Privacy Impact Assessment for the VA IT System called:

Microsoft Azure Services (MAS -E)

Office of Information & Technology

OIT Product Engineering Services

eMASS ID 2338

Date PIA submitted for review:

03/12/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov OITPrivacy@va.gov	202-632-8431
Information System Security Officer (ISSO)	Albert Comple	Albert.Comple@va.gov	303-914-5439
Information System Owner	Russell Holt	Russell.Holt2@va.gov	970-903-6991

Abstract

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

Microsoft Azure Services (MAS -E) provides inheritance, controls, and the parent relationship within the security boundary for component and minor applications. The components contain PHI/PII that is ingested by multiple minor applications. The minor applications listed in MAS are responsible for their own PTA and PIA.

Overview

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

1 General Description

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

Microsoft Azure Services (MAS -E) provides inheritance, controls, and the parent relationship within the security boundary for component and minor applications. MAS -E is owned by the Product Engineering Program Office. MAS -E is the framework housing Microsoft Power Platform (which includes Power BI, PowerApps, Power Automate, Dynamics365, Power Pages, Microsoft Copilot Studio, and Dataverse) and is part of the VA Azure Cloud environment.

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

Microsoft Azure Services is managed, owned, and operated by VA, Microsoft and their Center of Excellence Team.

2. Information Collection and Sharing

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

10 million unique records.

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

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

MAS is an Enterprise package. It is designed specifically to be a passthrough ATO framework to provide hierarchical controls to be inherited by minor apps (Asses Only packages) as well as the parent relationship that is unable to be provided by a -F or SOR. MAS does not contain hardware, software, databases, URLs, Ports, Protocols, or services. The MAS -E package covers Microsoft's Power Platform applications that are part of the VA Azure Cloud environment. Microsoft CoE team will manage premium license subscriptions and use cases for the VA enterprise. PowerApps is a suite of apps, services, connectors and data platform that provides a rapid application development environment to build custom apps for business needs. Using PowerApps, customers can quickly build custom business apps that connect to business data stored either in the underlying data platform (Common Data Service) or in various online and on-premises data sources (SharePoint, Excel, Office 365, Dynamics 365, SQL Server, and so on). PowerApps includes the Portal, Authoring Service, and RP. Power Automate is a service that helps organizations create automated workflows between applications and services to synchronize files, get notifications and collect data. The service provides a low code platform for workflow and process automation. Automated flows, button flows, scheduled flows, business flows and UI flows are supported by the service.

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

MAS -E houses Microsoft Power Platform, which is a cloud-based SaaS suite of apps that allow for creation of solutions, automations, analytics, portals, and bots.

F. Are the modules/subsystems only applicable if information is shared?

Yes, the module is only applicable if information is shared.

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

No, MAS is operated only at one site.

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

H. What is the citation of the legal authority?

31 U.S. Code 3512- Executive Agency Accounting and other Financial Management Reports and Plans; Federal Managers' Financial Integrity Act section 2 of 1982; Federal Financial Management Improvement Act of 1996; E-Government Act of 2002 title III., Federal Information Security Modernization Act (FISMA) of 2014; Clinger Cohen Act of 1996; 38 CFR part 17 17.120–17.132; OMB Circular A–123, Management's Responsibility for Internal Control. Title 38, United States Code, Sections 501(b) and 304, Inspector General Act of 1978, Public Law (Pub L.) 95–452, 5 U.S.C. App., as amended through Public Law 115–254 (IG Act), 38 U.S.C. 501, Section 527 of 38 U.S.C. and the Government Performance and Results Act of 1993, Public Law 103–62, 38 U.S.C. 1720F, Public Law 110–110 (Joshua Omvig Veterans Suicide Prevention Act); and Public Law 114–247 (No Veterans Crisis Line Call Should Go Unanswered Act), 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E.

I. What is the SORN?

131VA047/88FR60269, Individuals Submitting Invoices-Vouchers for Payment-VA (8/31/2023)
https://www.govinfo.gov/content/pkg/FR-2023-08-31/pdf/2023-18807.pdf

24VA10A7/85FR62406, Patient Medical Records-VA (10/2/2020)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

71VA53/84FR16138, The Office of Inspector General Management Information System (MIS)-VA (4/17/2019
https://www.govinfo.gov/content/pkg/FR-2019-04-17/pdf/2019-07648.pdf

90VA194/89FR19021, Call Detail Records-VA (3/15/2024)
https://www.govinfo.gov/content/pkg/FR-2024-03-15/pdf/2024-05535.pdf

97VA10 / 85 FR 84119 Consolidated Data Information System-VA (12/23/2020)
https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28342.pdf

158VA10/88FR38134, Veterans Crisis Line Records-VA (6/12/2023)
https://www.govinfo.gov/content/pkg/FR-2023-06-12/pdf/2023-12401.pdf

171VA056A / 78 FR 63311, Human Resources Information Systems Shared Service Center (HRIS SSC)-VA (10/23/2013)
https://www.govinfo.gov/content/pkg/FR-2013-10-23/pdf/2013-24830.pdf

172VA10/86FR72688, VHA Corporate Data Warehouse-VA (12/22/2021)
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

This system is not in the process of modifying the existing SORNs.

Yes, SORN will require an update.
171VA056A / 78 FR 63311, Human Resources Information Systems Shared Service Center (HRIS SSC)-VA (10/23/2013)
https://www.govinfo.gov/content/pkg/FR-2013-10-23/pdf/2013-24830.pdf

4. System Changes

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

☐ Yes
☒ No

I. Will the technology changes impact information collection and sharing?

☐ Yes
☒ No

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name ☒ **Full** Social Security

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

Other PII/PHI data elements: Veteran Call History, Beneficiary Profile Information, Debt- financial information, VA email address, User ID (VA employee/Contractor)

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

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

MAS -E/MPP collects information from individuals and VA IT systems.

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.

It is required because more information from VA IT systems than individuals.

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

MAS -E does not create information.

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

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

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?

PII is collected for the purposes of authentication and authorization services by Azure Active Directory. Where PII is collected for support purposes, users are informed that they need to ensure that their contact information is current. PII can be collected numerous ways throughout the Microsoft Azure Government environment: through connections to other system listed in the table above, user input, by report aggregation, electronic transmission, or created by the system.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

This system does not collect data from individuals via a form.

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

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

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

Where the PII is collected for the purposes of authentication and authorization, accuracy validation services are provided by at a minimum Azure Active Directory. Where PII is collected for support purposes, users are informed that they need to ensure that their contact information is current. For amendment of incorrect data via the Azure Portal, tenant admins can correct as necessary. Microsoft also has a process via the Privacy Response Center to redress user submissions for correction or amendment of inaccurate PII.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

This system uses Power BI and OData, commercial aggregators, to check for accuracy of information.

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

31 U.S. Code 3512- Executive Agency Accounting and other Financial Management Reports and Plans; Federal Managers' Financial Integrity Act section 2 of 1982; Federal Financial Management Improvement Act of 1996; E-Government Act of 2002 title III., Federal Information Security Modernization Act (FISMA) of 2014; Clinger Cohen Act of 1996; 38 CFR part 17 17.120–17.132; OMB Circular A–123, Management's Responsibility for Internal Control. Title 38, United States Code, Sections 501(b) and 304, Inspector General Act of 1978, Public Law (Pub L.) 95–452, 5 U.S.C. App., as amended through Public Law 115–254 (IG Act), 38 U.S.C. 501, Section 527 of 38 U.S.C. and the Government Performance and Results Act of 1993, Public Law 103–62, 38 U.S.C. 1720F, Public Law 110–110 (Joshua Omvig Veterans Suicide Prevention Act); and Public Law 114–247 (No Veterans Crisis Line Call Should Go Unanswered Act), 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E.

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: MAS receives data that is incomplete.
MAS -E collects Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation: Re-complete data call. Follow up with end users.
MAS -E employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control, awareness and

training, audit and accountability, certification, accreditation, and security assessments, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity. The Area employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Identification purposes	Identification purposes
Social Security Number	Identification purposes	Not used
Date of Birth	Identification purposes / clinical relevance	Not used
Mailing Address	Identification purposes / contact purposes	Not used
Phone Number	Contact purposes	Contact purposes
Fax Number	Contact purposes	Not used
Email Address	Contact purposes	Contact purposes
Emergency Contact Information	Contact purposes	Not used
Financial Information	Administrative purposes	Not used
Health Insurance Beneficiary Numbers	Communication / billing purposes	Not used
Medical Records	Clinical purposes	Not used
Tax Identification Number	Administrative purposes	Not used
Sex	Clinical relevance	Not used
Integrated Control Number	identification	Not used
Military History / Service Connection	Clinical purposes	Eligibility
Next of Kin	Contact purposes	Not used
Electronic Data Interchange Personal Identifier	Identification purposes	Not used
Veteran Call History	Clinical purposes	Not used

Beneficiary Profile Information	Identification / contact	Not used
Debt- financial Information	Administrative purposes	Not used
VA email address	user authentication, ensuring secure access and verification of authorized individuals	Not used
User ID	user authentication, ensuring secure access and verification of authorized individuals	Not used

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

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

No, MAS does not perform any analysis on the 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.

This system does not create or make available new or previously unutilized information about an individual.

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

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

All Azure services implement internal controls as defined via the Microsoft Privacy Standard. The Microsoft Privacy Standard is a corporate standard that identifies global privacy requirements across all Microsoft services. Security audit logging, controlled access via Azure JIT, and very limited persistent access for a few select individuals limit the risk of internal abuse of PII data in Azure. Data at rest is encrypted and FIPS 140-2 compliant.

Data in transit is encrypted and FIPS 140-2 compliant and employs TLS protocols for secure data transfers.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

The Microsoft Privacy Standard is a corporate standard that identifies global privacy requirements across all Microsoft services. In order to protect SSNs-PII/PHI SFTP works over an SSH data stream to establish secure connection. Encryption algorithms securely move data to a server, keeping files unreadable during the process. To further prevent unauthorized files access, authentication is also enabled.

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

Security audit logging, controlled access via Azure JIT, and very limited persistent access for a few select individuals limit the risk of internal abuse of PII data in Azure.

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

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

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

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

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

2.4a How is access to the PII determined?

IT/Technical people: Salesforce Product Request completed through DTC Marketplace. Added to Azure Security Group for access.
VA employees: Salesforce Product Request completed through DTC Marketplace. Added to Azure Security Group for access.

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

Policy and SOPs (internal is in Confluence, external is in a public facing Sharepoint)

2.4c Does access require manager approval?

Yes, manager approval is required.

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

Yes, there are logs set up by application.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

The Information System Owner is responsible for ensuring safeguards.

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*

Medical Records, Military History / Service Connection, Name, and User ID

3.2 How long is information retained?

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

MAS maintains for 90 days. The minor applications listed in MAS are responsible for their own privacy documents.

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

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

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

Yes, the general record schedule.

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

GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records

https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf

GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records, Item 10, Record Description: Transitory records, Disposition Instruction: Temporary. Destroy when no longer needed for business use, or according to an agency predetermined time period or business rule, Disposition Authority: DAA-GRS-2022-0009-0001.

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.

1. Electronic destruction - manual
3. Media Sanitation SOP
   VA Form 0750-System sanitation
   VA Form 7468- Records Management

Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

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

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

Yes, PII used for research, testing, or training, is required to be removed immediately after those functions have been completed, in accordance with the Acceptable Use Policy that the Business and Information Owner is required to sign. Testing environments can be re-baselined after test periods in order to accomplish this task as well.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

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

Follow the format below:

Privacy Risk: There is a risk that the information contained in the Microsoft Power Platform Dataverse system will be retained for longer than is necessary to fulfill the VA Mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: Azure's data handling policies dictate that customer data and PII tied to a customer must be retained as long as the subscription is active plus 90 days. At the end of the 90-day grace period customer data must be deleted within the subsequent 90 days.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

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

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Microsoft Power Platform (MPP) Apps included in MPP: Dynamics 365 Power Apps Power Automate Power BI Power Pages (Formerly part of Power Apps as "Power Apps Portals") DataVerse Microsoft Copilot Studio (formerly Power Virtual Agents (Bots)).	Yes	Yes	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Email Address • Emergency Contact Information • Military History/Service Connection • Medical Records • Next of Kin • Veteran Call History • Integrated Control Number (ICN) • Fax Number • Tax Identification Number (TIN) • Electronic data interchange personal identifier (EDIPI) • Financial Account Information • Debt- financial information • Beneficiary Profile Information • Health Insurance Beneficiary Numbers/Account Numbers • Sex	To enable secure access, support operational processes, and deliver application solutions, workflow and compliance services.	Encryption, MFA, audit logs, data minimization, least privileged access, privacy policies and training

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

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

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

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

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

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

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
VHA Various Business Offices within VHA	Improvement of services being delivered to Veterans and creating efficiencies for employees delivering that service or supporting those services.	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Email Address • Emergency Contact Information • Military History/Service Connection • Medical Records • Next of Kin • Veteran Call History • Integrated Control Number (ICN) • Fax Number • Tax Identification Number (TIN) • Electronic data interchange personal identifier (EDIPI)	Secure File Transfer Protocol (SFTP)

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		• Financial Account Information • Debt- financial information • Beneficiary Profile Information • Health Insurance Beneficiary Numbers/Account Numbers • Sex	
VBA Various Business Offices within VBA	Improvement of services being delivered to Veterans and creating efficiencies for employees delivering that service or supporting those services.	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Email Address • Emergency Contact Information • Military History/Service Connection • Medical Records • Next of Kin • Veteran Call History • Integrated Control Number (ICN) • Fax Number • Tax Identification Number (TIN) • Electronic data interchange personal identifier (EDIPI) • Financial Account Information • Debt- financial information • Beneficiary Profile Information • Health Insurance Beneficiary Numbers/Account Numbers • Sex	Secure File Transfer Protocol (SFTP)
VACO Various Business Offices within VACO	Improvement of services being delivered to Veterans and creating efficiencies for employees delivering that service or	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number(s) • Email Address	Secure File Transfer Protocol (SFTP)

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
	supporting those services.	• Emergency Contact Information • Military History/Service Connection • Medical Records • Next of Kin • Veteran Call History • Integrated Control Number (ICN) • Fax Number • Tax Identification Number (TIN) • Electronic data interchange personal identifier (EDIPI) • Financial Account Information • Debt- financial information • Beneficiary Profile Information • Health Insurance Beneficiary Numbers/Account Numbers • Sex	
Microsoft Azure Active Directory (Microsoft Entra)	The purpose is to utilize the PII for user authentication, ensuring secure access and verification of authorized individuals.	Name VA email address User ID	HTTPS/Port 443

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that information could be accessed by unauthorized individuals.

Mitigation: A defense-in-depth approach to protecting Employee PII, Veteran/dependent, and contractor data to include the following protection mechanisms: 1. The Application's loader API protected by a policy enforcement/policy decision point 2. VA hosts in MAG are protect by

FedRAMP High boundary protections at the hosting facility and only administrators have access to the administrative functions of the cloud services. 3. Data -at-rest encryption for any partition where PII will be contained 4. Data -in-transit encryption using TLS on any network traffic beyond the local enclave.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

			(can be more than one)	
Dogs for Life, West Palm Beach, FL	Eligibility and reporting	Name, Telephone number, Email address, Participation data (attendance, discharge reason)	MOU	Secure File Transfer Protocol (SFTP)
Puppies Assisting Wounded Servicemembers for Veterans (PAWS) for Purple Hearts, Anchorage, AK	Eligibility and reporting	Name, Telephone number, Email address, Participation data (attendance, discharge reason)	MOU	Secure File Transfer Protocol (SFTP)
Puppies Assisting Wounded Servicemembers for Veterans (PAWS) for Purple Hearts, San Antonio, TX	Eligibility and reporting	Name, Telephone number, Email address, Participation data (attendance, discharge reason)	MOU	Secure File Transfer Protocol (SFTP)
Warrior Canine Connection, Ashville, NC	Eligibility and reporting	Name, Telephone number, Email address, Participation data (attendance, discharge reason)	MOU	Secure File Transfer Protocol (SFTP)
Warrior Canine Connection, Palo Alto, CA	Eligibility and reporting	Name, Telephone number, Email address, Participation data (attendance, discharge reason)	MOU	Secure File Transfer Protocol (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.

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

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

Follow the format below:

Privacy Risk: There is a risk that information could be accessed by unauthorized individuals.

Mitigation: MAS -E takes a defense-in-depth approach to protecting Employee, Veteran and Dependent, and contractor PII data to include the following protection mechanisms: 1. The Application's loader API protected by a policy enforcement/policy decision point 2. VA hosts in MAG are protect by FedRAMP High boundary protections at the hosting facility and only administrators have access to the administrative functions of the cloud services. 3. Data -at-rest encryption for any partition where PII will be contained 4. Data -in-transit encryption using TLS on any network traffic beyond the local enclave.

Section 6. Notice

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

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

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

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

This system does not collect data from the individual, the PII/PHI data comes from the source system which provides notice to the individual. Awareness of this data collection is provided through the VA SORN in the Federal Register under "Consolidated Data Information System-VA", SOR # 97VA10, Federal Register Citation # 85 FR 84119, located at https://www.oprm.va.gov/docs/Current_SORN_List_08_17_2021.pdf. The Privacy Impact Assessment is also completed for all use cases of Microsoft Power Platform applications that process or store PII/PHI.

6.1b If notice was not provided, explain why.

The program office official records provide the notice

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

This system does not provide notice as it does not collect data from the individual, the PII/PHI data comes from the source system which provides notice to the individual. Each SORN provides the uses for the data collection in this system.

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.

No, MAS -E does not collect information directly from individuals, it only gathers pre-existing information located in various databases, reports, and repositories.

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.

No, MAS -E does not collect information directly from individuals, it only gathers pre-existing information located in various databases, reports, and repositories.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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

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

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

<u>Principle of Use Limitation:</u> The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must ensure that information is used only for the purpose articulated in the notice.
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

Follow the format below:

<u>Privacy Risk:</u> Source system of information data did not provide notice.
There is a risk that veterans and other members of the public will not know that the source system of information used by MAS -E exists or that it collects, maintains, and/or disseminates PII, PHI or PII/PHI about them.

Mitigation: Follow up with source and ensure notice provided.
This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP). Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

Section 7. Access, Redress, and Correction

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

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

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

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

Individuals requiring access to their information would be required to obtain that information from the original source. Individuals requesting access to records in MAS would submit a FOIA request. That FOIA request would be referred to the original data source for response.

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

This system is not exempt.

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?

This is a Privacy Act system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Go to source system to correct information identified through the SORN.
For Microsoft Azure Services, the individual will contact the source system of information as identified through the applicable SORN so the source system can provide specific steps on correcting information.

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.

Go to source system to correct information identified through the SORN.
Refer to list of SORNs in section 1.6 of this document. A link to VA Privacy Act System of Records Notices website is provided below.
https://department.va.gov/privacy/system-of-records-notices/

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.

Go to source system to correct information identified through the SORN.
The individual can contact the source system that collected the information as identified through the SORN. Additionally, they can contact VA Privacy Service at PrivacyService@va.gov or 202-273-5070.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information. There is also a risk that the source system has inaccurate records of an individual in the Official Record.

Mitigation: MAS -E mitigates the risk of incorrect information in an individual's records by authenticating information when possible, using the resources discussed in question 1.5. For information from a source system, MAS to provide individual whose information it was that is inaccurate with SORN and contact information or provide information for local privacy officer. To mitigate the risk of inaccurate records from the official risk, the individual would be provided with SORN and contact information or be given information for the local privacy officer.

Section 8. Technical Access and Security

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

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

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

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

Supervisor submits a yourIT ticket to the group managers and facilitates the provisioning/recreation/restoration of all new and returning user accounts as part of the on-boarding process based on submissions of User Access requests in the Service Catalog. The User Access workflow completes the creation of the Active Directory Account and Exchange Mailbox (email address). This group also manages any incidents related to status requests, escalations, or problems with accounts provisioned through the User Access workflow.

The workflow for User Access is as follows:

1. Area Manager provides approval.
2. ESD User Provisioning Team creates the Active Directory account, Share Drives, and Exchange Account.
3. Tier 2 Local Operations group completes any secondary tasks needed to complete account provisioning for the new hire.

The Area Manager Approval Task is assigned to the new user's local MGMT group, based on the location entered by the requester. Assigning the task to a group, instead of the individual Area Manager allows Area Managers and their designers to have access to view/approve the request without having to assign delegates.

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?

External entities have access through an authenticated external identity provider. Application owner establishes criteria.

No other government agencies have access to the system.

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

Non-IT personnel have access to this system such as:

Software Developers IT Software Developers
CIOs Executives, Senior Managers, CIOs and CFOs
Data Managers
IT Project Managers
IT Specialists
Network Administrators
System Administrators
Facilities Engineers
Human Resources Professionals
CIOs
VA employees
VA contractors

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

No for Business Associate Agreement. There is a non-disclosure agreement/confidentiality agreement.

8.2a. Will VA contractors have access to the system and the PII?

Yes, VA contractors have access to the system and the PII.

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractors are involved in the design, creation, and support of the Azure services. They all operate under NDAs, contractors with access to customer data and PII must sign additional contract addendums that ensure they understand and agree to Azure's privacy and data handling policies.

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.

All staff in an engineering role are required to take the annual training on standards of business conduct, which includes security, privacy, HIPPA, and VA Rules of Behavior.

Software Developers IT Software Developers- VA 1016925: Information Assurance for Software Developers IT Software Developers
CIOs Executives, Senior Managers, CIOs and CFOs - VA 3195: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
Data Managers - VA 1357084: Information Security Role-Based Training for Data Managers
IT Project Managers - VA 64899: Information Security Role-Based Training for IT Project Managers
IT Specialists - VA 3197: Information Security Role-Based Training for IT Specialists
Network Administrators - VA 1357083: Information Security Role-Based Training for Network Administrators
System Administrators - VA 1357076: Information Security Role-Based Training for System Administrators
Facilities Engineers - VA 1337064: Information Security for Facilities Engineers
Human Resources Professionals - VA 1016923: Information Security Role-Based Training for Human Resources Professionals
CIOs - VA 3193: Information Security for CIOs
VA employees - VA 10176: Privacy and Info Security Awareness and Rules of Behavior, VA 10203: Privacy and HIPAA Training, VA 3812493: Annual Government Ethics Role-based Training
VA contractors - VA 10176: Privacy and Info Security Awareness and Rules of Behavior, VA 10203: Privacy and HIPAA Training, VA 3812493: Annual Government Ethics Role-based Training

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status:* Complete
2. *The System Security Plan Status Date:* 03/28/2025
3. *The Authorization Status:* Authority to Operate (ATO)
4. *The Authorization Date:* 04/02/2024
5. *The Authorization Termination Date:* 04/02/2026

6. *The Risk Review Completion Date:* 03/11/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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 not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

Not applicable

Section 9 – Technology Usage

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

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

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

SaaS, Commercial cloud - Microsoft Azure Government/Microsoft Azure Public. The cloud is FedRAMP approved.

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

The Microsoft Azure Contract establishes VA ownership rights of all data including PII. The Contract Number is: 47QTCA22D003G; Task Order: 36C10B22F0089.

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.

MAS -E does not collect any ancillary data. All data used in Power Platform applications and within the MAG GCC environment is owned by VA.

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.

Microsoft Azure Services maintains compliance with all FedRAMP and VA security control requirements, to include all Privacy Overlay controls.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

No

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2025.04.15 12:52:23 -06'00'

Privacy Officer, Julie Drake

ALBERT COMPLE Digitally signed by ALBERT COMPLE
Date: 2025.04.15 12:00:22 -06'00'

Information Systems Security Officer, Albert Comple

RUSSELL HOLT Digitally signed by RUSSELL HOLT
Date: 2025.04.15 11:18:22 -06'00'

Information Systems Owner, Russell Holt

APPENDIX A-6.1

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

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

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