Privacy Impact Assessment for the VA IT System called:

Veteran's Affairs (VA) Enterprise Mobility Management - Cloud Assessing (VA EMM)

Veterans Affairs Central Office (VACO)

Mobile Technologies and Endpoint Engineering

Date PIA submitted for review:

03/10/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.Facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	James Boring	James.boring@va.gov	215-842-2000
Information System Owner (ISO)	Punit Patel	Punit.patel@va.gov	331-588-5355

Abstract

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

VA Enterprise Mobility Management (VA EMM) (formally MDM) is an implementation of AirWatch, a commercial off-the-shelf (COTS) enterprise mobile device management software solution. VA EMM provides the ability to deploy approved security profiles onto GFE mobile devices used by VA staff and veterans. These mobile devices (such as tablets and smartphones) are used to execute a variety of VA Mobile applications. The security profiles allow enforcement of the VA security settings and policies on these mobile devices to ensure the integrity and security of the device and data being processed. Additional features include the ability for VA authorized personnel to remotely wipe mobile devices that are reported lost or stolen. VA EMM has one authorized connection to a system outside the VA – the Department of Defense (DoD) DHA (Defense Health Agency); services are limited to Public Key Infrastructure (PKI) Certificate Authority (CA) issuance and software whitelisting/compliance tools. Only VA authorized Office of Information Technology (OI&T) personnel are granted access to VA EMM.

Overview

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

1 General Description

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

VA Enterprise Mobility Management – Cloud Assessing (VA EMM) – Office of Information Technology (OIT)

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

VA EMM's business purpose is to provide FIPS-compliant Authentication and Access services to VA mobile devices for employees throughout the Enterprise. VA EMM directly supports the OIT mission of providing secure connection mechanisms for Identity, Credential, and Access Management (ICAM) solutions for mobile VA devices.

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

OIT and Mobile Technology and Endpoint Engineering

2. Information Collection and Sharing

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

VA EMM serves over 150K VA employees across the Enterprise by managing ICAM services on VA mobile devices. No personal information is stored or collected by the system.

VA employees use their issued mobile devices to scan 'QR Codes' to receive Public Key Infrastructure (PKI) certificates from external Certificate Authorities (CA's). These PKI certificates are tied to Users' VA Personal Identity Vehicle (PIV) and serve to authenticate VA employees into the device and network. Typical Users include VA healthcare providers (doctors, nurses, etc.) with valid VA Active Directory (AD) accounts.

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

VA EMM provides the ability to deploy approved security profiles onto Government Furnished Equipment (GFE) mobile devices used by VA staff and veterans. These mobile devices (such as tablets and smartphones) are used to execute a variety of VA and Commercial-Off-The-Shelf (COTS) Mobile applications. VA employee Usernames are collected and attached to their assigned mobile device for security compliance tracking and continuous monitoring.

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

No VA EMM User information is shared with other systems; ICAM services are shared with 'Lookout-f' and 'Electronic Health Record Modernization – Mobile Application Platform' (EHRM) through an Interservice Connection Agreement (ISA) and Authority to Connect (ATC) with the Defense Health Agency (DHA). Lookout-f provides software whitelisting for mobile devices; EHRM utilizes VA EMM's Certificate Authority (CA) and whitelisting services.

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

N/A – VA EMM is hosted entirely within the VA Enterprise Cloud (VAEC).

3. Legal Authority and SORN

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

A SORN is not required for this system because there is no User information to retrieve based on device Hostname (VA Username/Email). Traffic is limited to SSL TCP passing host-based security services (HBSS) from EMM (VAEC) to the VA mobile devices (operating on the VAEC network). The VA EMM ATO Memo is the legal authority form the VA AODR, dated 23 Apr 2021, for legal-authority evidence to operate the system within the VAEC.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

N/A – VA EMM does not require a SORN. Per VA guidance from https://www.oprm.va.gov: "A system of records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual." No PII/PHI is attached to the mobile device hostname or the Users' names, nor can any be accessed within the VAEC and EMM boundaries. VA Active

Directory User profiles are not linked, and EMM is not responsible for any PHI/PII VA employees (i.e. healthcare providers) upload to the mobile device's internal storage.

D. System Changes

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

All business changes to VA EMM prompting the execution of this PIA have been reviewed and approved by the VA Authorizing Official (AO) and the Information System Owner (ISO) through attestations described in the EHRM/DHA Interservice Connection Agreement (ISA) and Authority to Connect (ATC) Memo available in eMASS. Changes include additional device tracking and documenting persistent DHA connections.

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

N/A – no further changes are being made to accommodate the DHA/EHRM Interservice Connection.

Section 1. Characterization of the Information

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

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

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI),

Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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

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

VA email address, Media Access Control (MAC) of mobile device.

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

PII Mapping of Components (Servers/Database)

Veteran's Affairs (VA) Enterprise Mobility Management (EMM) (Cloud) Assessing consists of approximately three dozen virtual components (databases and load balancers controlled through Amazon Web Services (AWS) Application Programming Interface (API). Each component has been analyzed to determine if any elements of that component collect PII, which they do not – Business Rolodex only. The type of PII collected by VA EMM (Cloud) Assessing and the reasons for the collection of the PII have already been identified. Types of servers include SQL 2016 - 2019, RHEL 8, and MS Server 2019.

PII Mapped to Components

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A	N/A	N/A	N/A	N/A	N/A

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

VA employees with valid PIVs; Email Address Internet Protocol (IP Address, mobile device Media Access Control (MAC) address, Name, VA Domain Account.

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

N/A – VA EMM does not utilize other (outside VAEC) sources of information for the establishment and monitoring of mobile device user accounts or data.

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

VA EMM can generate security compliance reports for every VA mobile device under its purview.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

VA EMM receives information via electronic transmission from the Certificate Authority (currently Entrust) that a valid, PIV-possessing VA employee has requested a new DigiCert PKI certificate; VA EMM then updates access lists for those devices.

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

N/A

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

- There is a synchronous relationship between VA Health systems. The systems write the data to both the primary and to the secondary area at the same time. In doing this, the data remains completely current and identical. The process works quickly and there is a extremely small margin of error. Because of this, it is ideal for disaster recovery and is the method preferred for projects that require absolutely no data loss.

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

N/A

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

5 U.S.C. 552, "Freedom of Information Act," c. 19675 U.S.C. 552a, "Privacy Act," c. 197418 U.S.C. 1030 (a) (3), "Fraud and related activity in connection with computers."38 U.S.C. 218, "Security and law enforcement on property under the jurisdiction of the Veterans Administration OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)Federal Information Security Management Act (FISMA) of 2002OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of2002Executive Order 13103, Computer Software Piracy FIPS 199, Standards for Security Categorization of Federal Information and Information Systems FIPS 200, Minimum Security Requirements for Federal Information and Information Systems FIPS 201-1, Personal Identity Verification of Federal Employees and Contractors FIPS 140-2, Security Requirements for Cryptographic Module

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The only PII is Business Rolodex (name and email) that ties to a Public Key Infrastructure (PKI) certificate used for VA mobile device authentication and non-repudiation. There

is no privacy risk to the User or the VA should a device be publicly traced to a specific User through the utilization of PKI certificates; the encryption system is designed to be publicly visible and traceable through a chain of trust.

Mitigation: VA EMM adheres to information security requirements instituted by the VA Office of Information Technology (OIT). VA EMM implements cryptography that is compliant with federal laws and regulations i.e., Federal Information Processing Standard (FIPS) 140-2. Any deviation from Federal requirements will be documented in a Risk-Based Decision Memo and approved as a long-term managed risk by VA management. VA employees and contractors with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

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 Rolodex: 1) Name; 2) Email address; 3) Device MAC address. Used to correctly identify the mobile application user and approved device. VA Employee and VA Contractor's names and email addresses are used to create accounts for environment administration (HBSS).

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

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

Information collected is utilized by Authentication and Authorization (A&A) services of Active Directory (AD) and mobile applications in both the pre-production/production application environments. Entrust PKI certificates are used in collaboration with PIV-D credentials and matched to the AD account of the user for non-repudiation.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

- New User information may include name and PKI certificate changes; these are made automatically when the User requests a new DigiCert certificate from the CA (Entrust). Employee name changes are made through the Office of Information Security (OIS) and new PIV credentials issued and stored in VA AD.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

- SSL encryption on all transmissions outside the accreditation boundary; FIPS-compliant encryption on all virtual Amazon Web Services (AWS) S3 storage buckets.

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

- N/A – VA EMM does not process SSNs.

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

- PII of VA employees is protected through the issuance of a user ID, User-generated private key (i.e., 'PIN'), and the VA Personal Identity Verification (PIV) card itself. This ensures the identity of the user by requiring two-factor authentication to the mobile device. Information stored on the device by VA employees is protected by the aforementioned ICAM resources and Lookout-f software whitelisting.

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

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***<u>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.</u>***

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

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

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

2.4a How is access to the PII determined?

- All employees and contractors with access to VA EMM are required to complete the VA Privacy and Information Security awareness training and rules of behavior annually; must possess valid VA PIV AD accounts.

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

- Please reference 'Active Directory User Account Management SOP_(April2022)' in eMASS for a complete description of how VA EMM privileged-User support personnel gain system access.

2.4c Does access require manager approval?

Yes

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

- Yes

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

- VA EMM Information System Security Officer (ISSO)

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

- VA Employee and VA Contractor's names and email addresses are used only to create an account for environment administration (HBSS). Names are used to correctly identify the mobile device user. VA Employee and VA Contractor's email addresses are used to create accounts for environment administration. Media Access Control (MAC) address are used to ID/track devices.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

• Retains PII (name and account information) for the minimum amount of time to fulfill the systems purpose or as required by law; dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and use approved records disposition schedules to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA Records Officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes, NARA requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization.

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

No records are stored by VA EMM; device MACs are tied to VA employee usernames/emails and are Business Rolodex only. Username, email, and device MAC records are maintained until the employee PIV card is revoked or disabled (after-which OPS stores them for 2 months as Access Control User Profile Records). MAC addresses are re-assigned to other Users as required. VA EMM

is not responsible for the data stored on the mobile devices it monitors, only Host-based Security Services (HBSS) and ICAM services helping to implement VA compliance policy.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

N/A

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

Yes, PII is used solely for production applications support to Veterans and providers. All test systems use test data that is not comprised of PII or PHI.

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

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

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

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

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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: The information is necessary to accomplish the purpose of Mobile Device Management implementation. It's possible that VA account credentials may be released to unauthorized individuals.

Mitigation: VA Employee and VA Contractor's names and email addresses are used only to create an account for environment administration. Any deviation from Federal requirements will be documented in a Risk-Based Decision Memo and approved as a long-term managed risk by VA management. VA employees and contractors with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
N/A	N/A	N/A	N/A

VA EMM does not share information internally.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: No risk associated with internal sharing of information.

Mitigation: N/A

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Lookout -f	Software Whitelisting/Device protection	Mobile Device MAC	ISA/MoU/BAA	TCP encrypted transmissions
Entrust	PKI CA	VA employee email; PKI certificates	ISA/MoU/BAA	TCP encrypted transmissions

EHRM (DHA/CERNER)	Software Whitelisting/Device protection; PKI CA	Mobile Device MAC; PKI Certificates	ISA; ATC	TCP encrypted transmissions

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: VA EMM is designed to use the PKI infrastructure for authentication and non-repudiation services to the VA mobile community, which 'shares' User account credentials with Entrust and Lookout external services tied directly to a PKI Certificate Authority (CA) and VA EPMO AD credentials. The only truly 'private' information in this system shared between the two aforementioned external connections is the Users' 'private key' (i.e., VA PIV-D PIN), which is encrypted with AES over a dedicated SSL connection to Airwatch, Entrust, and Lookout authentication and whitelisting servers hosted within their respective secure data centers (or secure contractor offices). Possible risks of this secure relationship include certificate spoofing, session hijacking and man-in-the-middle attacks. These risks are virtually eliminated by having a secure, dedicated (not dynamic) SSL connection to the CA source servers with PKI AES FIPS-compliant encryption requiring a private key (PIN) to decrypt the session before it can be established. Without the Users' VA PIV-D public key and private PIN, the connection will be refused, and access denied.

Mitigation: 24/7 automated intrusion alerts monitored by VA CSOC, VAEC, and SBG EMM OPS. Alerts are generated through 'deny all/except . . .' policies configured on virtual load balancers and Intrusion Detection Systems (IDS) and emailed to assigned support members. Furthermore, VA policy mandates the use of only U.S. Treasury-approved Certificate Authorities (CA's) for the purposes of verifying identity and ensuring non-repudiation in all digital communication. VA EMM possesses a defined Certificate Manager (CM) role dedicated to maintaining accurate and up-to-date certificate authorities and repositories. This role manages the revocation of revoked, denied, or expired certificates to maintain authenticity in all identity management solutions for VA EMM.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

Yes. All EMM-protected mobile Users are VA employees and must have accepted all VA-required Privacy Notices prior to receiving their VA PIV. Reference 'Outlook Mobile Setup O365 With Derived Credentials.pdf' in eMASS for step-by-step mobile device enrollment procedures all VA Users must follow for activation.

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

PRIVACY ACT STATEMENT: Use of VA Licensed Software by you may involve the collection of individually identifiable data that is entered into the Application and data about your use of the Application. As authorized by 38 U.S.C. Section 501, <https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=401&FType=2>, VA is asking you to provide information via this Application which may be included with other information VA uses to deliver health care to you.

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

- PRIVACY ACT STATEMENT: Use of VA Licensed Software by you may involve the collection of individually identifiable data that is entered into the Application and data about your use of the Application. As authorized by 38 U.S.C. Section 501, <https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=401&FType=2>, VA is asking you to provide information via this Application which may be included with other information VA uses to deliver health care to you.

- VA may disclose the information that is entered into the Application as permitted by law.

- VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the Veterans Health Administration (VHA) Notice of Privacy Practices.

- VHA will explain these routine uses and privacy practices upon further request.

Providing the information is voluntary. Failure to furnish your identifying information (username and login) when required by an application will prevent you from being able to use the Licensed Software but will not have any effect on any other benefits or care to which you may be entitled. VA may also use this information to identify users of the Licensed Software, and for other purposes authorized or required by law.

- The Licensed Software transfer of individually identifiable data will use secure methods to transmit the data. Data collected by the Licensed Software for patient care purposes will be securely transmitted into VA data systems to be stored as part of your health care records covered under a Privacy Act system of records.

- DATA USE: Data resulting from the use of the Licensed Software will be made available to VA authorized persons in the conduct of their official business. Data may be used for statistical and management purposes in assessing the benefit of this software. Data provided for research purposes will be made anonymous so that it is not personally identifiable. This Privacy Impact Assessment (PIA) serves as notice of system inheritance and compliance with the AWS GovCloud VAEC infrastructure. As required by the eGovernment Act of 2002, Pub. L. 107–347 §208(b) (1) (B) (iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

All Users must click an 'accept' button when enrolling their mobile device for the first time (see 'Outlook Mobile Setup O365 With Derived Credentials.pdf') and authenticate with their PIV in order for their VA account to operate correctly on the VA mobile device assigned to them.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Yes. VA mobile device access will not be possible. Single-sign on then caches the response so the User is not presented with the same Privacy notice the next time they login.

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.

Consent grants access to the mobile device using the AD profile of the VA User. No granularity is applicable, it's just access. Lookout-f and EMM whitelisting hardens each mobile device according to VA Handbook 6500 and National Institute of Standards in Technology (NIST) guidance, recommendations, and best practices.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk: Using VA usernames (i.e., network logon) and email addresses for ICAM services on assigned (or unassigned, i.e., shared) mobile devices presents hostile actors using network traffic sniffers with a consistent list of VA logons (sans PIV's and private keys). Although no access to VA systems would be granted just by knowing a user's logon, full names of VA employees with mobile devices protected by VA EMM ICAM and HBSS services could be made available to the general public.

Mitigation: The VA mobile network is encrypted and passes through a Trusted Internet Connection (TIC) – the VAEC. Network sniffing or username tagging is not possible from outside the mobile environment. Insider threats make the risk of username tagging more likely.

Section 7. Access, Redress, and Correction

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

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Public Key Infrastructure (PKI), by its nature, is public-facing. A User's public key is already publicly available. Private keys (i.e. PIN numbers) are the property of the user and not subject to FOIA or Privacy Act practices. All other EMM platform services utilize no PII/PHI and are comprised of internal VAEC network and infrastructure-related components only.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

N/A – VA EMM is exempt from the access provisions of the Privacy Act because there is no Privacy information to store or share; HBSS data (system scans, continuous monitoring logs, etc.) is the property of VA OIT; FOIA requests can be made through that office. PKI certificates tied to VA user accounts are already publicly available, per the design of PKI and identity non-repudiation.

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

Access is dependent upon valid VA employment with a functioning PIV. An individual could request HBSS information for their device: access attempts, security and app updates applied, blocked app installs, etc. This request would not be made to VA EMM, but to the local IT Admins managing the device at the VA installation, who would then contact VA EMM Tier 1 support to make the formal request. These procedures are not documented.

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.

N/A

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.

N/A

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

N/A

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

Authentication and authorization are used to determine access to all systems within VA EMM. VA staff or veteran information collected is only utilized for pre-production/production mobile application purposes. VA-managed AD provides the user management of all VA EMM administrative/operations users. All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

N/A – Other agencies do not have access to VA EMM.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Please see the VA EMM Configuration Management Plan (CMP) in eMASS for a complete description of access control and other ICAM responsibilities.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes. Contracts are reviewed annually by the Contracting Officer or Contracting Officer's Technical Representatives to ensure that security requirements and security specifications are explicitly included in the information systems and information system support service acquisition contracts. In addition, contracts contain the appropriate security language necessary for compliance with FISMA and 38 U.S.C 5721-28 and provide adequate security for information and information systems used by the contractor. All VA contractors are required to sign Non-Disclosure Agreements (NDA's) prior to receiving access to the system and working on the project. Contractor involvement will include System Administration of the database servers that house the PII Business Rolodex information.

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.

VA requires Privacy and Information Security Awareness training be completed on an annual basis. The Talent Management System offers the following applicable privacy courses: VA 10176: Privacy and Information Security Awareness and Rules of Behavior.

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

Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* Active and current as eMASS export
2. *The System Security Plan Status Date:* 01 Apr 2021
3. *The Authorization Status:* ATO - Full
4. *The Authorization Date:* 23 Apr 2021
5. *The Authorization Termination Date:* 22 Apr 2024
6. *The Risk Review Completion Date:* 19-Apr-2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

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

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

Section 9 – Technology Usage

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

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

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

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

Yes - VAEC

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

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.

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.

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).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.05.02 15:05:24 -04'00'

Privacy Officer, Tonya Facemire

JAMES BORING

Digitally signed by JAMES BORING
Date: 2023.05.02 15:38:40 -04'00'

Information System Security Officer, James Boring

Punit V Patel 318371

Digitally signed by Punit V Patel 318371
Date: 2023.05.02 14:22:08 -05'00'

Information System Owner, Punit Patel

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).

Outlook_Mobile_Setup_O365_With_Derived_Credentials.pdf

Please see Entrust Mobile O365 Enrollment Instructions 'Outlook Mobile Setup O365 With Derived Credentials.pdf' in eMASS for all EMM-specific system notices presented to VA EMM mobile device Users upon first enrollment of a device.

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices