pathogens Initiative (EPI)	• Benefits Management • Compensation Management • Data transfer for end use applications and programs	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Race/Ethnicity	Transmitted via secure electronic data exchange
Central Fee (FEE)	• Benefits Management • Compensation Management • Data transfer for end use applications and programs	Name • Social Security Number (SSN) • Date of Birth (DOB) • Mailing address • Zip Code • Financial Information • Health Insurance Beneficiary Numbers Account numbers • Current Medications • Previous Medical Records	Transmitted via secure electronic data exchange
Functional Status Outcomes Database (FIM)	• Benefits Management • Compensation Management • Data transfer for end use applications and programs	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mailing address • Zip Code • Phone Number(s) • Race/Ethnicity	Transmitted via secure electronic data exchange

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***
Home Based Primary Care (HBC)	• Benefits Management • Compensation Management • Data transfer for end use applications and programs	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Zip Code • Race/Ethnicity	Transmitted via secure electronic data exchange
Hospital Laboratory (LAB)	• Data transfer for end use applications and programs	• No PII or PHI	Transmitted via secure electronic data exchange
First Party Lockbox (LBX)	• Data transfer for end use applications and programs	• Name • Social Security Number (SSN) • Financial Information	Transmitted via secure electronic data exchange
Non- VA Hospital System (NVH)	• Benefits Management • Compensation Management • Data transfer for end use applications and programs	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mailing address • Zip Code • Phone Number(s)	Transmitted via secure electronic data exchange
Patient Treatment File (PTF)	• Benefits Management • Compensation Management • Data transfer for end use applications and programs	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mother's Maiden Name • Mailing address • Zip Code • Phone Number(s) • Fax Number • Email Address • Financial Information • Health Insurance Information • Vehicle License Plate Number • Race/Ethnicity	Transmitted via secure electronic data exchange

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***
Treasury Offset Process (TOP)	• Benefits Management • Compensation Management • Data transfer for end use applications and programs	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mother's Maiden Name • Mailing address • Zip Code • Financial Information • Health Insurance Beneficiary Numbers Account numbers • Current Medications • Previous Medical Records	Transmitted via secure electronic data exchange
Electronic Data Interchange – Procurement (EDP)	• Benefits Management • Compensation Management • Data transfer for end use applications and programs	• Name • Mailing address • Zip Code • Phone Number(s) • Fax Number • Email Address • Financial Information • Procurement Data • Race/Ethnicity	Transmitted via secure electronic data exchange
LOG Procurement History and Cataloging (ISM)	• Benefits Management • Compensation Management • Data transfer for end use applications and programs	• Name • Zip Code • Email Address	Transmitted via secure electronic data exchange
Credit Card System (CCS)	• Data transfer for end use applications and programs	• Financial Information	Transmitted via secure electronic data exchange
Computer Assisted Payment Processing System (CAP)	• Data transfer for end use applications and programs	• Financial Information	Transmitted via secure electronic data exchange
Electronic Data Interchange – FSC (EDF)	• Benefits Management • Compensation Management	• Name • Mailing address • Zip Code • Phone Number(s)	Transmitted via secure electronic data exchange

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***
	• Data transfer for end use applications and programs	• Fax Number • Email Address • Financial Information	
Financial Management System (FMS)	• Benefits Management • Compensation Management • Data transfer for end use applications and programs	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mother's Maiden Name • Mailing address • Zip Code • Phone Number(s) • Fax Number • Email Address • Emergency Contact • Financial Information • Health Insurance Information • Vehicle License Plate Number • Race/Ethnicity	Transmitted via secure electronic data exchange
National Item File (NIF)	• Benefits Management • Compensation Management • Data transfer for end use applications and programs	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mother's Maiden Name • Mailing address • Zip Code • Phone Number(s) • Fax Number • Email Address • Emergency Contact • Financial Information • Health Insurance Information • Vehicle License Plate Number • Race/Ethnicity	Transmitted via secure electronic data exchange
Logistics (LOG)	• Benefits Management • Compensation Management	• No PII or PHI	Transmitted via secure electronic data exchange

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*
	• Data transfer for end use applications and programs		

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: Privacy risk may be if the data that is available through the application is disclosed and/or misused by an authorized user of the system.

Mitigation: Users are required to sign a rules of behavior document which outlines specific uses for the claims data and the penalty which could be imposed because of misuse of that data. Additionally, access to the DMI system is controlled. The only users with access to the DMI application are the application administrators that manage the system, and the mainframe administrators which manage the mainframe. No other users have access to login and access the application. The Mainframe security group sends an alert when unauthorized access is attempted.

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***
Defense Logistics Agency (DLA) Transaction Services	This is for exchanging cataloging data between two SFTP servers owned by DLA Transaction Services and the Data Management Interface (DMI) application owned by the Enterprise Operations. Then cataloging data is used to order DLA items used by the VA.	Financial Information	Interface Control Agreement (ICA) June 2020	Secure File Transfer Program (SFTP)

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that the data received from DLA could not be processed by the VA because it is not formatted correctly.

Mitigation: The DLA is notified that transmission failed and they must provide an access to a new file.

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.

Notice is provided at the time of collection by the feeder systems in Defense Logistics Agency (DLA). DMI does not collect data from Veterans or the public directly.

DLA Notice: https://www.defense.gov/Legal-Administrative/Privacy-Security
If you choose to provide us with personal information -- like filling out a Contact Us form with email and/or postal addresses -- we only use that information to respond to your message or request. We will only share the information you give us with another government agency if your inquiry relates to that agency, or as otherwise required by law. We never create individual profiles or give it to any private organizations. Defense.gov never collects information for commercial marketing. While you must provide

an email address or postal address for a response other than those generated automatically in response to questions or comments that you may submit, we recommend that you NOT include any other personal information, especially Social Security numbers. The Social Security Administration offers additional guidance on sharing your Social Security number.

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

Notice is provided at the time of collection by the feeder systems Defense Logistics Agency (DLA). DMI does not collect data from Veterans or the public directly. See notice in appendix A.

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 Department of Veterans Affairs does provide public notice that the system does exist. Notice is provided at the time of collection by the feeder systems. DMI does not collect data from Veterans or the public directly. This Privacy Impact Assessment (PIA) serves as notice of the DMI system. As required by the Government Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Individuals may or may not have the right to provide the information collected by the VA Medical Centers. DMI does not participate in the data collection process. Notice is provided at the time of collection by the feeder systems. DMI does not collect data from Veterans or the public directly. Any right to consent would be made through those medical centers and other source applications.

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.

Individuals providing their information, consent when they enter their information to the source system DLA may contact the DLA's Customer Interaction Center is staffed 24/7. You can contact the center via email at dlacontactcenter@dla.mil or toll-free 1-877-DLA-CALL (2255).

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: DMI does not collect information from individuals and therefore does not provide any notice to an individual, DLA is the collection point, and they provide notice. There is a risk that members of the public may not know that the Insurance Payment System exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing the public with a notice that the system exists using this Privacy Impact Assessment. Privacy notices are mailed to each Veteran every 3 years, personnel whom have records in the system can also contact the source record system at DLA's Customer Interaction Center is staffed 24/7. You can contact the center via email at dlacontactcenter@dla.mil or toll-free 1-877-DLA-CALL (2255).

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.***

Information passed through DMI is received from Defense Logistics Agency (DLA) and then transmitted to other VA systems. To access information in the source DLA System please contact the DLA customer Interaction Center below:

The information below provides access to online tools that will answer many basic questions related to doing business with DLA. DLA's self-help tools offer immediate resolutions to common inquiries such as requisition or backorder statuses, as well as on-hand status and stock availability. DLA's network of customer support personnel stands ready to assist customers, but the agency also offers tools to help its customers help themselves. Please note that some of the on-line tools may require individual logins and passwords.

If you find that you have additional questions that the information below doesn't answer for you, DLA's Customer Interaction Center is staffed 24/7. You can contact the center via email at dlacontactcenter@dla.mil or or toll-free 1-877-DLA-CALL (2255).

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).

The DLA record source system and the DMI system are not exempt.

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.

DMI system is not a Privacy Act System of Records. Information passed through DMI is received from Defense Logistics Agency (DLA) and then transmitted to other VA systems.

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.

Information passed through DMI is received from Defense Logistics Agency (DLA) and then transmitted to other VA systems. To correct inaccurate or erroneous information in the source DLA system please contact the DLA customer Interaction Center below:

The information below provides access to online tools that will answer many basic questions related to doing business with DLA. DLA's self-help tools offer immediate resolutions to common inquiries such as requisition or backorder statuses, as well as on-hand status and stock availability. DLA's network of customer support personnel stands ready to assist customers, but the agency also offers tools to help its customers help themselves. Please note that some of the on-line tools may require individual logins and passwords.

If you find that you have additional questions that the information below doesn't answer for you, DLA's Customer Interaction Center is staffed 24/7. You can contact the center via email at dlacontactcenter@dla.mil or toll-free 1-877-DLA-CALL (2255).

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.

At the time of collection and on the DLA page it provides contact information:
If you find that you have additional questions that the information below doesn't answer for you, DLA's Customer Interaction Center is staffed 24/7. You can contact the center via email at dlacontactcenter@dla.mil or toll-free 1-877-DLA-CALL (2255).

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.
Formal redress is provide by DLA:
If you find that you have additional questions that the information below doesn't answer for you, DLA's Customer Interaction Center is staffed 24/7. You can contact the center via email at dlacontactcenter@dla.mil or toll-free 1-877-DLA-CALL (2255).

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: There is no risk related to the VA's access, redress, and correction policies and procedures for this system since messages are not altered in the DMI application

Mitigation: There is no access grated to messages other than the application which owns them, there is no redress in DMI to a function that does not exist. Users may visit the DLA web page or contact the DLA's Customer Interaction Center is staffed 24/7. You can contact the center via email at dlacontactcenter@dla.mil or toll-free 1-877-DLA-CALL (2255).

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.

At the Enterprise Operations, users will submit a completed access request application for General Service System (GSS) access using a VA Form 9957 (or other access request method approved by AITCs Chief, Security Services (00E)) to their first-line supervisor. Or, if appropriate, the user's supervisor may prepare the initial request. The supervisor must sign this request application and submit it to AITCs Security Services (00E). The signed requests are submitted in a digitally signed electronic document. Electronic requests may only be submitted by supervisors physically located within AITC and must be transmitted directly from the supervisor's individual e-mail account to AITC System Access Requests. Security Services personnel will forward completed requests to the GSS Information Security Officer (ISO) and/or technical lead for approval concurrence and then to the appropriate system administrator to create the user account, issue a temporary first login password, and notify the user. User access requests will be maintained and disposed of according to form management requirements. User access requests will be held for 3 years after the termination of each user account. Access to mainframe resources require a 9957 request, with specification as to the needed functional task codes, profiles, and/or data set level of access. Once a user is granted access to the DMI application, their access will be restricted to the messages which are destined to or created by the applications which they are associated with, administer, or manage.

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?

Not Applicable. DMI has no users from other agencies who have access to the system. Although DMI have an interface Control Agreement (ICA) in place with DLA, none of their personnel can access the data in the DMI system.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

All approved DMI users have granted read-only access to the system for the data related to their application area.

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.

Will VA contractors have access to the system and the PII? Yes.

If yes, what involvement will contractors have with the design and maintenance of the system?

Contractors will have one hundred percent (100%) involvement 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? Yes

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.

In accordance with Enterprise Operations (EO) guidance, EO personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VAs Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 2020-06-16
3. *The Authorization Status:* Authorized to Operate (ATO)
4. *The Authorization Date:* 2020-11-02
5. *The Authorization Termination Date:* 2023-11-02
6. *The Risk Review Completion Date:* Please provide response here
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH)*

DMI is a moderate system with an active Full Authorization To Operate (ATO) granted in 2/11/2020

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.***

Not Applicable. See "Yes' response above.

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)*

DMI does not use cloud technology.

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.*

DMI does not use Cloud technology

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.

DMI does not use Cloud technology

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.

DMI does not use Cloud technology

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).

DMI does not use RPA.

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.

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2023.06.09 06:56:06 -06'00'

Privacy Officer, Julie Drake

JOSEPH FACCIOLLI Digitally signed by JOSEPH FACCIOLLI
Date: 2023.06.09 07:05:36 -04'00'

Information Systems Security Officer, Joseph Facciolli

MARK KELLEY Digitally signed by MARK KELLEY
Date: 2023.06.08 14:33:14 -05'00'

Information System Owner, Mark S. Kelley

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).

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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

Defense Logistics Agency Privacy and Security:

The Defense.gov website is provided as a public service by the Office of the Assistant Secretary of Defense for Public Affairs.
If you choose to provide us with personal information -- like filling out a Contact Us form with email and/or postal addresses -- we only use that information to respond to your message or request. We will only share the

information you give us with another government agency if your inquiry relates to that agency, or as otherwise required by law. We never create individual profiles or give it to any private organizations. Defense.gov never collects information for commercial marketing. While you must provide an email address or postal address for a response other than those generated automatically in response to questions or comments that you may submit, we recommend that you NOT include any other personal information, especially Social Security numbers. The Social Security Administration offers additional guidance on sharing your Social Security number.

We maintain a variety of physical, electronic and procedural safeguards to protect your personal information. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration guidelines.

Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

If you have any questions or comments about the information presented here, please forward them to us using our Contact Us page.

Use of Measurement and Customization Technology:

This website uses measurement and customization technology known as a "cookies." Cookies are used to remember a user's online interactions with a website or online application to conduct measurement and analysis of usage or to customize the user's experience.

Two kinds of cookies are used on this website. A single-session cookie (Tier 1) is a line of text that is stored temporarily on a user's computer and deleted as soon as the browser is closed. A persistent or multisession cookie (Tier 2) is saved to a file on a user's hard drive and is called up the next time that user visits a website. Use of these cookies does not involve the collection of a visitor's personally identifiable information.

The Defense Department does not use the information associated with cookies to track individual user activity on the internet outside DOD websites, nor does it share the data obtained through such technologies, without the user's explicit consent, with other departments or agencies. DOD does not keep a database of information obtained from the use of cookies.

Cookies are enabled by default to optimize website functionality and customize user experience. Users can choose not to accept the use of these cookies by changing the settings on their local computer's web browser. The USA.gov website, https://www.usa.gov/optout-instructions, provides general instructions on how to opt out of cookies and other commonly used web measurement and customization technologies. Opting out of cookies still permits users to access comparable information and services; however, it may take longer to navigate or interact with the website if a user is required to fill out certain information repeatedly.

Specific Technologies/Vendors:

Tier 1 cookies are used for technical purposes to improve a user experience and to allow users to more easily navigate the website.

Akamai speeds the delivery of content and applications for customers through using automatic, intermediate and temporary information storage to make the onward transmission of that information to other recipients more efficient. Temporary storage processes retain information only as long as is reasonably necessary to transmit the data. Intermediate storage processes retain information only so long as is reasonably necessary for continued transmission, to maintain the security of the network and the data, to monitor and improve website performance and for related administrative purposes.

Akamai does not collect, use or disclose personally identifiable consumer information.

Foresee Results software measures user satisfaction and assesses website effectiveness through optional surveys presented to website visitors. The information gathered from these surveys is used to identify and prioritize improvements to functional website elements and content for visitors. Survey users provide ratings and feedback related to a series of questions about website performance, aesthetics, usability, user experience, and so forth; however, users are not required to provide any personal information. Tier 2 cookies are used to remember if the user has already been offered the survey and to ensure that users are prompted only once every 60 days.

Urchin software collects aggregate statistics of website visitor characteristics, traffic, and activity. This information is used to assess what content is of most and least interest, determine technical design specifications, and identify system performance or problem areas. The software records a variety of data, including IP addresses (the locations of computers or networks on the internet), unique visits, page views, hits, referring websites and what hyperlinks have been clicked. Tier 2 cookies are used to distinguish between summary statistics for users who have been to the site before and those that are visiting the site the for the first time. The Defense Department does not gather, request, record, require, collect or track any internet users' personally identifiable information through these processes.

Client side opt-out mechanisms allow the user to opt out of web measurement and customization technologies by changing the settings of a specific application or program on the user's local computer. For example, users may be able to disable persistent cookies by changing the settings on commonly used web browsers. For general instructions on how to opt out of some of the most commonly used web measurements and customization technologies, go to https://www.usa.gov/optout-instructions.

Use of Third-Party Websites and Applications

Third-party websites and applications that are not owned, operated, or controlled by the Defense Department are integral to internet-based operations across DOD and used to augment official communication. These capabilities include, but are not limited to, networking services, media sharing services, wikis and data mashups. A list of DOD's authorized pages and uses of these services is available at https://dod.defense.gov/About/Military-Departments/DOD-Websites/. These sites may collect personally identifiable information and may make it available to the DOD and other users; however, the information is not collected on behalf of, nor is it provided specifically for DOD. DOD does not harvest and additionally collect, maintain, share or otherwise use such personally identifiable information for any purpose other than that for which it is made available to all users.