Privacy Impact Assessment for the VA IT System called:

Microsoft Entra ID -E

Enterprise Cloud Solutions Office (ECSO)

eMASS ID #2628

PIA submitted for review:

03/24/2025

System Contacts:

System Contacts

Title	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.facemire@va.gov OITPrivacy@va.gov	202-632-8423
Information System Security Officer	Albert Estacio	Albert.estacio@va.gov	909-528-4958
Information System Owner	Christopher Cardella	Christopher.cardella@va.gov	512-590-9414

Abstract

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

Microsoft Entra ID (previously called Azure Active Directory (Azure AD)) is Microsoft's multi-tenant, cloud-based directory, and identity management service. Entra ID combines core directory services, advanced identity governance, and application access management. Entra ID also offers a rich, standards-based platform that enables developers to deliver access control to their applications, based on centralized policy and rules. Microsoft Entra ID Premium edition adds feature-rich enterprise-level identity management capabilities and enables hybrid users to seamlessly access on-premises and cloud capabilities.

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?

Entra ID is a Microsoft service that serves as a central identity and access management solution, allowing businesses to securely manage employee identities, control access to applications and data across various platforms, and enforce strong authentication methods to protect sensitive information within their organization.

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 Entra ID is VA Controlled/non-VA Owned and Operated

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?

Approximately 850,000 VA employees (Government and Contractors) are the expected resource objects stored in Microsoft Entra ID. The VA business PII data Microsoft Entra ID uses on individuals is: Name, Personal Mailing Address, Work Mailing Address Personal Phone Number(s), Work Phone Number(s) and Business Email Address.

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?

Name, Work/Personal Address, Work/Personal Telephone Number, Work Electronic Mail (Email) Address. The data is for the purposes of allowing identification and globally enforced authentication on VA resources to initially access the VA network.

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

The data is for the purposes of allowing identification and globally enforced authentication on VA resources to initially access the VA network.

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

There is sharing of Microsoft Entra ID data.

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?

Entra ID is installed in a cloud environment.

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

H. What is the citation of the legal authority?

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301; 38 U.S.C. 501; 40 U.S.C. 11331; 44 U.S.C 3544; Executive Order 9397; Homeland Security Presidential Directive 12; Federal Information Processing Standard 201–1
https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf

I. What is the SORN?

146VA005Q3 / 73 FR 16093, Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008)

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

The SORN does not require revision.

4. System Changes

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

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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:
• Business Phone number
• Username

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?

Information is collected from the Individual during the onboarding process.

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

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.

Information for this system is not collected from sources other than the individual

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

No

1.3 Methods of information collection

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?

Information is synchronized from VA Active Directory

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?

The Entra ID does not collect PII data on 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.

Entra ID data is synchronized from Active Directory.

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?

No the system does not check for accuracy

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

SORN and Federal Privacy laws associated with HSPD-12 guidelines requiring PIV smartcards, and OPM processes for hiring employees are examples of federal authorization for collecting PII business data on VA employees during initial onboarding processes.
Laws and Regulations: Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law, United States Code, and Homeland Security Presidential Directives.

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: Unauthorized individuals gain access to user information.

Mitigation: Multi factor authentication with required Public Key Infrastructure (PKI) hard coded or derived encryption certificates on elevated permission accounts are globally enforced via enterprise security groups and GPOs.

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	File Identification purposes	Not used
Personal Mailing Address	File Identification purposes	Not used
Work Mailing Address	File Identification purposes	Not used
Personal Phone Number(s)	File Identification purposes	Not used
Work Phone Number(s)	File Identification purposes	Not used
Business Email Address	File Identification purposes	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?

The information officially collected for the Entra ID accounts is used solely to identify basic business data on VA employees, security groups, service accounts and devices approved for initial access to the VA network. As such there is no need to analyze or manipulate this data. Automated or ad-hoc reports gather account information for

responsible parties. This information is processed and formatted to produce access control reports. Various statistical data is reviewed to maintain accuracy and maintenance of accounts in Entra ID.

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.

Entra ID does not create duplicate accounts on individual users (VA employees). Entra ID does not make available new or previously unutilized information or create newly derived data on 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?

Encryption of data, controlled access through Just in Time (JIT), logical isolation between each account, and logging of access

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).

Entra ID does not process or retain SSNs.

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

Microsoft Entra ID employs multiple layers of encryption to secure data both at rest and in transit. Data stored within Microsoft's cloud services is protected using strong encryption protocols such as BitLocker, TLS, and AES. These technologies ensure that data remains confidential and secure against unauthorized access.

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

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

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

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

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

2.4a How is access to the PII determined?

During VA onboarding processes for employees when PIV card is issued and accounts created. Administrative access is granted via the VA's Non-eMail Enabled Account (NMEA - 0 account) request process. The VA requires manager approval on NMEA requests, processed through ePAS.

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?

Yes. Reference: VA Account Management Standard Operating Procedure (SOP) and Global Security Groups (GPOs) during onboarding processes on employees.

2.4c Does access require manager approval?

Yes

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

Administrative access is granted via the VA's Non-eMail Enabled Account (NMEA - 0 account) request process. The VA requires manager approval on NMEA requests, processed through ePAS.

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

VA and VA employees are responsible for assuring safeguards for the PII.

Section 3. Retention of Information

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

3.1 What information is retained?

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

Name
Personal Mailing Address
Work Mailing Address
Personal Phone Number(s)
Work Phone Number(s)
Business Email Address

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.

Basic PII user data on VA employees is retained and stored in Entra ID for as long as the user has approved access for the VA enterprise network and is a VA employee. If a user leaves the VA or no longer requires access; the VA Service Line/Facility Teams are required to disable and remove the account. Global group policies deactivate accounts which are inactive greater than 90 days. Entra ID data is only maintained for the duration of time that an individual is a Federal employee, contractor, or other partner requiring initial access to the VA network with enforced multi-factor smartcards (VA PIV cards).

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?

Entra ID as designed and implemented for the VA does not allow dormant/inactive accounts to linger indefinitely after an employee leaves VA; it would be a security risk. There is no retention schedule for Entra ID data.

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

There is no records retention, series, and disposition authority on a deleted account. In accordance with HSPD–12, PIV Cards are deactivated within 18 hours from the notification time for cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by shredding, typically within 90 days after deactivation.

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.

Entra ID is synchronized with Active Directory. When a record is removed in Active Directory it is also removed from Entra ID. Logical access to the data is removed and eventually overwritten when the sectors on the physical storage media are recycled.

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.

Entra ID does not use collected PII data on employees 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 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 information could be stored for longer than necessary.

Mitigation: Entra ID is synchronized with Active Directory. When a record is removed in Active Directory it is also removed from Entra ID. Logical access to the data is removed and eventually overwritten when the sectors on the physical storage media are recycled.

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 <**Information System Name**> consists of <**number**> 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 <**Information System Name**> 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 Entra ID SaaS	Yes	Yes	Name, Personal and Business Address, Personal and Business phone number.	User Authentication	LDAP Protocol. Shared data electronically transmitted.

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***
VA Microsoft Active Directory (AD) Service Database	Synchronization with Entra ID for User ID and Authentication	Name, Work/Personal Address, Work/Personal telephone number, Work/Personal email address	LDAP Protocol. Shared data electronically transmitted.

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: Sharing of VA information increases the potential of an exposure.

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

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 (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: There is no external sharing of Microsoft Entra data.

Mitigation: There is no external sharing of Microsoft Entra data.

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.

No privacy notice is given because the system is syncing with active directory without user interface. No information is input by the user.

6.1b If notice was not provided, explain why.

System is syncing with active directory without user interface

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

No privacy notice is given because the system is syncing with active directory without user interface. No information is input by the user.

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.

Users can not decline to register as the information is synced from Active Directory.

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.

Entra ID does not provide a means for consent. Basic business PII data collected on VA employees for Entra ID is mandatory to comply with identification and authentication to initially access the VA Network. Right to consent examples from other processes: VA Banner, employee signed forms through HR, COR, VA PIV Smartcard Sponsor.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your 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:

Principle of Transparency: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: 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:

Privacy Risk: There is a risk that collected/stored information on user accounts in Entra ID could be accessed by someone with elevated permissions who does not have a need to know.

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

Section 7. Access, Redress, and Correction

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

7.1 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.***

VA procedures are the Service Now (SNOW) work ticket process and/or application known as YourIT for employees to gain access to their information or make changes.

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)?

No exemption.

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?

VA employees with VA PIV smartcard or PIV-Derived (PIV-D) credentials can query their own information for inaccuracies or updates. A work ticket through ServiceNow or YourIT can be submitted by the employee, local ISSO, HR, COR, Manager or the PIV Sponsor to correct VA owned information as needed on the user. VA required annual Privacy training classes in the Training Management System (TMS) for all employees provides links/contacts. VA procedures in place that allow access to information includes 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ for information about FOIA points of contact and information about agency FOIA processes.

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.

VA employees can request changes to correct inaccurate or erroneous information via the ServiceNow (SNOW) work ticket or YourIT process.

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.

Bulletins, emails, internal portals, and shortcuts on VA government furnished equipment notifies individuals to submit Service Now (SNOW) tickets directly via YourIT or provide the phone number or email to contact the VA Help Desk to correct information on PII data for their employee name, work location/address, work phone and work email address in Entra ID.

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.

Redress can also be accomplished for the employee by contacting their Manager, HR or ISSO. Authenticated users of Entra ID can query their own information for inaccuracies or updates. A work ticket through ServiceNow or YourIT can be submitted to correct VA owned information. Please note: Entra ID is not an official system of record. Entra ID does not maintain records related to members of the public. As there are no medical records on Veterans or members of the public in Entra ID, and there are no 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 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 stored user information in Entra ID could be accessed by a Hacker; however, if access is attempted by a non-authorized user; an "Access Denied" alert is sent automatically to the requestor, ISO, Entra ID Team and VA-CSOC.

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

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?

Documented in place procedure examples determine which users may access the system includes: VA Account Management Standard Operating Procedure (SOP) and globally enforced security groups (GPOs).

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?

Users from other agencies do not have access to VA Entra ID.

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.

The Entra ID ISO in conjunction with the approval of the requesting employee's Supervisor/Facility CIO verifies identity and training requirement completion of the requesting employee to approve elevated permission access accounts to access the VA System servers. Verification is accomplished by documented access control forms or by automated process using ePAS. Requesting employees must have confirmed completion of VA required training to 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. ISO, Supervisors, ISSO, OIS conduct quarterly reviews of user access requests for NMEA, 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. All users must be Federal employees, contractors, or authorized partners. All users must complete a background investigation and complete the VA PIV smartcard processes before acquiring credentials to login.

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?

Contractors follow the VA onboarding process, which includes signing a confidentiality agreement.

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

Yes

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

Contractors supporting Entra ID will have access with PII data on users. The contract must be current for a contractor to request and maintain access. Clearance is required in the form of a Risk Background Investigation.

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) is provided and signed by each VA employee before access is granted to their email account. Annual Government Ethics and Privacy & HIPAA Training is also required of all users. All VA employees take a yearly VA Privacy and Information Security Awareness and Rules of Behavior training class in the TMS system.

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

8.4a If completed, provide:

1. *The Security Plan Status:* TBD
2. *The System Security Plan Status Date:* TBD
3. *The Authorization Status:* TBD
4. *The Authorization Date:* TBD
5. *The Authorization Termination Date:* TBD
6. *The Risk Review Completion Date:* TBD
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.***

IOC date July 1, 2025 - classification of the system: High

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)***

Software as a Service (SaaS) hosted in Microsoft Azure Commercial.

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.*

Yes, VA owns the data. (C03) 47QTCA22D003G
36C10B22F0089
Updated final MSEA (Dell Federal)
Microsoft - Azure Commercial Cloud

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

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

No ancillary data is collected.

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.

Entra ID roles and responsibilities between the VA and FEDRAMP Government Cloud Service Providers are documented in the System Security Plan (SSP).

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 Robotic Process Automation (RPA).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

TONYA FACEMIRE

Digitally signed by TONYA FACEMIRE
Date: 2025.04.07 15:56:35 -04'00'

Privacy Officer, Tonya Facemire

ALBERTINO ESTACIO

Digitally signed by ALBERTINO ESTACIO
Date: 2025.04.08 14:49:52 -07'00'

Information Systems Security Officer, Albert Estacio

CHRISTOPHER CARDELLA

Digitally signed by CHRISTOPHER CARDELLA
Date: 2025.04.09 12:25:39 -05'00'

Information Systems Owner, Christopher Cardella

APPENDIX A-6.1

No privacy notice is given because the system is syncing with active directory without user interface. No information is input by the user.

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)