Privacy Impact Assessment for the VA IT System called:

Microsoft - Office 365 Multi-Tennant & Supporting Services Assessing

VACO (Includes Enterprise, OI&T)

OIT – Connectivity and Collaboration Service (CCS)

eMASS ID # 0079

Date PIA submitted for review:

08/12/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	OITPrivacy@va.gov Tonya.facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Albert Estacio	Albert.Estacio@va.gov	909-583-6309
Information System Owner	Jason Miller	Jason.Miller5@va.gov	630-421-2133

Abstract

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

The Department of Veteran's Affairs (VA) Microsoft (MS) Office 365 Multi-Tenant Software-as-a-Service enclave hosted in the FEDRAMP Government Azure Cloud herein referred to as "M0365." M0365 provides a means for the Department of Veteran's Affairs (VA) employees to create/send/receive electronic mail (email) messages, internal calendars, internal Instant Messages (IMs)/chats, use internal portals between VA employees (government and contractors) and approved internal protection on VA endpoints using globally enforced multi factor authentication for initial enterprise network accessibility and identification using FIPS compliant devices: smartcards, VA Personal Identification Verification (PIV) cards with active Public Key Infrastructure (PKI) security encryption certificates encoded or derived (PIV-D). Encrypted email by VA end users is a sub-function of the Exchange/Outlook client from M0365 enclave using a separate VA Information System known as PIV or derived credentials.

Projects hosted in the Cloud and as defined by NIST is a modernization technology model for enabling convenient, on-demand enterprise network access to a shared pool of configurable mission essential computing resources (e.g., networks, servers, storage, applications, and services) which can be rapidly provisioned and released with minimal management effort by the Agency or Cloud provider interaction. Further, as defined within NIST SP 800-145 (NIST Definition of Cloud Computing), the service model for the VA M0365 enclave is Software-as-a-Service (SaaS). This is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service with data stored in the Cloud. The main purpose is to reduce the total cost of hardware and software development, maintenance, and operations with the security provisions carried out mainly by the hosting Cloud Service Provider.

Overview

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

1 General Description

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

Microsoft - Office 365 Multi-Tennant & Supporting Services Assessing; OIT – Connectivity and Collaboration Service (CCS)

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

The purpose is to support VA internal communications for over 650,000 employees with a projected increase of 145,000 endpoints due to the COVID pandemic in 2020. M0365 is the modernization technology solution to facilitate communications for end users within the VA toother VA end users internally and to external persons via transmitted email. The end user mailboxes from the legacy VA email system was migrated to M0365 and are stored in the Cloud. Microsoft (MS) provides encryption protection of M0365 data at rest.

C. *Who is the owner or control of the IT system or project?*
VA Controlled / non-VA Owned and Operated

2. Information Collection and Sharing

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

The system stores VA internal communications for over 650,000 VA employees and contractors.

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

MO365MT collects and uses names and contact information of VA users and other individuals who communicate with VA users via email messages (including any attachments) which may contain a variety of information. The information potentially could include PII about VA employees and VA contractors such as but not limited to SSN, date of birth, personal address, personal email, personal telephone. These elements fall outside of the scope, recommended usage and VA Policies applying of Microsoft 365 Applications, however there is potential for such data elements to be transmitted.

MO365MT Applications:

- SharePoint Online - SharePoint Online is a cloud-based service that provides a secure and collaborative platform for managing and sharing content, data, and applications within an organization.
- OneDrive - OneDrive is a cloud storage service that allows users to store, access, and share files securely an internet connection.
- Teams - Microsoft Teams is a comprehensive collaboration platform that offers chat, messaging, meetings and calling.
- Exchange Online - Exchange Online is a cloud-based email and calendaring service
- M365 Applications
    - Microsoft Bookings - Microsoft Bookings is a scheduling and appointment management tool
    - MS Planner - Microsoft Planner is a planning and task management application
    - MS Shifts - Microsoft Shifts is a scheduling and workforce management tool
    - MS Stream - Microsoft Stream is a video management and sharing service
    - MS Forms - Microsoft Forms is an online survey and quiz creation tool
    - MS Power Automate - Microsoft Power Automate is a cloud-based workflow automation platform
    - MS Viva Insights - Microsoft Viva Insights is a tool that is designed to help improve employee well-being and productivity
    - MS Lists - Microsoft Lists is a tool that helps users track information and organize work
    - MS Todo - Microsoft To-Do is a cloud-based task management and to-do list application
    - MS OneNote - Microsoft OneNote is a digital note-taking and organization application
    - MS Whiteboard - Microsoft Whiteboard is a digital whiteboard and collaboration tool
    - MS Contacts – Microsoft Contacts is a contacts organization tool
    - MS Visio - Microsoft Visio is a diagramming and visualization software tool
    - MS Power Pages - Microsoft Power Pages is a website builder and hosting platform

- MS Outlook (Online App) - Microsoft Outlook Online is the web-based version of the Microsoft Outlook email and personal information management application
- MS Word (Online App) - Microsoft Word Online is the web-based version of the Microsoft Word word processing application
- MS Excel (Online App) - Microsoft Excel Online is the web-based version of the Microsoft Excel spreadsheet application.
- MS Teams (Online App) - Microsoft Teams Online is the web-based version of the Microsoft Teams application.
- MS Power Point (Online App) - Microsoft PowerPoint Online is the web-based version of the Microsoft PowerPoint presentation software.
- MS Project (Online App) - Microsoft Project Online is the web-based version of the Microsoft Project portfolio management software.

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

MO365MT enclave at VA includes: work email, electronic calendars, and instant message communication. PKI is used for identification, digital signature, and encryption as a sub-function from a separate VA internal Information System known as VACO Personal Identification Verification (PIV). MO365MT is sponsored by the ITOPS Enterprise Messaging and Collaboration Solution Delivery organization.

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

VA MO365 is hosted in the FedRAMP Government Azure Cloud.

3. Legal Authority and SORN

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

Federal agencies are required to manage their email records in accordance with the Federal Records Act (44 U.S.C. Chapter 31) and 36 Code of Federal Regulation (CFR) Chapter XII Sub- chapter B. There is no specific legal authority that authorizes the use of email, chats, or M0365. VA security policies and procedures surrounding the support of the email software and hardware include the VA Handbook 6500; OMB CIRCULAR No. A-130, "Management of Federal Information Resources;" National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, "Risk Management Guide for Information Technology System."

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?

There are no SORNS applicable to this system.

4. System Changes

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

Completion of this PIA will not result in circumstances that require changes to business process.

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

Completion of this PIA will not result in technology changes.

Section 1. Characterization of the Information

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

1.1 What information is collected, used, disseminated, created, or maintained in the system?

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Information
☒ Health Insurance Beneficiary Numbers Account numbers
☒ Certificate/License numbers[1]
☒ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☒ Gender
☒ Integrated Control Number (ICN)

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

☒Military History/Service Connection
☒ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Other Data associated with VA work location, work phone number, VA work email and employee name on a smartcard.
In order to support the services requested by the VA, systems/modernization technology solutions such as M0365 collects information directly from VA AD to allow end users (VA employees) to authenticate and communicate via email, chats, internal portals. VA email is used solely to facilitate communications between users within VA to others internal and external to the VA. These emails can include any type of information, including PII data points, in their body. PII data elements within the body of an email can be sent from any person outside of the VA-to-VA users in both encrypted and/or unencrypted formats. It is impossible for the VA to manage or prevent all members from the public from sending PII or Sensitive Personal Information (SPI) to VA email accounts.

PII Mapping of Components (Servers/Database)

VA MO365 enclave consists of **five** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **MO365** 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.

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

• SharePoint Online
• OneDrive
• Teams
• Exchange Online
• M365 Applications
  ○ Microsoft Bookings
  ○ MS Planner
  ○ MS Shifts
  ○ MS Stream
  ○ MS Forms
  ○ MS Power Automate
	Yes – only Business	**No**	Name, Social Security number, Date of Birth, Mother's maiden Name, Personal Phone Number, Personal Fax Number, Personal Email Address, Emergency Contact Information, Financial Information, Health Insurance Beneficiary Numbers Account	VA Employees with smartcards (VA PIV cards) or derived certificates (certs) to send/receive and transmit encrypted email	Globally Enforced Multi Factor User Authentication (Active PKI certs on smartcards or derived certs)

○ MS Viva Insights ○ MS Lists ○ MS Todo ○ MS OneNote ○ MS Whiteboard ○ MS Contacts ○ MS Visio ○ MS Power Pages ○ MS Outlook (Online App) ○ MS Word (Online App) ○ MS Excel (Online App) ○ MS Teams (Online App) ○ MS Power Point (Online App) ○ MS Project (Online App)			Numbers, Certificate/License Number, Vehicle License Plate Number, Internet License Plate Number, Internet Protocol (IP) Address Number, Medications, Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integrated Control Number (ICN), Military History/Service Connection, Next of Kin.		

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 sources of information in VA M0365 are from the VA AD and VACO PIV Information Systems and Authority to Operate (ATO) projects for VA employees (Government and Contractors) which includes basic data: employee name, work location, work phone number, work email address.

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 business information is used to create end user and VA email accounts to access the VA enterprise network and access M0365software applications.

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

The system does not create information such as score, analysis or report.

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?

Basic employee data is collected during the VA initial on boarding process for a smartcard, network and email accounts; for example, through VA End User Operations (EUO) and/or VA Active Directory Federated Services (ADFS) to provide the services agreed to for the VA employees. Generally, Teams with elevated permissions will collect the necessary information from new VA employees (Government or Contractors) to create end user accounts. Requests for changes or updates to end user accounts (network, email, security groups) are submitted to the VA Service Desk managed work ticket 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?

No information is ever obtained or collected on a form and therefore not subjected to the Paperwork Reduction Act.

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.

Initial information that the VA M0365 enclave receives on a VA employee is presumed to be accurate; however, when an end user is assigned a VA network and email account, an email notification is sent to the user's VA work email address. The end user may then review their information in the VA Global Address List (GAL) and submit necessary change requests via the internal VA Service Now work ticket system.

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?

Due to its nature, the information shared with the VA in emails or other components of the system are not checked for accuracy.

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

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any 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

There is no specific legal authority which authorizes the use of email, internal chat or portals provided by M0365 enclave hosted in the Cloud. VA M0365 is a basic enterprise infrastructure software service within the VA. The VA security policies and procedures surrounding the support of the work email software and hardware, usage, etc. includes the VA Handbook 6500; OMB CIRCULAR No. A-130,"Management of Federal Information Resources"; National Institute of Standards and Technology (NIST)Special Publication (SP) 800-30, "Risk Management Guide for Information Technology System."

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:

<u>Principle of Purpose Specification:</u> 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: Although users are instructed not to send sensitive information in the clear, Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) contained in emails could be accessed by unauthorized users if the users do not encrypt their email.

Mitigation: Only authorized VA email users have access to the system.
Information collected on the VA email system may include (but not be limited to) full names, e -mail addresses and business addresses. The actual information collected will be from all fields held within the VA Active Directory system that is used to synchronize data with the Exchange 2010 and M0365systems; therefore, the above fields are just examples. The information for VA personnel will be protected using all moderate impact security controls required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3 for compliance with FISMA. The Exchange 2010system is currently undergoing the security authorization and approval process.

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	To allow end users to authenticate	Not used
Social Security Number	Not used	Not used
Date of Birth	Not used	Not used
Mother's Maiden Name	Not used	Not used

Personal Mailing Address	Not used	Not used
Personal Phone Number(s)	Not used	Not used
Personal Fax Number	Not used	Not used
Personal Email Address	Not used	Not used
Emergency Contact Information (Name, Phone Number, etc. of a different individual)	Not used	Not used
Financial Information	Not used	Not used
Health Insurance Beneficiary Numbers Account numbers	Not used	Not used
Certificate/License numbers[2]	Not used	Not used
Vehicle License Plate Number	Not used	Not used
Internet Protocol (IP) Address Numbers	Not used	Not used
Medications	Not used	Not used
Medical Records	Not used	Not used
Race/Ethnicity	Not used	Not used
Tax Identification Number	Not used	Not used
Medical Record Number	Not used	Not used
Gender	Not used	Not used
Integrated Control Number (ICN)	Not used	Not used
Military History/Service Connection	Not used	Not used
Next of Kin	Not used	Not used
VA Work email	To allow end users to authenticate	Not used

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

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

The MO365 multi-tenant system does not perform any data analysis or and data creation.

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

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.

The information officially collected by the VA M0365 enclave is used solely to contact individuals within the VA. As such there is no need to analyze or manipulate this 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?

The MO365 Multi-tenant system utilizes Azure Information Protection (AIP) data loss prevention policies that are VA implemented to protect both the potential of inadvertently sent protected data and protected data at rest. The system also uses end-to-end encryption policies to protect data in transit.

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

The system doesn't collect, process, or retain social security numbers. MO365MT protects SSN data with Data Loss Prevention (DLP) policies. Additionally, all data is encrypted at rest in transit.

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

The system doesn't collect, process, or retain social security numbers. MO365MT protects PII/PHI data with Data Loss Prevention (DLP) policies. Additionally, all data is encrypted at rest in transit.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to PII that is available on the admin console is only granted to individuals who are technical system administrators for the MO365 multi-tenant system. Access to other available PII may be present during basic utilization of the system tools.

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

The active management of VA network and email accounts by End User Operations annually on regular end users and quarterly on end user accounts with elevated permissions in accordance with VA Handbook 6500 enables the VA to remove personnel who no longer require access. VA account management features provide additional security including the ability to change passwords or re-create accounts if needed for security reasons. This ensures unauthorized access to internal data is a low risk. The VA also requires employees (Government and Contractors) to read and sign the VA Rules of Behavior (ROB) before access is granted to the VA network or email accounts.

2.4c Does access require manager approval?

Yes

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

Yes

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

MO365 Multi-tenant technical system administrators

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

The information listed in question 1.1 is retained by the VA M0365 enclave in order to populate the VA email Global Address List (GAL) and maintain user accounts for example in the VA Active Directory (AD) Services Information system for network access. Identification and nonrepudiation. Data point examples:

• Employee Name

• VA Zip Code
• VA Phone Number(s)
• VA Fax Number
• VA Email Address
In addition to basic employee work data obtained electronically from the VA Active Directory Services Information System; M0365 data hosted and stored in the FEDRAMP Azure Cloud also includes VA mailboxes, chats and SharePoint. Generally, the VA M0365 enclave data retention timeline is 7 years; however, variances or specific information on the SaaS applications includes:
• SharePoint Online (SPO)Data retention policies for SharePoint Online (SPO) as part of VA M0365 are managed by the Data/Content owner. Files stored on SPO; e.g.; recorded meetings are stored in Stream, and connected Apps such as Forms, PowerApps, and Flows are retained based on the business need which is determined by the Data/Content Owner or Developer.
Reference: the SharePoint Online Governance Plan for the VA from Microsoft is located at:https://dvagov.sharepoint.com/:w:/r/sites/spo/_layouts/15/guestaccess.aspx?share=EXCYz_ySoIRKsmBRjvG2R3UBJ7xvZ49bUQwGMP0Phkf69Q
• OneDrive - VA employee (Government and Contractor) personal data files stored on One Drive fall under the same governance situation as VA employee personal files and chats: the employee is the Data Owner/Content Owner of stored personal data.
• MS TEAMS - Data retention is only for internal Instant Messages (chats) on MS TEAMS. Microsoft will release the capability in the future for end users to delete their chats. If a chat is deleted; any attachments to that chat will also be deleted. TEAMS is internal only; attachments in chats cannot be forwarded externally from within TEAMS.
• Legacy Email - The VA tape storage contract will expire September 25, 2021 on the legacy VA Exchange 2003/2007 data/mailboxes. Data retention on the legacy email tapes date back to 2011 and are part of the Exchange 2010 ATO project sponsored by Solution Delivery (SD). The ISO for the Exchange 2010 project is also the ISO for the VA M0365 enclave.
• Email/Mailboxes in the FEDRAMP Government Azure Cloud – Data retention is 7 years.
• Clearing/Purging/Disposal - for VA on-premise devices which are being decommissioned the VA OIT ITOPS IO SP PLM group is responsible and managing disposal as part of the overall migration project. Their email address is: OIT-ITOPS-IO-SP-PLM@va.gov The FEDRAMP Government Cloud Service Provider is responsible for the purging and disposal of the M0365 Azure online devices.
Additionally, Federal agencies are required to manage their email records in accordance with the Federal Records Act (44 U.S.C. Chapter 31) and 36 Code of Federal Regulation (CFR)Chapter XII Sub-chapter B. The Email Archiving System automatically archives emails sent to and from authorized VA users. This means that any information contained within the email is also retained.

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.*

Access control records: OIT Record Control Schedule: OIT 005-1 Part I, Section P, item 6, User Identification, Profiles, Authorizations, and Password Files Destroy/delete inactive file. 6 years after user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.
General Non-Capstone, General Record Schedule, section 6.5 item 011: Temporary. Delete when 7 years old, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS 2022-0006- 0002.
General Support and/or administrative positions, General Record Schedule, section 6.5 item 012: Temporary. Delete when 3 years old, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS 2022-0006 0003Capstone, General Record Schedule, section 6.5 item 010: Permanent. Cutoff and transfer in accordance with the agency's approved NA 1005, Verification for Implementing GRS 6.1. This will be between 15 and 30 years, or after declassification review (when applicable), whichever is later. Disposition Authority: DAA-GRS 2022-0006 0001

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?

Information stored in the Cloud for M0365 is subject to VA Office of Information & Technology (OI&T).

3.3b Please indicate each records retention schedule, series, and disposition authority?
Records Control Schedule (RCS) 005-1, Section C, Item 7 as well as the NARA General Records Schedule 20, item 14, Electronic Mail Records. https://www.archives.gov/records-mgmt/grs.html

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.

Archived email in the VA legacy email system is on back up tapes which currently have unlimited retention policies therefore VA archived emails will not be deleted until there is a VA policy change or FEDRAMP change on data retention. Data destruction and disposal of M0365data stored in the Cloud other than mailboxes is through the FEDRAMP Cloud Service Provider; for example, the deletion of an end user account will delete the user calendar and chats.

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.

The M0365 enclave does not use PII for testing, research, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the archived VA emails may need to be retained longer than 7 years or as required by law. Records, especially those containing Personally Identifiable Information (PII) or Sensitive Personal Information (SPI) that are held longer than required are at a greater risk of unauthorized access or breach, increasing the risk that an individual's information may be accessed by individuals without reasonable need to know.

Mitigation: VA M0365 information is only kept for as long as required by VA Office of Information &Technology (OI&T), Records Control Schedule (RCS) 005-1, Section C, Item 7 unless directed to retain email accounts beyond 7 years; the archived VA emails are disposed of following the procedures discussed in 3.4. Only VA Team members with approved elevated permissions in accordance with VA Handbook 6500 have access to archived emails to decrypt emails for official investigations as requested.

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?

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***
VA Active Directory/ Entra ID	VA Active Directory Services System	Employee Name, Work Location, Work Phone Number, Work Electronic Mail (Email) Address.	End user list of VA employees and groups transmitted by VA AD DCs and received by MO365. Transmission protocol is TLS 1.2.

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: MO365MT collects and uses names and contact information of VA users and other individuals who communicate with VA users via email messages (including any attachments) which **may** contain a variety of information. The information **potentially** could include PII about Veterans/Dependents, VA employees, VA contractors/Members of the Public, and Clinical Trainees. These elements fall outside of the scope, recommended usage and VA Policies applying of Microsoft 365 Applications, however there is potential for such data elements to be transmitted.

Mitigation: VA internal and gateway network firewalls, "routing traffic cops" to prevent packets in or out from the VA AD forwarding agent from the Exchange server connectors using Simple Mail Transfer protocol (SMTP).

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.

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

The information stored in the FEDRAMP Azure Cloud for the VA M0365 enclave that is received from the VA AD Information System on VA employees includes business contact information within the Global Address List (GAL) for internal purposes only and not routinely shared with any agency or organization outside of the VA. However, as emails stored within the system are considered electronic public records, they may be searched for relevant information in the event of a Freedom of Information Act (FOIA) request or as part of the discovery process in a legal case the VA is a part of. In the event that information is shared outside of the VA, it will be pursuant to a FOIA request or discover in a legal case. All FOIA requests are governed by The Freedom of Information Act, 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048. Any disclosures made in relation to a legal case are governed by the Federal Rules of Civil Procedure (Fed. R. Civ. P.) 26-37.

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	

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 no external sharing.

Mitigation: There is no external sharing.

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 was provided to VA employees during initial orientation and onboarding processes. (https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=487&FType=2). (Appendix A-2).

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

Notice was provided. (https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=487&FType=2).

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.

For information officially collected for the creation of a user account, notice is provided prior to the new account request being processed, although the exact mechanism may be slightly different for each government client. VA form 9957 is required to be signed, approved, and submitted for role-based access with enforced multi factor authentication. Initial required training and follow up required annual training for users; active smartcard (VA PIV card and PKI certifications hard coded on the smartcard or derived certificates) for email access are provided knowledge from the VA Training Management

Systems (TMS) via training scenarios; for example, users who are provided information to the VA through unsolicited emails with potential PII or SPI in email messages who do not receive notice prior to the "collection" of the information should notify their management and local Information System Security Officer (ISSO) and use approved encryption technology (VA PIV card/smartcard/derived certificates) to safeguard the data prior to responding. In instances where a user is providing requested information for another program or system, such as through a VA form submitted via email, notice of the information collection is delivered via that program. This PIA does serve as notice that the VA M0365 enclave collects or retains VA emails which may contain Personally Identifiable Information (PII) or other Sensitive Personal Information (SPI).

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.

Yes, individuals have the opportunity and right to decline. If so; denial of service is no access to the VA enterprise network and email. The only information officially collected and solicited as part of the VA M0365 enclave is VA staff name and business contact information (VA office address and VA provided phone number(s)). This information is required in order to create a VA email account. As such, VA staff are not able to decline to provide this information.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

The information officially collected by the VA AD system for the VA M0365 enclave is only business contact information for VA staff and contractors. VA staff and users are not given the opportunity to consent to particular uses of their VA business contact information.

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 System ISSO 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> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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: There is a risk that VA employees and contractors are not aware that their business contact information is collected and used to create a user account and a Global Address List (GAL) record about the employee.

Mitigation: The end user is notified when their information is initially collected using approved VA Forms during onboarding for example VA 9957 Access form in this PIA at Appendix A-2.

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.***

O365 uses a combination of conditional access policies and role-based access to control and limit access to information.

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)?

O365 is not exempt from the access provisions of the Privacy Act.

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

Business contact information is available internally for VA employees (Government and Contractor) to review using enforced multi factor authentication via smartcards (VA PIV cards, PIV-D derived credentials) through a Global Address List (GAL) maintained by the VA. End users may view their information by going into Exchange/Outlook software in the VA M0365 enclave and selecting the "Search Address Book" icon and entering their name with their last name first. Once located, the end user must double click on his/her VA Active Directory listing and their basic VA work data will appear.

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.

If the VA user's name, VA phone number, or VA email address with the GAL is incorrect they can notify the VA Help Desk and request the information be corrected. At the present time the user does not have the ability to update/correct their data directly; however, this feature may be available in the future. Please note: the VA M0365 enclave which includes work email, internal chat and portal software applications are not official systems of record. The VA M0365 enclave does not maintain, or store records related to members of the public. As there are no records on Veterans or members of the public, there are not any records for an individual to request redress.

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.

VA employees (Government and Contractor) are sent an email notification when their VA network and email accounts are created. The work email informs them that their information is available and to contact the VA ServiceNow work ticket system for any discrepancies. Please note: the VA M0365 enclave hosted in the Cloud and end user mailboxes are not an official system of record; M0365 does not maintain records related to members of the public. As there are no records on Veterans or members of the public, there are not any records for an individual to request redress.

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.

Currently end users must contact the VA ServiceNow work ticket system to update their email information in the GAL. The VA is working to institute a process by which an end user can directly update their basic work data after onboarding that is displayed in the GAL. The VA is also working with Microsoft in the future for end users to have the ability to delete chats in the MS TEAMS software application which is part of the VA M0365 enclave. Please note: the VA M0365 enclave is not a system of record and does not maintain records related to members of the public. As there are no records on Veterans or members of the public, there are not any records for an individual to request redress.

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: The privacy risk to the VA is minimal, as no formal record about the users is maintained by O365. Unauthorized access to data poses risks, including potential breaches of confidential information and damage to organizational reputation.

Mitigation: The end user (VA employee) is notified when their information is initially collected for the VA AD Information System when using VA Form 9957 during the VA initial onboarding process.

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?

The VA End User Operations (EUO) group in conjunction with the approval of the requesting employee's supervisor verifies identity and training requirement completion of the requesting employee and approves access to the VA enterprise networks and email. EUO conducts reviews of user access requests, including identification, to ensure compliance with information security requirements in VA

Handbook 6500; NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems; and the Information Security Reference Guide. EPAS approvals are reviewed quarterly.

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?

There is no access to the MO365 multi-tenant system granted to other agencies and therefore no users from outside 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.

Verification for end users with elevated permission is accomplished by documented access control forms and an automated process known as EPAS. Requesting employees for elevated access requires confirmed completion of VA required training classes which include Privacy, Information Security and Rules of Behavior. Background investigation must also be submitted and completed and/or renewed based on current terms of service and sensitivity level of the position on all VA employees (Government and Contractor).

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.

Yes, if they have an approve and active VA network and email account with enforced multi factor authentication; smartcard (VA PIV card or PIV-D. derived credentials). Clearance is required for Contractors as if they were VA Government employees.

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.

The Rules of Behavior (ROB) training is a mandatory requirement. Training is provided and confirmed employee signed ROB before access is granted to a VA network and email account. Annual Government Ethics and Privacy & HIPAA Training is also required of all end users.

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:* 04/08/2024
3. *The Authorization Status:* Authorized to operate (ATO)
4. *The Authorization Date:* 04/08/2024
5. *The Authorization Termination Date:* 04/08/2026
6. *The Risk Review Completion Date:* 04/08/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Authorization and Accreditation has been completed for this system.

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.

Private, Software as a Service (SaaS) provided by Microsoft.

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.*

Dynamic 365 Customer Service, Enterprise Edition for Government - Microsoft Dynamics 365 Customer Voice for Customer Service Enterprise for GCC Power Apps for Dynamics 365 for Government Power Automate for Dynamics 365 for Government SharePoint Plan 2GProject Online Essentials for Government Office for the Web for Government Exchange Foundation for Government Dynamics 365

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.

The CSP does not collect any ancillary data.

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.

The CSP provides security and privacy tools to be utilized and configured by the VA.

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.

TONYA FACEMIRE

Digitally signed by TONYA FACEMIRE
Date: 2024.10.04 12:07:39 -04'00'

Privacy Officer, Tonya Facemire

ALBERTINO ESTACIO

Digitally signed by ALBERTINO ESTACIO
Date: 2024.10.03 13:49:43 -07'00'

Information Systems Security Officer, Albert Estacio

JASON MILLER

Digitally signed by JASON MILLER
Date: 2024.09.24 12:03:55 -05'00'

Information Systems Owner, Jason Miller

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).

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

HELPFUL LINKS:

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices