Privacy Impact Assessment for the VA IT System called:

VA Microsoft (MS) Active Directory Assessing Azure (AD Azure)

Veterans Affairs Corporate Office (VACO)

Infrastructure Operations

Date PIA submitted for review:

September 12, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	Gina.siefert@va.gov	224-558-1584
Information System Security Officer (ISSO)	Albert Estacio	Albert.Estacio@VA.Gov	909-583-6309
Information System Owner	James Gunter	James.Gunter2@VA.Gov	385-282-3593

Abstract

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

The Department of Veteran's Affairs (VA) Microsoft (MS) Active Directory Azure Information System known as AD Azure is a Commercial off-the-Shelf (COTS) directory service application that stores end user, group, computer, and other device objects in an encrypted database that is replicated internally between the VA Domain Controller (DC)/Domain Name Server (DNS) servers. The AD Azure System allows approved VA identities to authenticate and access enterprise network services and resources using globally enforced multifactor factor authentication and identification. The AD Azure System and services is used by a majority of VA systems for access controls, initial employee identification and global security groups. Please see the PIA of those individual systems for the applicable connection to VA Microsoft Active Directory Azure Assessing. Due to the volume the individual systems are not listed on this PIA.

The AD Azure Information System (IS) does not store or retain individual Personally Identifiable Information (PII) from VA employees as a transfer connector agent for the MS Exchange, M0365 or PIV IS. The AD Azure Service accounts do not contain Personally Identifiable Information (PII) and Sensitive Personal Information (SPI) from veterans or other members of the public who use email to correspond with Department of Veterans Affairs staff and medical personnel. There is no specific legal authority on Active Directory Services, Exchange Email or M0365. The systems are FIPS compliant as basic support for the enterprise core infrastructure also known as general support services within the VA. However, VA security policies and procedures surrounding the support of the 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."

Overview

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

1 General Description

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

The IT system name in eMASS is VA Microsoft Active Directory Azure Assessing (AD). The name of the program office that owns AD Azure is VACO, Infrastructure Operations (IO).

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

The business and technology purpose is basic identification and authentication for employees and devices to initially connect/access the VA enterprise network.

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

VA owns and controls the AD Azure information system.

2. Information Collection and Sharing

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

Approximately 850,000 VA employees (Government and Contractors) and devices are the expected resource objects stored in the AD Azure System. The VA business PII data the AD Azure System uses on individuals is: employee name, work location, work phone, work email.

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

The AD Azure System initially collects data on individuals via the VA onboarding process and on the VA devices via the VA ServiceNow process. PII data on individuals: employee name, work location, work phone, work email. Initial data on VA devices is hostnames on servers, workstations, laptops, mobile phones. AD data is for the purposes of allowing identification and globally enforced authentication on VA resources to initially access the VA network.

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

PII data for AD Azure is shared electronically via the Lightweight Directory Access Protocol (LDAP) between the VA Domain Controller (DC) servers. The DCs replicate the VA MS Active Directory Services database internally between DCs.

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

The AD Azure servers are operated in more than one site. Use of the AD Azure servers and the PII data on the AD Azure servers is maintained consistently in all sites. For example; the VA Microsoft (MS) Active Directory database is replicated 24/7 to all VA Domain Controller (DC) servers at all sites. The same controls for the AD Azure System are used across the sites.

3. Legal Authority and SORN

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

Legal authority to operate references and governance includes:

5 U.S.C. 552, "Freedom of Information Act," c. 1967
5 U.S.C. 552a, "Privacy Act," c. 1974
17 U.S.C. 106, “Exclusive rights in copyrighted works”
18 U.S.C. 1030 (a) (3), "Fraud and related activity in connection with computers."
21 U.S.C., Food and Drugs
38 U.S.C. 218, "Security and law enforcement on property under the jurisdiction of the Veterans Administration"
38 U.S.C. 3301, "Confidential nature of claims"
38 U.S.C. 3305, "Confidentiality of medical quality assurance records"
38 U.S.C. Section 44132 covers Drug and Alcohol treatment and scheduling records
PL 100-322 covers the confidentiality of AIDS patients’ data
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
OMB Circular A-130, Appendix III, “Security of Federal Automated Information Systems”
Page 3 of 29
Information Technology Management Reform Act of 1996 (known as Clinger-Cohen Act)
Federal Information Security Management Act (FISMA) of 2002
Government Paperwork Elimination Act (GPEA), PL 105-277
OMB M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
Executive Order 13103, “Computer Software Piracy”
FIPS 199, “Standards Security Categorization Federal Information & Information Systems”
FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems”
FIPS 201-1, “Personal Identity Verification of Federal Employees and Contractors”
FIPS 140-2, “Security Requirements for Cryptographic Modules”

SORN: 145VA005Q3. Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA located at https://www.govinfo.gov/content/pkg/FR-2022-07-01/pdf/2022-14118.pdf

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?

The SORN does not require amendment or revision; SORN covers Cloud storage.

D. System Changes

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

The completion of this PIA will not result in circumstances that require changes to VA business processes.

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

The completion of this PIA will not potentially result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☐ Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Other Data Elements (list below)

Personal Phone Number is Not Collected for AD Azure but Could be Provided As A Business Number Personal Address is Not Collected for AD Azure but Could be Provided As A Business Number during initial onboarding.

PII Mapping of Components (Servers/Database)

The **VA Microsoft (MS) Active Directory Azure Assessing (AD Azure)** information system consists of over 600 key components (servers). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the AD Azure System and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VA Microsoft Active Directory Service Database	Yes	Yes	Employee Name, Work Location, Work Phone Number, Work Electronic Mail (Email) Address	VA Resources - User Accounts, Global Security Groups - Users	MS Defender, Change Auditor, Splunk Auditing, VA-CSOC Scans, TIC Gateway

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?

Information is collected directly from the individual as part of the VA onboarding process.

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.

Sources other than the individual is not required.

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

The AD Azure information system does not create a score. analysis or report as a source of information.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Information is collected directly from the individual as part of the VA onboarding and multi-factor smartcard processes for a VA PIV card via HR, VA Sponsor/Manager or Contracting Officer Representative (COR.) The PII data is transmitted internally/electronically from Identify Management and PIV systems.

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

The AD Azure System does not collect PII data on a form. The employee initial onboarding process is via HR, Contracting Officer Representative (COR), and VA PIV Card Sponsor processes in accordance with the HSPD-12 guidelines and is the initial starting point for creating the PII employee business data for reuse by multiple VA systems. HR, COR and Sponsor review automation forms such as the Electronic Computer Access Request Form (ECARF) which support a SNOW ticket for the Identity Management group to create the Directory Service user account. Requests for changes or updates to the PII information in the AD Azure System is submitted by the employee, their Manager/COR or HR directly to the Service Now work ticket system.

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.

Information VA receives from each employee is presumed to be accurate; however, when IDM creates a Directory Services (DS) account, an e-mail notification is sent to the employee's VA e-mail address. The employee, HR, COR or ISSO can submit any necessary change requests via the VA YourIT or ServiceNow system. Due to its nature, the information shared with the VA in emails or other components of the AD Azure System is not checked for accuracy. Computer matching checks on employee name accuracy is through VA HR security background and adjudication checks, fingerprinting, biometrics, and National Agency Checks, HSPD-12, GSA USAccess for creating VA PIV smartcards for employees which requires multiple identification artifacts.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

The AD Azure System does not check for accuracy on employee data. Accuracy process is initially handled prior to data being added to AD Azure via the HR, Security and PIV processes during initial onboarding. After the onboarding process, HR, Managers or employees submit Service Now (SNOW) work tickets to update the PII data.

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

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. There is no specific legal authority that authorizes the use of data for Active Directory Azure (AD Azure) Services user accounts; however, the security policies and procedures surrounding the support of the confidentiality, identification, authentication and email includes 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;" Appendix II and the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347). The authoritative publications require that all users of a system be uniquely identified to be able to use a federal information system. The MS Active Directory Services as a required component of the AD Azure System database implements the NIST requirements by using the individual's name as part of the identification process.

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. (*Work with your System ISSO to complete this section)*

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

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

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

Follow the format below when entering your risk assessment:

Privacy Risk: Attempts to access AD Azure data on the VA Domain Controller (DC) servers without an active smartcard (VA PIV card) and elevated permission accounts could be attempted.

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. Unauthorized access to AD data on VA DCs is mitigated by Change Auditor, Splunk, MS Advanced Threat Protection Defender, VA-CSOC scans, continuous monitoring, reviews and VA Policy for compliance. Anonymous access or public access to the DCs is not permitted.

Section 2. Uses of the Information

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

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

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

PII data collected for the AD Azure System is used internally for employee authentication and identification. The business information collected and maintained in the AD Azure System provides VA with a single search point for VA staff with approved role-based permissions and enforced multi factor authentication to identify VA employees.

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 information officially collected for the AD Azure System Directory Service 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 the AD Azure System.

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 AD Azure System does not create duplicate accounts on individual users (VA employees). The AD Azure System does not make available new or previously unutilized information or create newly derived data on an individual.

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?

Protection of data at rest examples: full disk encryption, Bitlocker is installed on AD DC servers, MS Defender to protect data at rest, Change Auditor, Splunk, VA-CSOC Continuous Monitoring

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

The AD Azure System and DCs do not collect, process or retain SSNs.

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

PHI data is not collected and stored on the AD Azure System. PII data is basic work-related data. PII data types are provided in PTA/PIA Tables which are used by IDM to create a VA Active Directory Services account for initial enterprise network access. AD Azure data includes: Employee Name, Work Address, Work Phone number. PII safeguard examples includes: enterprise global security groups (GPOs), MS Advanced Threat Protection (ATP) Defender, Change Auditor, Splunk Auditing, VA-CSOC processes (ICAMP, REEF), VA gateway, Firewalls, Host Intrusion Protection (HPS).

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?

During VA onboarding processes for employees when PIV card is issued, and accounts created.

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

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. VA Sponsor/Manager approves access. Approval is required for a VA PIV card, global security groups, and network access on VA employees as part of the onboarding process.

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

Reference: Abstract. Business PII data is collected for the VA Active Directory (AD) System from the VA employee onboarding systems/processes Access to data on the AD Azure System DC servers is monitored and tracked. Examples include: the VA Office of Information Security (OIS) Systems and Teams supporting Human Resources (HR), PIVA; Change Auditor, Splunk Auditing, Global Security Groups (GPOs), MS ATP Defender. The account management of VA Active Directory Service user accounts initially created by Identify Management (IDM) during the onboarding process will enable VA to remove employees who no longer require enterprise network access and work email. The management features provide for additional security including the ability to change passwords or re-create accounts as needed for security reasons to ensure that unauthorized access to AD records is a low risk. The VA requires employees and contractors to read and sign the VA Rules of Behavior (ROB) before access is allowed to the VA network and email account. Additionally, all VA employees and contractors must take Annual Government Ethics & Privacy and HIPAA Focused annual training. The "Privacy and HIPPA Focused Training" course is designed to address the controls regarding the proper handling and use of user information. VA utilizes the Talent Management System (TMS) for yearly privacy training and evidence training was completed. All users must complete this yearly training.

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

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*

Employee Name, Work Address, Work Phone, Work Email; Personal Phone Number and Personal Address is Not Collected for the AD Azure System but could be provided as business data during onboarding processes via other systems.

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.*

Basic PII user data on VA employees is retained and stored in the AD Azure System 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. AD Azure 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) or approved accounts with hardened passwords. Daily backups are performed on the AD Azure System. AD Azure accounts can only be recovered natively by the MS operating system for up to 180 days if the account was disabled for inactivity or if deleted.

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?

AD Azure 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 the AD Azure System data. Other systems on VA employees retain records.

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

There is no records retention, series, and disposition authority on a deleted AD account. When an employee leaves the VA; several items handled via the local Facility which includes disabling/deleting the AD Azure account with the basic Business PII data on the employee.

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.

Reference sources: Account Management SOP, VA, HR and HSPD-12 Policies. The VA AD accounts on employees are eliminated electronically in the Directory Services system by VA OIT Service Lines/Facility Teams with elevated permissions via ServiceNow processes when an employee leaves VA. The process used is called deletion; to remove the account and removes the account from security groups for authentication/identification and access to the VA network. AD Azure accounts are not transferred to NARA; and there is no mandatory retention period as with other VA systems. VA DCs in the FEDRAMP Government Cloud are the backup solution for VA Active Directory Services accounts. Retention is 15 days of AD data at which time the information is "tombstoned". Tombstoning is an automated process that takes data and marks it for deletion; the AD Azure data is automatically be deleted by the system after 180 days and cannot be retrieved.

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 AD Azure System does not use collected PII data on employees for testing, research or training.

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

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

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

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

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 an AD Azure account could be stored longer than necessary to accomplish the mission.

Mitigation: Information is purged after 15 days on the VA AD Azure information system backups. The AD Azure System utilizes a "Recycling Bin" to recover 180 days' worth of deleted user account information that authorized users with elevated permission accounts can restore. The information stored is private and owned by the VA; it is not public data. The data backup process for the VA AD Azure System resides in the approved FEDRAMP Government Cloud Service Provider.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VA MS Active Directory Assessing	AD Database is Replicated between the VA Domain Controllers (DCs)	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 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: Expired or inactive accounts are a risk if access control lists and inactive accounts are not disabled/enforced/deleted.

Mitigation: Expiration dates and service account activity are tracked through Change Auditor and reviews; global policies are also monitored through VA OIS Security Teams.

Section 5. External Sharing/Receiving and Disclosure

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

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

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

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

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

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

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

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

Data Shared with External Organizations

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Not applicable as data is not shared externally.

Mitigation: Not applicable as data is not shared externally.

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.

Examples include OMB Form No. 2900-0673 and VA Form 0711 REQUEST FOR PERSONAL IDENTITY VERIFICATION (PIV) employee identification badge during VA onboarding process and Federal Register System of Record Notice (SORN) 145VA005Q3, "Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA" Privacy Act System of Records Notices (SORNs) - Privacy

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

Notification is given to potential VA applicants prior to their information being stored as back up data in the AD Azure System. The information is for employment, employees, contractors and affiliates. This notice is on OMB Form No. 2900-0673 and VA Form 0711 REQUEST FOR PERSONAL IDENTITY VERIFICATION (PIV) CARD. Please see the notice below on a VA PIV Card Application Form. The System of Record Notice (SORN) 145VA005Q3. Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA
https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf
PRIVACY ACT STATEMENT: VA is authorized to ask for the information requested on this form by Homeland Security Presidential Directive (HSPD)-12, and 31 USC 7701. The information and biometrics collected, collected as part of the Federal identity-proofing program under HSPD-12 are used to verify the personal identity of VA applicants for employment, employees, contractors, and affiliates (such as students, WOC employees, and others) prior to issuing a department identification credential. The credentials themselves are to be used to authenticate electronic access requests from VA employees, contractors, and affiliates issued a department identification credential to gain access to VA facilities and networks (where available) through digital access control systems, as well as to other federal government agency facilities and systems were permitted by law. The information collected on this form is protected by the Privacy Act, 5 USC Section 552(a) and maintained under the authority of 38 USC Section 501 and 38 USC Sections 901905 in VA system of records "Police and Security Records-VA (103VA07B)". VA may make a "routine use" disclosure of the information in this system of records for the routine uses listed in this system of records, including civil or criminal law enforcement, constituent congressional communications initiated at your request, litigation, or administrative proceedings in which the United States is a party or has an interest, the administration of VA programs, verification of identity and status, and personnel administration by Federal agencies. Failure to provide all of the requested information may result in VA being unable to process your request for a Personal Identity Verification Card, or denial of issuance of a Personal Identity Verification Card. If you do not have a Personal Identity Verification Card, you may not be granted access to VA facilities or networks, which could have an adverse impact on your application to become, or status as, a VA employee, contractor or affiliate where such access is required to perform your assigned duties or responsibilities. Your obligation to respond is mandatory. A web search for the PIV request form where this paragraph was quoted from shows the form: https://www.va.gov/files/2022-04/PIV-0711-form.pdf

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.

VA banner notices on Web sites are reviewed by VA legal prior to posting on the web; and is per HSPD-12 guidelines and NIST requirements.

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.

The only information officially collected and solicited prior to it being stored/maintained as back up data on the AD Azure System is basic employee PII data. The obligation is mandatory to provide the user an individual unique username as approved credentials to initially login to the VA network and perform their assigned duties. If the user declines to provide basic PII data via HR, COR or PIV smartcard Sponsor for a Service Now (SNOW) ticket; a unique AD account cannot be created for initial VA network access.

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 AD Azure System does not provide a means for consent. Basic business PII data collected on VA employees for the AD Azure System 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 System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

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

Mitigation: Access to data stored on the AD Azure System servers with user accounts is not possible without a valid credentialed Non-Mailed Enabled Account (NMEA), multi-factor authentication, and EPAS. AD servers log all credentialed logons. Anomalous behavior is logged, and auto alerts are generated. Change Auditor, server logs and monitoring provide evidence of access of individuals with elevated permissions accessing AD Azure System servers.

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.***

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.

Correction procedures are the same as 7.1. References: VA Account Management SOP; 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 the PII data for their employee name, work location/address, work phone and work email address in the AD Azure System.

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 the AD Azure System 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: The AD Azure System is not an official system of record. AD Azure does not maintain records related to members of the public. As there are no medical records on Veterans or members of the public in AD Azure, 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 System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:

Privacy Risk: There is a risk that stored user information in the AD Azure System could be accessed by an unauthorized party such as a Hacker. Hacker attempts generate an "Access Denied" alert is sent automatically to the requestor, ISO, AD Azure System Team and VA-CSOC.

Mitigation: Anonymous access to information in the AD Azure System is not possible without a valid credentialed elevated permission account. VA Domain Controller (DC) servers log all credentialed logons to the VA domain. Anomalous behavior is logged, and auto alerts are generated. In place compensating controls include Change Auditor, Splunk, MS ATP Defender, and OIS Security Team scans/monitoring. Service Now tickets are generated on Access Denied elevated permission accounts.

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.

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 the system; references include the VA Account Management SOP and FY23 AD/AD AZURE SOPs.

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 AD 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 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, contractors supporting the VA AD Azure System as VA employees will have access to the AD Azure servers 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. Contracts are reviewed by the Contracting Officer Representative (COR). AD accounts for contractor employees have an expiration date (Contract end date) in IAM (Identity and Access Management)/MIM and VA PIV smartcard. Contractor access is disabled automatically based on the contract expiration date. NDA is contract specific. If it is stated in contract that they have to sign. BAA (Business Associate Agreement) at the executive level can cover it, as well.

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

Yes.

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* 05/17/2023
3. *The Authorization Status:* Completed
4. *The Authorization Date:* 01/06/2022
5. *The Authorization Termination Date:* 01/05/2025
6. *The Risk Review Completion Date:* 05/16/2023
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 No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Not applicable.

Section 9 – Technology Usage

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

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

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

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

FEDRAMP Government Microsoft Amazon (AWS)

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.*

FEDRAMP Government Amazon (AWS) System Security Plan (SSP)

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.

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 AD Azure System 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).

Not applicable. 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**

ID	Privacy Controls
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.

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2023.10.12 05:47:43 -05'00'

Privacy Officer, Gina Siefert

Albertino M. Estacio 119921 Digitally signed by Albertino M. Estacio 119921
Date: 2023.10.12 12:22:58 -07'00'

Information Systems Security Officer, Albert Estacio

JAMES GUNTER Digitally signed by JAMES GUNTER
Date: 2023.10.12 07:20:29 -05'00'

Information Systems Owner, James Gunter

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).

A link to the notice or verbiage referred to in Section 6 is not from the AD System on the collected basic employee business data from the VA employee onboarding processes; it's from the forms used by HR, COR, PIV, IDM (Identify Management) which are different security boundaries.

Notification is given to potential VA applicants prior to their information being stored as back up data in the AD Azure System. The information is for employment, employees, contractors and affiliates. This notice is on OMB Form No. 2900-0673 and VA Form 0711 REQUEST FOR PERSONAL IDENTITY VERIFICATION (PIV) CARD. Please see the notice below on a VA PIV Card Application Form. The System of Record Notice (SORN) 145VA005Q3. Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf

PRIVACY ACT STATEMENT: VA is authorized to ask for the information requested on this form by Homeland Security Presidential Directive (HSPD)-12, and 31 USC 7701. The information and biometrics collected, collected as part of the Federal identity-proofing program under HSPD-12 are used to verify the personal identity of VA applicants for employment, employees, contractors, and affiliates (such as students, WOC employees, and others) prior to issuing a department identification credential. The credentials themselves are to be used to authenticate electronic access requests from VA employees, contractors, and affiliates issued a department identification credential to gain access to VA facilities and networks (where available) through digital access control systems, as well as to other federal government agency facilities and systems were permitted by law. The information collected on this form is protected by the Privacy Act, 5 USC Section 552(a) and maintained under the authority of 38 USC Section 501 and 38 USC Sections 901905 in VA system of records "Police and Security Records-VA (103VA07B)". VA may make a "routine use" disclosure of the information in this system of records for the routine uses listed in this system of records, including civil or criminal law enforcement, constituent congressional communications initiated at your request, litigation, or administrative proceedings in which the United States is a party or has an interest, the administration of VA programs, verification of identity and status, and personnel administration by Federal agencies. Failure to provide all of the requested information may result in VA being unable to process your request for a Personal Identity Verification Card, or denial of issuance of a Personal Identity Verification Card. If you do not have a Personal Identity Verification Card, you may not be granted access to VA facilities or networks, which could have an adverse impact on your application to become, or status as, a VA employee, contractor or affiliate where such access is required to perform your assigned duties or responsibilities. Your obligation to respond is mandatory. A web search for the PIV request form where this paragraph was quoted from shows the form: https://www.va.gov/files/2022-04/PIV-0711-form.pdf

VA banner notices are reviewed by VA legal prior to posting on the web; and is per HSPD-12 guidelines and NIST requirements.

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices