Privacy Impact Assessment for the VA IT System called:

VA Microsoft (MS) Active Directory (AD)
Assessing

ITOPS Solution Delivery

Date PIA submitted for review:

09/28/2020

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>Rita Grewal</td>
<td><a href="mailto:Rita.Grewal@va.gov">Rita.Grewal@va.gov</a></td>
<td>202-632-7861</td>
</tr>
<tr>
<td>Information System Security Officer</td>
<td>Mary K. Jones</td>
<td><a href="mailto:Mary.Jones3@va.gov">Mary.Jones3@va.gov</a></td>
<td>302-893-6772</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>James E. Gunter</td>
<td><a href="mailto:James.Gunter2@va.gov">James.Gunter2@va.gov</a></td>
<td>385-282-3593</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) Assessing Information System (IS) herein referred to as “AD” provides enterprise Directory Services for VA employees and VA contractors using globally enforced two factor smartcard authentication and accessibility using VA Personal Identification Verification (PIV) cards with active Public Key Infrastructure (PKI) security encryption certificates) to authenticate, identify and access 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.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and sub-systems, 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?
- Does the system use cloud technology? 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.

- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
- 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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?

The VA MS Active Directory Assessing Authority to Operate (ATO) project represents Directory Services which is sponsored by the ITOPS Enterprise Messaging and Collaboration Solution Delivery organization. The purpose to provide authorization and authentication to the VA network. An estimated count of users having information stored in AD is 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 systems 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 AD 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. The Department of Veteran Affairs (VA) uses AD for authentication and identification and to perform as the Domain Name Services using FIPS compliant solutions to support Microsoft (MS) Exchange (VA Email and Calendaring) and MS Office 365 (M0365) for over 800,000 employees using smartcards (VA PIV Cards).

The AD IS does not store or retain individual PII from VA employees as a transfer connector agent for Exchange, M0365 or PIV. 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.”

The specific authority to operate references and governance includes:

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.
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
- Tax Identification Number
- Medical Record Number
- Other Unique Identifying Number (list below)

The AD Information System is the VA enterprise infrastructure starting point for network authentication and basic identification of VA employees. In order to support the services requested by VA employees to support Veterans the Service Now Help Desk and Integrated Campus Support Teams can access basic employee work data listed above which is stored in the AD Information System profile on an employee. For example; employee name, work mailing address, work electronic mail address (email) and work phone number. During onboarding work data is the approved parameters from Sponsors or Managers for employees: work location, work email and work phone number; however it is possible for exceptions to policy which allow a personal address, email or phone number on an emergency basis or approved short term as needed basis. Personal data is not the approved standard data type; but because it is possible combined AD data is considered PII. No medical data or social security numbers are required to create an AD account for employees to access the VA network.

**PII Mapping of Components**

<Information System Name> consists of <number> key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by <Information System Name> and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**
**PII Mapped to Components**

<table>
<thead>
<tr>
<th>Components of the information system (servers) 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>Email text within body of the email or attachment to VA email</td>
<td>Yes</td>
<td>Yes</td>
<td>Work contact information</td>
<td>VA Staff with VA PIV (smartcards) to send/receive email</td>
<td>Multi-factor User Authentication (Active PKI certs on smartcards)</td>
</tr>
<tr>
<td>Email header packet which can be from the VA Global Address List (GAL) Exchange/Outlook</td>
<td>No – only business</td>
<td>No – only business</td>
<td>Work contact information</td>
<td>VA Staff with VA PIV (smartcards) to send/receive email</td>
<td>Multi-factor User Authentication (Active PKI certs on smartcards)</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 contact information used to create user identification network and email accounts for VA staff will be provided by role-based access and approved VA administrators working with the individual staff members. For example; Enterprise Service Desk 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.
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 technology 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 Enterprise Service Desk. Generally, administrators and other support personnel will collect the necessary information from new VA employees or contractors and will then provide the information to the Enterprise Service Desk in order to create the initial user accounts. Any requests for changes or updates to user accounts and the information contained within them will be submitted by the user directly to the Enterprise Service Desk and managed using a ticketing system. ADFS does not aggregate or store data, it is a proxy that allows users/applications to authenticate against the organization’s Active Directory.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose.

This question is related to privacy control AP-2, Purpose Specification.

The purpose of collecting information, using, disseminating, creating and maintaining the information stored in Directory Services (DS) is for initial access to the VA network and VA email. The AD IS provides the means for DS authentication and authorization to the VA network. DS is the central repository for account information for finding contacts in VA Exchange Email and MS 0365 Systems and enabling internal VA users the ability to locate and communicate is facilitated by DS. In the course of maintaining VA MS AD,
M0365 Systems via internal connectors, VA Teams collect and maintain different categories of information. Examples include:

- Collect and authenticate business contact information from VA employees, contractors, and other end users, such as e-mail address, name, work address, and telephone number. This information populates the VA Active Directory and the address book (Global Address List). It is required for user authentication and the interactive features provided by the service.
- Business contact information, at VA’s discretion, may be submitted to VA Enterprise Service Desk (ServiceNow ticketing system), to assist in responding to support incidents or troubleshooting.

1.5 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 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 Enterprise Service 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/Region Teams and VA Human Resources Teams validate AD data for accuracy to ensure the information is correct in the AD IS.

Individual (user) soft-certificates are issued under Homeland Security Presidential Directive (HSPD-12) and under the Federal Common Policy Root Certificate Authority (FPC CA.) The identity proofing, request, issuance and conditional usage of the software certificates is governed by Federal Information Processing Standards 201 (FIPS 201) mandates and guidelines under FCP CA. A copy of a valid PIV card is required for issuance. If a requestor has not had a PIV card issued OR they are an external Partner, two forms of ID are required to be documented.
1.6 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 Veterans Affairs Personnel Security File System (VAPSFS) is the applicable reference provided from the PIA Support Team on the MS AD Information System. The employee data used in the AD Information System to create an enterprise network account is a subset of employee data (name, email, phone location); it’s not all-inclusive employee data.

There is no specific legal authority which authorizes the use of work email, specifically the MS Exchange Information System used electronic mail (email) or the VA AD Information System used to create an enterprise account to access the network with enforced two factor authentication/identification; 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) Directory Services as a required component of the VA MS AD IS and connectors for the Exchange IS (VA email system), implements requirements by using the individual's name as part of the identification process.

1.7 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:** Although users are instructed not to access the VA network without an active smartcard (VA PIV card) attempts for access could be attempted.

**Mitigation:** The risk is low. It is possible but unlikely because only authorized VA users have access to the VA network and email systems with enforce multi-factor authentication. Unauthorized access to AD information is mitigated by regular system scans and reviews of the VA network 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. Example parameters shared between the VA MS AD IS, Exchange, PIV and M0365:

**Network Identification:** Network log on to identify user and VA Domain

**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 **VA MS AD Assessing Information System** is used solely to identify individuals 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 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.

Add answer here:
The active management of Directory Service VA MS AD accounts will enable VA to remove personnel that no longer require access and account management features provide for additional security including the ability to change passwords or re-create accounts if needed for security reasons. This will ensure that unauthorized access to records is a low risk. The VA requires employees and contractors to complete and sign the VA Privacy and Information Security Awareness and Rules of Behavior training prior to initial access and annually thereafter. All requests for access require an access request approved by the supervisor or designee. Additionally, all VA employees and contractors must take Annual Government Ethics & Privacy and HIPAA Focused annual training. The “Privacy and HIPAA 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 created and maintained in the VA MS AD Information Systems in order 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. 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.

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 maintained as long as users are approved to actively using the VA network and email. If a user leaves VA and no longer requires access, VA personnel will be 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). Backups are performed on the VA MS AD IS accounts; accounts can be restored within 15 days. An account can be recovered natively by the MS operating system 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 for the VA MS AD IS, the VA Directory Services Teams follow guidelines established in the NARA-approved Department of Veterans’ Affairs Record Control Schedule (RCS)-10 (http://www1.va.gov/vhapublications/rcs10/rcs10-1.pdf); Department of Veterans Affairs, Office of Information & Technology RCS 005-
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 backups never leave control of the VA, retention is for 15 days of AD data at which time the information is “tomb stoned”. 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 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 user account could be stored longer than necessary to accomplish the mission.

**Mitigation:** Information is purged after 15 days on the VA MS AD 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. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

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

Data Shared with Internal Organizations

<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 data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Office of Inspector General (OIG)</td>
<td>Yearly auditing and assessments</td>
<td>Custom reports for user activity and review</td>
<td>Electronically encrypted Approved Queries</td>
</tr>
<tr>
<td>Veterans’ Health Administration</td>
<td>MO365</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</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 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) project using FIPS compliant approved devices</td>
</tr>
</tbody>
</table>

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:** Logical MS connector to VA Microsoft Exchange and M0365 Assessing projects as a forwarding agent; and VA network access authentication validation agent may be a risk if access control lists are not enforced. There is also risk that information shared with the OIG could be accessed by an unauthorized party while it is in transition.

**Mitigation:** VA internal and gateway network firewalls, “routing traffic cops” to prevent packets in or out from the VA MS AD IS forwarding agent used approved ports/protocols and enforced access control lists. Data shared with the OIG is secured with access controls and those who access it at the OIG are required to go through VA security and awareness training. OIG group accounts are tracked through Change Auditor; and traffic is 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:** This question is #7 in the Privacy Threshold Analysis.

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

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

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

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

The information stored within the VA Microsoft Active Directory Environment is created for internal VA purposes only and it is not routinely shared with any agency or organization outside of the VA. However, data stored within the system are considered electronic public records which may be used to search for relevant information in the event of a Freedom of Information Act (FOIA) request or as part of the discovery process in a legal case the VA is a part of. In the event that information is shared outside of the VA, it will be pursuant to a FOIA request or discover in a legal case. All FOIA requests are governed by The Freedom of Information Act, 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048. Any disclosures made in relation to a legal case are governed by the Federal Rules of Civil Procedure (Fed. R. Civ. P.) 26-37.
### Data Shared with External Organizations

<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 data element types such as PII/PHI that are shared/received 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>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

### 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:** There is a risk that data shared with DoD or legal discovery request such as a FOIA request may contain Personally Identifiable Information (PII); e.g.; username(s) not specified in the FOIA or is not relevant to the legal case.

**Mitigation:** User Access Control mitigates the availability to internal employees when processing a FOIA request. AD information normally is not transmitted and or shared with external agencies outside of the VA control by default. Anonymous activity to information in AD is not possible without a credentialed account on the domain. Domain Controllers log all credentialed logons to the VA domain. Anomalous behavior is logged, and automatic alerts are generated.
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 for employment, employees, contractors and affiliates. This notice is on OMB Form No. 2900-0673 and VA Form 9957 REQUEST FOR PERSONAL IDENTITY VERIFICATION (PIV) CARD. Please see the notice below on a VA PIV Card Application Form.

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 where 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.

The System of Record Notice (SORN) Identification (ID) #145VA005Q3 for the Department of Veterans Affairs Personnel Security File System (VAPSFS) is the applicable reference provided from the PIA Support Team on this Information System. The VA AD Information System is the approved commercial off the shelf application software system to create an enterprise network account with basic employee data (name, email, location, phone number). The AD system has a subset of employee work data; it is not all inclusive.

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 as part of the VA MS AD IS is basic user data for access to the VA network and email. 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

The VA MS AD system is not an authoritative system and does not provide a means for consent. The data collected is basic employee data (name, location, phone number) 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 VA user accounts to access the network could be accessed by someone with elevated permissions who does not have a need to know.

**Mitigation:** Anonymous access to information in the AD is not possible without a valid credentialed account and 2FA. The VA MS AD Domain Controllers log all credentialed logons to the VA domain. Anomalous behavior is logged, and alerts are generated. Change Auditor, server logs and monitoring provide evidence of access even of individuals with elevated permissions or external hackers.

**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.
Authenticated users can query their own information for inaccuracies or updates. A help desk work ticket through ServiceNow or YourIT can be submitted to correct VA owned information.

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 AD system can query their own information for inaccuracies or updates. A help desk service ticket 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 Veterans Affairs Personnel Security File System (VAPSFS) is the applicable reference provided from the PIA Support Team on the MS AD Information System. The employee information in AD is used to create an enterprise network account. AD is a subset of employee data (name, email, phone, location); it’s not an all-inclusive employee data 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.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.
Authenticated users of the AD system can query their own information for inaccuracies or updates. A help desk service ticket through ServiceNow or YourIT can be submitted to correct VA owned information. Please note: The VA MS AD Information System is 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 system is not possible without a valid credentialed account. Domain Controllers log all credentialed logons to the VA domain. Anomalous behavior in the AD Information System is logged and 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 of the AD IS, VA network and email 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 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, VA contractors will need access to the VA network and email through the VA MS AD IS to authenticate 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) and set to expire upon the contract end date automatically disabling the contractor’s access.
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) 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 date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. 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.

VA Microsoft (MS) Active Directory (AD) Assessing was granted full Authority to Operate (ATO) approval on 09/14/2020 for 180 days. The current expiration is 03/13/2021. This system is categorized as High impact.
### 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>
</tbody>
</table>

Section 9. References
<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<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>
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).

Signature of Responsible Officials

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

RITA K GREWAL
114938

Digitally signed by RITA K GREWAL 114938
Date: 2020.09.30 13:00:51 -04'00'

PO, Rita Grewal

Mary K Jones
185798

Digitally signed by Mary K Jones 185798
Date: 2020.09.30 10:12:33 -04'00'

Information Security Systems Officer, Mary K. Jones

James E. Gunter
1722289

Digitally signed by James E. Gunter 1722289
Date: 2020.09.30 09:28:59 -05'00'

System Owner, James E. Gunter