Privacy Impact Assessment for the VA IT System called:

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

VACO,

Development, Security and Operations (DSO), Solution Delivery (SD)

Date PIA submitted for review:
9/7/2022

VA System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Gina Siefert</td>
<td><a href="mailto:gina.siefert@va.gov">gina.siefert@va.gov</a></td>
<td>(202) 632-8430</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Albert Estacio</td>
<td><a href="mailto:Albert.estacio@va.gov">Albert.estacio@va.gov</a></td>
<td>909-583-6309</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>James Gunter</td>
<td><a href="mailto:James.gunter2@va.gov">James.gunter2@va.gov</a></td>
<td>801-588-5044</td>
</tr>
</tbody>
</table>
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 (AD) Azure Assessing Information System (IS) herein referred to as “AD AZURE” provides the backup system hosted in the approved FEDRAMP MS Azure Cloud for enterprise Directory Services supporting VA employees and VA contractors who use globally enforced two factor authentication (2FA) through VA Personal Identification Verification (PIV) smart cards with active Public Key Infrastructure (PKI) security encryption certificates or approved network accounts with enforced hardened passwords and global policies for authentication, identification and access to the VA network and enterprise infrastructure resources. PKI is used for non-repudiation, digital signatures and encryption as a sub-function from a separate system known as the VACO PIV.

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:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- 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.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes.
- Whether the completion of this PIA could potentially result in technology changes.
- 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 VA MS Active Directory Azure Assessing Authority to Operate project is the recommended back up cloud technology solution hosted in the FEDRAMP MS Azure cloud for the VA Active Directory (AD) production Servers physical and virtual machines (VMs) sponsored by the ITOPS Enterprise Messaging and Collaboration Solution Delivery organization. The purpose of AD data is to provide identification and authentication. An estimated count of users having information stored in AD over 400,000. VA federal employees requiring access to the VA network will have an account in AD along with VA contractors and approved partners. All Districts/Regions are integrated into a VA enterprise infrastructure system. Information stored in the AD system is VA owned data and/or VA owned PII data, e.g., Address, Phone Number and Logon Name are stored for system integration with Microsoft Exchange Information System (email). Private information outside of the scope of the VA network is not to be stored in AD.

The structure of VA AD on premise data that is stored as a backup in the Azure cloud consists of one root domain named va.gov along with sub subdomains. The main offices/subdomains are cem.va.gov, dva.va.gov, med.va.gov, and vba.va.gov which equate to 33 Domains for the VA enterprise infrastructure design in the Azure Cloud. The VA uses AD services for authentication and identification and to perform as the Domain Name Service using FIPS compliant solutions to support Microsoft (MS) Exchange (VA Email and Calendaring) and MS Office 365 (MO365) for over 400,000 employees using smartcards (VA PIV Cards).

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, MO365 or PIV IS. The AD 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 MO365. 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.”

The specific authority to operate references and governance includes:

- 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)
• Information Technology Management Reform Act of 1996 (also known as the 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 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”

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://va.gov/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 Account Information
- Health Insurance Beneficiary Numbers
- Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
VA Personal Identification Verification (PIV) smartcard data for end users to digitally sign and encrypt VA email using Public Key Infrastructure (PKI) certificates hard coded on PIV cards. The VA PIV card not M0365 contains PII and PKI certificates. PIV is a VHA system not VBA.

PII Mapping of Components

The AD AZURE system consists of 0 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by AD AZURE and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The business information used to create user identification network and service accounts which are stored as AD back up data are provided by role-based access service accounts with elevated permissions and approved VA System or Network Administrators in accordance with VA Handbook 6500. Elevated accounts are audited quarterly. For example, the VA Information System Security Officer (ISSO) reviews a work service ticket request which includes the user’s name and other VA owned information like address and phone number submitted by VA Human Resources or Sponsor, e.g., Manager/Supervisor or Contracting Office Representative. The work ticket is facilitated by the District/Regional Directory Services (DS) Administrator to create a DS and email account which will be stored as back up data in the AD Azure solution in the cloud.

1.3 How is the information collected?

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?

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.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information used by the Department of Veteran Affairs and Enterprise Messaging and Collaboration to provide the services agreed to for VA will be provided by VA personnel through the Help Desk Center. VA support personnel collect the necessary information from employees/service accounts and provide the information to OI&T Teams to create the user network and email accounts. Requests for changes or updates to user accounts and the information contained within them will be submitted by the user directly to the National Help Desk and managed using a ticketing system. The ISO reviews automation forms such as the Electronic Computer Access Request Form (ECARF) which support a ServiceNow work ticket for the District/Regional Directory Services (DS) Team to create a DS and email account.
1.4 How will the information be checked for accuracy? How often will it be checked?

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.

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.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Information that VA receives from each employee is presumed to be accurate; however, when a user is assigned a Directory Services (DS) network and VA e-mail address, an e-mail notification is sent to the user’s new VA e-mail address. The user may then review their information in the Exchange 2010 or M0365 Global Address List (GAL) and submit any necessary change requests via the VA National Help Desk also known as YourIT or ServiceNow system. Due to its nature, the information shared with the VA in emails or other components of the system is not checked for accuracy. The District/Regional Support Teams and VA Human Resources Teams validate AD data for accuracy to ensure the information is correct before the information is backed up in the AD AZURE IS.

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

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

This question is related to privacy control AP-1, Authority to Collect

The System of Record Notice (SORN) Identification (ID) #145VA005Q3 Department of Veteran’s Affairs Personnel File System (VAPSFS) is the applicable reference from the PIA Support Team on Active Directory data that is backed up and hosted in the FEDRAMP Microsoft (MS) Azure cloud. The employee data which is backed up in AD AZURE is by the on-premise Active Directory Services system for creating an enterprise network account; it’s a subset of employee data (name, email, phone, location). It is not all-inclusive employee data.

There is no specific legal authority that authorizes the use of email, specifically the Exchange system used for email or Directory Services. However, 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. Microsoft (MS) Active
Directory Services as a required component of the VA MS AD AZURE IS and connectors for the MS Exchange IS (VA email system), implements 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.

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 cloud data without an active smartcard (VA PIV card) and electronic token could be attempted.

**Mitigation:** The risk is low. Two factor authentication (2FA) and E-Tokens with active Public Key Infrastructure (PKI) hard coded encryption certificates are globally enforced. Unauthorized access to AD back up information is mitigated by Change Auditor, regular system scans, reviews and continuous monitoring of the VA network and Cloud Host Service Provider for baseline compliance. Anonymous access or public access 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.

Business contact information is collected and maintained in the Directory Services system which provides the VA with a single search point for VA staff with approved role-based permissions and enforced 2FA to identify VA employees. Shared data between AD, Exchange, PIV and M0365 includes:

**Network Identification:** Network log on to identify users/service accounts and Domain Name

**Other Internal System Name(s) i.e., Unique System Identifiers, Distinguished Name, Common Name**

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual’s existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The information officially collected for and stored in the **VA Microsoft (MS) Active Directory (AD) Azure Assessing Information System** is used solely to identify back up data on individuals, groups and service accounts granted 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.

2.3 How is the information in the system secured?

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

MS DEFENDER to protect data at rest, Dell Change Auditor, FSS Splunk, Continuous Monitoring (VA & Government AZURE)
2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

AD Azure System does not collect, process, or retain SSNs.

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

No PHI data. PII data is basic work-related data provided in the Section 1 Table to create a VA network account: Employee Name, Work Address, Work Phone number.

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

The active management of Directory Service accounts which are initially created, stored and located on premise and backed up to AD Azure hosted in the cloud will enable VA to remove personnel that no longer require access and account management features and provide for additional security including the ability to change passwords or re-create accounts as needed for security reasons. This will ensure that unauthorized access to 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.

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.

Information listed in question 1.1 is maintained in the AD Information System (IS) on premise to populate parts of the Global Address List (GAL) in Exchange and associated with M0365 database parameters; and to identify/maintain approved user accounts for example in Directory Services. The AD IS/Directory Services data is backed up in the AD AZURE system hosted in the cloud. In addition to the network log on account identification; Exchange and M0365 data points include:

- Name
- (VA) Mailing Address
- (VA) Zip Code
- (VA) Phone Number(s)
- (VA) Fax Number
- (VA) Email Address

Federal agencies are required to manage records in accordance with the Federal Records Act (44 U.S.C. Chapter 31) and 36 Code of Federal Regulation (CFR) Chapter XII Sub-Chapter B.

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?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. This question is related to privacy control DM-2, Data Retention and Disposal.

Data will be retained and stored in the AD AZURE backup solution as long as users are approved to access the VA enterprise network, special programs and email with an active smartcard or approved Directory Services account and hardened password. If a user leaves the VA or no longer requires access; VA personnel are required to disable and then remove the account as required. Global group policies deactivate accounts which are in active greater than 90 days. AD information is only maintained for the
duration of time that an individual is a Federal employee, contractor, or other partner requiring access to the VA network with enforced 2FA smartcards (VA PIV cards) or approved network accounts with hardened passwords. Backups are performed on the VA MS AD AZURE IS accounts; accounts can be restored within 15 days. An account can be recovered natively by the MS operating system hosted in the Azure cloud for up to 180 days if disabled for inactivity or deleted.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

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.

This question is related to privacy control DM-2, Data Retention and Disposal.

When managing and maintaining VA data and records, the VA Directory Services Teams follow guidelines established in the NARA-approved Department of Veterans’ Affairs Record Control Schedule (RCS)-10 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf); Department of Veterans Affairs, Office of Information & Technology RCS 005-1 (http://www.rms.oit.va.gov/docs/RCS005-1-OIT-8-21-09.pdf) and the General Records Schedule (http://www.archives.gov/records-mgmt/grs/).

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?

This question is related to privacy control DM-2, Data Retention and Disposal.

Data backup information does leave the control of the VA. Retention is for 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 data will 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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

The VA MS AD AZURE Information System does not use PII for testing, research or training.
3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

**Mitigation:** Information is purged after 15 days on the VA MS AD AZURE IS backups. The AD system utilizes a “Recycling Bin” to recover 180 days’ worth of deleted user account information that authorized users can restore. The information stored is private and owned by the VA; it is not public data. The data backup process resides in the approved FEDRAMP Cloud Service Provider known as Azure managed by Microsoft.

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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veterans Health Administration (VHA)</td>
<td>VA Active Directory Services System</td>
<td>VA logical access for enterprise network for access, identification, and authentication</td>
<td>End user list of VA employees electronically transmitted by VA Domain Controllers</td>
</tr>
<tr>
<td>Veterans Health Administration (VHA)</td>
<td>VACO PIV System</td>
<td>VA Personal Identification Verification (PIV) smartcard data for end users to digitally sign and encrypt VA email using Public Key Infrastructure (PKI) certificates hard coded on PIV cards. The VA PIV card not M0365 contains PII and PKI certificates. PIV is a VHA system not VBA.</td>
<td>Electronically pulled from the VA Card Management System (CMS) under the VACO PIV Authority to Operate (ATO) Information System (IS) project using</td>
</tr>
</tbody>
</table>
List the Program Office or IT System information is shared/received with | List the purpose of the information being shared/received with the specified program office or IT system | List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system | Describe the method of transmittal

Veterans Health Administration (VHA) | PKI | PKI Certificates (encoded or derived) | approved devices and systems.

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.

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.

**Mitigation:** Expiration dates and service account activity are tracked through Change Auditor; global policies are also monitored through VA 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

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

### 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.
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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

Notification is given to potential VA applicants prior to their information being stored as back up data in AD AZURE. 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 901-905 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

6.2 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 AD AZURE is basic user data. The obligation is mandatory to provide the user an individual username such that they can have credentials to login to the VA network and perform their assigned duty. If the individual declines to provide information a unique identification account cannot be created for VA network access or email.

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*
AD AZURE does not provide a means for consent. The data collected is the user’s name and is mandatory to comply with identification and authentication to the VA Network and for an email account.

### 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.

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 stored information on user accounts could be accessed by someone with elevated permissions who does not have a need to know.

**Mitigation:** Access to information in AD AZURE is not possible without a valid credentialed account and 2FA. AD servers log all credentialed logons. Anomalous behavior is logged, and auto alerts are generated. Change Auditor, logs and monitoring provide evidence of access of individuals with elevated permissions.

### 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?

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.
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).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Authenticated users can query their own information for inaccuracies or updates through AD on premise. A work ticket through ServiceNow or YourIT can be submitted to correct VA owned information as needed.

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.

Authenticated users of the VA AD system can query their own information for inaccuracies or updates through AD on premise. A work ticket through ServiceNow or YourIT can be submitted to correct VA owned information.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The System of Record Notice (SORN) Identification (ID) #145VA005Q3 Department of Veteran’s Affairs Personnel File System (VAPSFS) is the applicable reference from the PIA Support Team on Active Directory data which is backed up and hosted in the FEDRAMP Microsoft (MS) Azure cloud. The employee information in AD used to create an enterprise network account is a subset of employee data (name, email, phone, location); it’s not an all-inclusive employee data system. The local Information Technology (IT) Teams and/or District/Regional IT Support Teams will inform the user the correct procedure to correct his or her information through the AD on premise system. Please note: AD on premise Information System (IS) and the AD AZURE IS are not an official system of record and do not maintain records related to members of the public. As there are no records on Veterans or members of the public, there are not any records for an individual to request redress.
7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Authenticated users of the AD 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: AD on premise and AD AZURE are not an official system of record and does not maintain records related to members of the public. As there are no records on Veterans or members of the public, there are not any records for an individual to request redress.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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 information could be accessed by an unauthorized party.

Mitigation: Anonymous access to information in the AD on premise or AD AZURE systems are not possible without a valid credentialed account. Domain Controller 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 and Security Team scans/monitoring.

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?

Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

The ISO in conjunction with the approval of the requesting employee’s supervisor and facility CIO verifies identity and training requirement completion of the requesting employee and approves access to the VA Network and email. 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. ISOS conduct reviews of user access requests, including identification, to ensure compliance with information security requirements in VA Handbook 6500; NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems; and the Information Security Reference Guide. EPAS approvals are reviewed quarterly. All users must be Federal employees, contractors, or authorized partners. All users must complete a background investigation and complete the PIV Form 0711 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.
Yes, contractors supporting Cloud Service Providers have access to VA AD AZURE virtual machines with a smartcard (VA PIV card). 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). Contractors have an expiration date (Contract end date) in IAM (Identity and Access Management)/MIM and PIV card, and contractor’s access will be disabled automatically in 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 PHI are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

The Rules of Behavior (ROB) are provided and signed by each 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?

If Yes, provide:

1. The Security Plan Status,
2. The Security Plan Status Date,
3. The Authorization Status,
4. The Authorization Date,
5. The Authorization Termination Date,
6. The Risk Review Completion Date,
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

If No or In Process, provide your Initial Operating Capability (IOC) date.
The Authorization and Accreditation (A&A) has been completed for AD AZURE for formal reviews, recommendations, and Authority to Operate (ATO) approval. A&A paperwork is reviewed and stored in the official VA data repository systems known as eMASS.

1. Security Plan Status: Approved
2. Security Plan Status Date: 30 Sep 2021
3. Authorization Status: Authority to Operate (ATO)
4. Authorization Date: 06 Jan 2022
5. Authorization Termination Date: 05 Jan 2025
6. Risk Review Completion Date: 28 Dec 2021
7. FIPS 199 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).

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.

VAEC Azure Government.

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

AD Azure is a backup system for domain controller AD. VA is the data owner not the Cloud Service Provider.
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.

CSP doesn’t collect any ancillary data.

9.4 NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A.

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).

The system doesn’t utilize Robotic Process Automation (RPA). The system uses services accounts and group managed service accounts
# Section 10. References

Summary of Privacy Controls by Family

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

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

Gina A Siefert
Privacy Officer, Gina Siefert

Digitally signed by Gina A Siefert
273290
Date: 2022.09.14 15:01:00 -05'00'

Albertino M. Estacio
Information Systems Security Officer, Albert Estacio

Digitally signed by Albertino M. Estacio
119921
Date: 2022.09.14 11:50:25 -07'00'

JAMES GUNTER
Information Systems Owner, James Gunter

Digitally signed by JAMES GUNTER
Date: 2022.09.14 12:09:09 -05'00'
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).

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