Privacy Impact Assessment for the VA IT System called:

VA Emergency Alerting and Accountability System (VA EAAS)

VA Central Office (VACO)
Human Capital Services Center (HCSC)

Date PIA submitted for review:

5/8/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.Drake@va.gov	202-632-8431
Information System Security Officer (ISSO)	Joseph Guillory	Joseph.Guillory@va.gov	619-204-6840
Information System Owner	Shannon E. Jones	Shannon.Jones1@va.gov	202-461-6176

Abstract

The VA Emergency Alerting and Accountability System (VA EAAS) is an enterprise-wide system used for alerting and accountability purposes. The system is a method to send rapid, reliable, and widespread notifications and collect the safety status of all VA employees, contractors, and affiliates in times of an emergency. The method is to provide leadership situational awareness of all personnel safety status, safety notifications to employees, and provide actionable intelligence to leadership through data analysis and compilation.

Overview

1 General Description

A. The IT system name and the name of the program office that owns the IT system.
VA EAAS is owned by HCSC

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
VA Emergency Alerting and Accountability System Assessing sends rapid, reliable, and widespread notifications and collect the safety status of all VA employees, contractors, and affiliates in times of an emergency. The method is to provide leadership situational awareness of all personnel safety status, safety notifications to employees, and provide actionable intelligence to leadership through data analysis and compilation. VA requires a scalable, flexible tool that will: (1) enable the notification of incidents of an emergency nature to employees, contractors, affiliates and associates of sub-groups at the lowest level appropriate through multiple communication venues (e.g. email, cell phone, land line, SMS text, pager, mobile app, and desktop popup); (2) generate reports of employees and contractors who have and have not responded; (3) allow designated personnel to monitor/manage select groups of employees/contractors. VA EAAS is a SaaS platform hosted by the vendor (Blackberry AtHoc) with FedRAMP classification of Moderate. The BlackBerry AtHoc has a small module that integrates with VA Active Directory (AD) and resides within the VA network to pass AD data to the VA EAAS hosted solution.

C. Indicate the ownership or control of the IT system or project.
VA EAAS is owned by HCSC. All contracts, communications with the BlackBerry vendor, and project backlog are owned and managed by HCSC.

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 EAAS supports up to 600,000 VA employees, contractors and affiliates.

E. A general description of the information in the IT system and the purpose for collecting this information.
VA EAAS identifies up to 600,000 VA employees, contractors and affiliates to obtain names, work address, work email, work phone, work cell (GFE), computer login username, IP address and employeeID from the AD. VA EAAS will also maintain the following personal information from the individual: home phone, personal cell phone, personal email, emergency contact information and home address. The information is used to contact personnel when alerts are generated by the system.

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

The AD is considered the authoritative and accurate source for work-related identity information. VA EAAS will identify up to 600,000 VA employees, contractors and affiliates to obtain names, work address, work email, work phone, work cell (GFE), computer login username, IP address and employeeID from the AD. VA EAAS will also maintain the following personal information from the individual: home phone, personal cell phone, personal email, emergency contact information and home address. Personal contact information is mandatory per VA Directive 0325. The information is held while the employee, contractor or affiliate is with VA. Once the employee, contractor or affiliate is no longer in VA and their AD information is inactive, the VA EAAS account for the individual will be disabled to prevent further notifications. All accounts disabled for 30 days or more will be deleted from the system. A small User Synch Module that integrates with AD resides within the VA network and passes AD data to the VA EAAS hosted solution, the BlackBerry-hosted system, via HTTPS outbound web services requests. VA EAAS does not share data with any other internal or external system.

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.

VA EAAS is VA's enterprise tool for emergency notification and accountability. As such, it is available to users across VA. The tool is web-based and all data is centrally managed by the SaaS.

3. Legal Authority and SORN

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

189VA006H/86 FR 66620 - VA Emergency Alerting and Accountability System (VA EAAS) – VA (11/23/2021) https://www.govinfo.gov/content/pkg/FR-2021-11-23/pdf/2021-25509.pdf

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: The authority which the system of records will be maintained includes: (a) Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements. January 17, 2017. (b) Federal Continuity Directive 2 (FCD 2), Federal Executive Branch Mission Essential Functions and Candidate Mission Essential Functions Identification and Submission Process, June 13, 2017. (c) National Security and Homeland Security Presidential Directive (National Security Presidential Directive NSPD 51/Homeland Security Presidential Directive) HSPD–20, May 4, 2007. (d) VA Directive 0320 VA Comprehensive Emergency Management Program, August 13, 2012. (e) VA Handbook 0320 VA Comprehensive Emergency Management Program, March 24, 2005. (f) VA Directive 0323 VA Continuity Program, November 5, 2010. (g) VA Directive 0325 Department of Veterans Affairs Personnel Accountability, October 8, 2020.

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?

No major updates to the VA EAAS system are currently planned that would require SORN update.

D. System Changes

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*
No changes to business processes are anticipated.

K. *Whether the completion of this PIA could potentially result in technology changes*
No changes to technology are anticipated.

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)

work address, work email, work phone, work cell (GFE), computer login username, IP address and employeeID.

PII Mapping of Components (Servers/Database)

VA EAAS consists of two key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VA EAAS and the reasons for the collection of the PII are in the table below.

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
BlackBerry AtHoc Software as a Service (https://alerts7.athoc.com, https://delivery.athoc.com, https://delivery2.athoc.com, https://mobile.athoc.com)	Yes	Yes	Names, work address, work email, work phone, work cell (GFE), computer login username, employeeID, computer IP address, personal email, home phone, personal cell, text number, home address, and emergency contact name and number.	For the sole purpose of alerting and collecting personnel accountability safety status during an emergency.	FedRAMP 3PAO Accreditation, role-based access for VA employees that is controlled by the VA system owner.

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.

The VA EAAS collects information from AD and individual employees. The BlackBerry AtHoc User Sync Client is installed on the VA network and maintains an AD Sync on a daily recurring basis. By automation, the query of the AD database provides VA EAAS minimal data fields: names, work address, work email, work phone, work cell (GFE), computer login username, IP address and employeeID. All information is used to create accounts or update/delete accounts, as needed. If the BlackBerry AtHoc desktop client is installed on a VA workstation, it will collect the workstation IP address for the purpose

of computer desktop notification. VA Directive 0325 mandates employees are required to provide personal contact information.

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.

The VA EAAS obtains information from AD to create new accounts for new employees, or updates as AD changes are made, and deletes accounts for employees no longer in VA. Ensuring the accounts are created, updated, and deleted on a timely basis ensures an employee is able to receive a safety or emergency message/alert. It also ensures prior VA employees are removed from the database to prevent further notifications.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
VA EAAAS does not create information.

1.3 How is the information collected?

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

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

Data is collected in VA EAAS via synchronization with AD . Data synchronization is executed by the User Synch Module that resides within the VA network. All data collected from VA is transmitted outbound to the hosted services using industry-standard HTTPS encryption. Employees may also update their contact information in VA EAAS via a web-based Self-Service portal.

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.

VA EAAS does not utilize any forms in the collection of data.

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.

The AD is the considered authoritative and accurate source for work-related information. It has data fields to identify active or inactive VA accounts and whether a person has a name, username, or location change. Using this information, VA EAAS will be able to: (1) create new accounts for newly created AD accounts; (2) update accounts; (3) moves an account from one location to another for any transferring employees; and (4) disable or delete accounts based on the AD inactive status indicators. Also, there are VA EAAS administrators who are assigned permissions to view, edit, or delete accounts. The accounts that have access are restricted to the level necessary to successfully complete their tasks as emergency managers / coordinators, HR specialists, Safety Officers/Chiefs, etc. Directive 0325 states employees shall review and update their contact information on a quarterly basis. The administrators of the system will send reminders to their facility employees to update their contact information. Device information that is supplied by users (i.e. home phone number) is validated against a rule set built into the VA EAAS software to make sure that the device addresses conform to known formats before saving into the database. If the user still manages to input an invalid address, when an alert is published to that address, it will error when attempting to deliver to that address and flag it as unreachable in the VA EAAS alert delivery reports. VA EAAS operators will then be able to retrieve the report and review it for unreachable addresses and take appropriate action with this information.

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.

VA EAAS does not perform checks for accuracy through the use of commercial information aggregators.

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

1. Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements. January 17,2017
2. Federal Continuity Directive 2 (FCD 2), Federal Executive Branch Mission Essential Functions and Candidate Mission Essential Functions Identification and Submission Process, June 13, 2017
3. National Security and Homeland Security Presidential Directive (National Security Presidential Directive NSPD 51/Homeland Security Presidential Directive HSPD-20, May 4, 2007
4. National Incident Management System (NIMS) doctrine, October 2017

5. National Response Framework (NRF), May 2013
6. VA Directive 0320 VA Comprehensive Emergency Management Program, August 13, 2012
7. VA Handbook 0320 VA Comprehensive Emergency Management Program, March 24, 2005
8. VA Directive 0323 VA Continuity Program, November 5, 2010
9. VA Directive 0325 Department of Veterans Affairs Personnel Accountability, November 27, 2013

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: Information in VA EAAS may not be accurate, relevant, complete, and current.

Mitigation: The majority of information within VA EAAS is derived via synchronization with AD. The AD is an authoritative data source for VA. The only VA data that is synchronized to VA EAAS is contact information and organizational hierarchy data that facilitate delivery of alerts. The AD data is synchronized automatically on a daily basis, ensuring that any new, changed, or deactivated/deleted information from AD is mirrored within VA EAAS. In addition, every individual within VA can access their VA EAAS user profile via a Self-Service portal to update certain data elements.

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.

The information that VA EAAS synchronizes from AD, and that End Users can update via Self-Service, enables the system to send notifications to all VA employees, contractors, and affiliates in times of an emergency.

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.

1. Name – First, middle and last name and suffix are used to identify personnel accounts in VA EAAS.
2. VA Login Username – Used to identify recipients for an alert. Also used to verify someone's identity before granting access into the system.
3. Employee ID - Used to identify and match AD account to VA EAAS account during the User Synch data synchronization process.
4. Work / Home Address – Used to determine a population in an area affected by an emergency.
5. VA / Personal Email Address – Used to send alerts and messages.
6. Phone numbers (home/work phone and cell) – Used to send alerts and messages.
7. IP Address – Used for security auditing purposes and to identify workstations for the purposes of sending computer desktop popups.
8. Emergency Contact Information (Name, Phone Number, etc. of a different individual) – used by supervisors or emergency managers. An emergency contact is the designated person which supervisors will get in touch within an emergency at the workplace.

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

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

The VA EAAS provides the capability to pull the following reports indicated below. The information provided in each report is noted.

1. VA EAAS End User Manager Page: Provides authorized users the capability to view all personnel within their assigned office. User profiles are viewable and editable (if given

appropriate user permissions). Authorized users can manage all personnel profiles as needed from this page.

2. VA EAAS Alert Reports: There are several alert reports available in VA EAAS to provide situational awareness of an alert (i.e. number of targeted populations, number of sent messages, number of received messages, number of responses, if required, and how each person responded, error codes, etc.).

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.

Reports that can be generated from VA EAAS pertain to the status of alert messaging, as well as details on organizational units. Any details on specific users primarily relate to the success or failure of messaging to the person. Only application Administrators can generate a report in VA EAAS and they are the only individuals that can view them in the system. Reports do not affect user records. Records are not generated from reports.

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?

VA data from AD that is synchronized to the VA EAAS SaaS is transmitted to the hosted services using industry-standard HTTPS encryption. That data, in addition to user contact information that is entered via the Self-Service web portal, is stored in the BlackBerry AtHoc encrypted SaaS database.

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

VA EAAS does not contain SSN data.

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

The Blackberry AtHoc FISMA Moderate-Impact Cloud Hosting Environment, owned by Blackberry AtHoc is Federal Risk and Authorization Management Program (FedRAMP) Authorized as a SaaS service, in a hybrid cloud deployment model at the moderate impact level, certified per NIST SP 800-53 Rev 4 (at a moderate FIPS 199 classification). These certifications go beyond the typical SAS 70 Type II / SSAE 16 SOC 2 certification to include actual assessment of service security provisions:

- Continuous monitoring (per latest federal mandates)

- Security scans and hardening compliant with DISA (Defense Information System Agency) STIGs (Security Technology Implementation Guides)
    - Facility and system inspections
    - Contingency / Failover testing
- Secure communications using BlackBerry AtHoc U.S. Cloud Services has been certified and accredited through the Defense Information Assurance Risk Management Framework (DIARMF) by all Military Services (Army, Navy, Air Force and Marines)

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to PII is determined by the need to notify employee, contractor or affiliates during emergency situations. VA Directive 0325 identifies roles and responsibilities including individuals who can gain into VA EAAS. Any administrator requiring access to send notifications or manage user accounts are required to complete VA EAAS training prior to receiving authorized access. Additionally, employee, contractor or affiliate are required to complete annual training for VA Privacy and Information Security Awareness and Rules of Behavior (ROB) and VA Privacy. Employees, contractors and affiliates are required to agree to all rules and regulations outlined in the trainings, along with any consequences that may arise for failure to comply.

VA EAAS administrators and operators will be a combination of Emergency Managers, Safety Officers or Safety Division Chiefs and Human Resources liaisons. Roles are not specific to any position or function. The roles are given based on the specific need for the Administration, Staff Office, or facility to notify staff members of emergency situations.

All roles and user types are provided below:

End User: End Users can access the details of their own individual records via the Self-Service web portal and perform updates to certain contact and organization data elements

within the record. End Users cannot access any other records within the system and cannot access any of the system alerting or reporting functionality.
End User Manager: An Operator with privileges to manage end user accounts.
Distribution Lists Manager: An Operator with privileges to manage distribution lists.
Draft Alert Creator: An Operator with privileges to create and manage draft alerts.
Alert Publisher: An Operator with privileges to send alerts, manage draft alerts, manage alert templates and access previously sent alerts.
Advanced Alert Manager: An Operator with privileges to send alerts, manage draft alerts, manage alert templates, access previously sent alerts, manage end user accounts, and manage distribution lists.
Report Manager: An Operator with privileges to access sent alert reports.
Organization Administrator: An Administrator with privileges to access one specific organization (example: all VHA VISNs, VBA, NCA, OIG, and VACO), access to the settings page, manage Operators and Administrators, send alerts, manage draft alerts, manage alert templates, access previously sent alerts, manage end user accounts, and manage distribution lists.
Enterprise Administrator: An Administrator with privileges to access all organizations (example: all VHA VISNs, VBA, NCA, OIG, and VACO), access to all settings, manage Operators and Administrators, send alerts, manage draft alerts, manage alert templates, access previously sent alerts, manage end user accounts, and manage distribution lists.

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

Access to PII is determined by the need to notify employee, contractor or affiliates during emergency situations. VA Directive 0325 identifies roles and responsibilities including individuals who can gain into VA EAAS. Any administrator requiring access to send notifications or manage user accounts are required to complete VA EAAS training prior to receiving authorized access. Additionally, employee, contractor or affiliate are required to complete annual training for VA Privacy and Information Security Awareness and Rules of Behavior (ROB) and VA Privacy. Employees, contractors and affiliates are required to agree to all rules and regulations outlined in the trainings, along with any consequences that may arise for failure to comply.

2.4c Does access require manager approval?

Access to PII is determined by the need to notify employee, contractor or affiliates during emergency situations. VA Directive 0325 identifies roles and responsibilities including individuals who can gain into VA EAAS. Any administrator requiring access to send notifications or manage user accounts are required to complete VA EAAS training prior to receiving authorized access. Additionally, employee, contractor or affiliate are required to complete annual training for VA Privacy and Information Security Awareness and Rules of Behavior (ROB) and VA Privacy. Employees, contractors and affiliates are required to agree to all rules and regulations outlined in the trainings, along with any consequences that may arise for failure to comply.

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

Yes. User Access and certain actions are logged within the SaaS and are available for review/audit.

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

The VA Information System Owner (ISO), application Administrators, and the BlackBerry SaaS vendor are responsible for assuring safeguards for the PII. BlackBerry assures that data in the SaaS solution is protected in accordance with FedRAMP/ National Institute of Standards and Technology (NIST) continuous monitoring guidance and controls. For full information on the controls and processes in place, please refer to the BlackBerry Cloud - AtHoc Services for Government FedRAMP package.

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*

1. Full Name
2. Work and home address
3. Email Address(es)
4. Phone Number(s)
5. Computer Login Username
6. Employee ID
7. IP Address
8. Emergency Contact Information (Name, Phone Number, etc. of a different individual)

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.*

The information listed above is collected and maintained in an account created for each individual VA employee, contractor and affiliate. The accounts and information will be kept secured in the VA EAAS databases as long as each person is working with VA. The information is maintained for the purpose of personnel accountability and emergency notifications. Once the individual retires or separates from the Department, the listed

information within their VA EAAS account will be stored for 30 days as a disabled account. If the individual's account is not reactivated within the 30 days, the account will be deleted permanently from the VA EAAS databases.

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.

The NARA General Records Schedule (December 2017) 5.3-Continuity and Emergency Planning Records, Item 020 applies. Accessible through https://www.archives.gov/files/records-mgmt/grs/grs05-3.pdf.

Records Description: Employee emergency contact information.
Records used to account for and maintain communication with personnel during emergencies, office dismissal, and closure situations. Records may also include other information on employees such as responsibilities assigned to the individual during an emergency.

Exclusion: This item does not include employee directories that contain information about where employees are located in facilities and work phone numbers which are covered under GRS 5.5, item 020).

Disposition Instructions: Temporary. Destroy when superseded or obsolete, or upon separation or transfer of employee.

Disposition Authority: DAA-GRS-2016-0004-0002

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

Yes

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

The NARA General Records Schedule (December 2017) 5.3-Continuity and Emergency Planning Records, Item 020 applies. Accessible through https://www.archives.gov/files/records-mgmt/grs/grs05-3.pdf. Disposition Authority: DAA-GRS-2016-0004-0002

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.

Once the VA EAAS account is disabled for 30 days, the record in VA EAAS is deleted. Only the name of the person may be retained and will only be viewable only through historic alert reports or audit logs.

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

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

The VA EAAS system has two Virtual Private Systems (VPS) used for training, demos, and testing. There is no PII information in either VPS when testing or training. VA EAAS is used solely for sending notifications and information as it relates to emergencies.

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: There is a risk that information could be retained for an inappropriate time period.

Mitigation: Updates from AD are obtained on a daily basis. Any inactive AD account will prompt VA EAAS to disable the account. After 30 days, all disabled accounts will be deleted from VA EAAS. In addition, application Administrators monitor the End Users who are assigned to their respective office, site, department, or VISN in the VA EAAS system to ensure that only proper personnel are listed.

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***
Active Directory (AD)	Information is received from AD to aid VA EAAS with populating the database with new hires and deleting records no longer needed based on the AD account status (active or inactive).	Names, work address, work email, work phone, work cell (GFE), computer login username, IP address and employeeID.	Lightweight Directory Access Protocol (LDAP), Lightweight Directory Access Protocol Over SSL (LDAPS), Global Catalog Query, Hypertext Transfer Protocol Secure (HTTPS)
Authorized VA EAAS Administrators (Emergency Manager, HR, Safety, and VA EAAS Liaisons) for all Administrations and Staff Offices	Information is shared to ensure personnel information is current. Both Emergency Coordinators and HR Reps use information for accountability and/or emergency notification purposes.	Full Name, Work address, Home Address, Email Address(es), Phone Number(s) Computer Login Username, Employee ID, IP Address, Emergency Contact Name and Phone Number	Role-based access to VA EAAS only.

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: Personal Information may be released to unauthorized individuals.

Mitigation: VA EAAS allows one account for each username. To prevent or reduce unauthorized access to PII, VA EAAS has integrated the on-boarding and off-boarding of information from the AD. Any accounts with names, usernames, and emails not matching the AD will be disabled for 30 days. If the account is not reactivated, the account will be deleted.
Secondly, All VA employees, contractors and affiliates are required to complete the TMS training titled VA Privacy and Information Security Awareness and ROB. The VA Privacy and Information Security Awareness and ROB provides information security and privacy training important to everyone who uses VA information systems or VA sensitive information. The training also requires all VA employees, contractors and affiliates to electronically acknowledge and accept the ROB.
Lastly, VA EAAS Operators and Admins have restricted access to their assigned offices only, as needed.

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***
Blackberry AtHoc FISMA Moderate-Impact FedRAMP Approved Cloud Hosting Environment	Data is required to facilitate rapid and accurate alerting of personnel of emergency situations and to conduct personnel accountability functions.	VA employees, contractors and affiliates data from the AD such as full Name, Work address, Home Address, Email Address(es), Phone Number(s), Computer Login Username, Employee ID, IP Address, Emergency Contact Name and Phone Number.	VA EAAS MOU/ISA: Not currently required. The current Enterprise ATO is authorized until 10/07/2023. SORN number 189VA006H/ 86 FR 66620.	HTTPS

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 the information contained in the system can possibly be breached or compromised.

Mitigation: The VA EAAS system hardware is maintained within the Blackberry AtHoc FISMA Moderate-Impact FedRAMP Approved Cloud Hosting Environment. The Blackberry AtHoc FISMA Moderate-Impact Cloud Hosting Environment, owned by Blackberry AtHoc is Federal Risk and Authorization Management Program (FedRAMP) Authorized as a SaaS service, in a hybrid cloud deployment model at the moderate impact level, certified per NIST SP 800-53 Rev 4 (at a moderate FIPS 199 classification). These certifications go beyond the typical SAS 70 Type II / SSAE 16 SOC 2 certification.

Access to the system can only be granted to authorized users who have completed VA EAAS training. In addition, the daily updates with AD will identify accounts which can be disabled or deleted

Section 6. Notice

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

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

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

Yes. See Appendix-A 6.1.

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.

The VA EAAS website has the statement “UNCLASSIFIED - FOUO Contains Personal Data - Privacy Act of 1974 Applies (5 USC 552a)” at the bottom of the website. A Privacy Notice was added as a popup on the Administrator and Employee splash page. The Privacy Notice is shown in the Appendix A-6.1.

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

The VA EAAS website has the statement “UNCLASSIFIED - FOUO Contains Personal Data - Privacy Act of 1974 Applies (5 USC 552a)” at the bottom of the website. A Privacy Notice was added as a popup on the Administrator and Employee splash page. The Privacy Notice is shown in the Appendix A-6.1.

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.

The VA EAAS website has the statement “UNCLASSIFIED - FOUO Contains Personal Data - Privacy Act of 1974 Applies (5 USC 552a)” at the bottom of the website. A Privacy Notice was added as a popup on the Administrator and Employee splash page. The Privacy Notice is shown in the Appendix A-6.1.

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.

VA EAAS has a daily recurring schedule to update from AD, therefore the system already has most of the work contact information. All work address and contact information is required to be updated periodically. VA Directive 0325 mandates employees to provide their personal contact information. Individuals who do not update their personal contact information will not receive critical information that can prevent injury or loss of life. There is no penalty or denial of service if they chose to decline updating their personal information.

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.

Personnel updates for work address and contact information are required. This requirement is met by obtaining the work contact information from the AD. The system requires additional personal information from employees to be efficient. Once provided, customers are unable to consent particular uses of their information. They are able to provide their preference for accountability or notifications through a specific modality (phone, email, cell, etc.).

The VA EAAS work order number 36C10B18F2843, Section B3.1 VA Information Custodial Language, states “Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the contractor / Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1)”. Section B3.2 states “VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor’s information systems or media storage systems in order to ensure VA
requirements related to data protection and media sanitization can be met. If co-mingling must be
allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA’s sanitization requirements”.

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: It is possible the employee providing the information is unaware an account is automatically created using their work contact information from the AD and what the account is used for.

Mitigation: A Privacy Notice was added to a popup notice window at the Administrator and Employee login splash page. Additionally, new Employee Orientations or the on-boarding processes will introduce VA EAAS, its purpose, who uses it, and when it is typically used.

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.***

All employees with a VA EAAS account can login using the VA EAAS Self Service Link which validates a person's computer login with their VA EAAS username. If there is no match, the employee will not be granted access and will be given an error message stating they either have a disabled account or they don't have an account. Employees can update and provide other contact information, as needed. The Enterprise Service Desk (ESD) also provides assistance to personnel when needed.

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).

VA EAAS not exempt from the Privacy Act.

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.

All employees with a VA EAAS account can login using the VA EAAS Self Service Link which validates a person's computer login with their VA EAAS username. If there is no match, the employee will not be granted access and will be given an error message stating they either have a disabled account or they don't have an account. Employees can update and provide other contact information, as needed. The Enterprise Service Desk (ESD) also provides assistance to personnel when needed.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Procedures for updating erroneous information in VA EAAS can be done by the employee or any VA EAAS Help Desk Tier 2 and Tier 3 Group members by accessing the VA EAAS Self Service link specific to the employee's organization and location. Callers are vetted by opening a ticket with the VA OIT Enterprise Service Desk (ESD) ticketing system. The VA Service Now obtains the caller's or requester's name, VA email, and problem they are experiencing.

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.

All employees have access to their account and the information in the account by clicking on a VA EAAS Self Service Link. Employees can update any outdated information in VA EAAS. If needed or requested, assistance can be provided by contacting the VA Enterprise Service Desk (ESD) by calling 1-855-NSD-HELP (or 1-855-673-4357). The ESD technicians has access to knowledge documents (user guides) to assist the employee with accessing or updating their account. The ESD knowledge documents are reviewed and updated annually or when procedures change. Changes and review is coordinated between the ESD and the VA EAAS program manager.

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.

A redress process is available through the VA EAAS Self Service Link. The VA EAAS Self Service Link allows user login. Once logged in, users will be able to view or edit work address, home address, home phone, work phone, personal cell, alternate work cell, work email, and personal email. Any information from AD that is incorrect may be changed through the ESD.

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: Some individuals may find access to their account through the VA EAAS Self Service Link is denied due to not having a VA EAAS account, their account is disabled, or their username does not match their computer login.

Mitigation: The ESD has access to many knowledge documents to assist the user with accessing their account. If the login error persists, the knowledge documents will guide the ESD Technicians in updating the user's VA EAAS username or enabling the account. Any other issues are escalated to the VA EAAS Tier 2 and Tier 3 Group and addressed within 24 hours.

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.

Only VA authorized users are able to access data and vendor supporting product. VA employees and contractors can login as end users. Authorized administrators can access

the system to maintain the user database or to send notifications. Authorized administrators are granted access by the VA business owner after receiving training, as required. Emergency Managers requesting authorized administrator access will open a Service Now ticket which will be assigned to the VA EAAS Tier 2 and 3 help desk group. Once ticket is received by the VA EAAS Tier 2 and 3 help desk group, the VA EAAS Help Desk will reach out to the emergency manager's supervisor to obtain supervisor approval for access to VA EAAS. The help desk will also guide the emergency manager to complete the VA EAAS Operator and Administrator training available in TMS. Once the help desk receives the TMS certificates, the help desk will provide access to VA EAAS. The VA has established the criteria for what PII will be shared. VA's Human Capital Services Center (HCSC) works in conjunction with the vendor to define the data parameters.

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?

VA EAAS is not accessible to personnel from outside of the VA or any other Federal agencies. Only users who have been fully on-boarded and granted VA network access can access the VA EAAS system.

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.

In general, Administrator and Operator user types (Advanced Alert Manager, Alert Publisher, Distribution Lists Manager, Draft Alert Creator, End User Manager, Enterprise Administrator, Organization Administrator, and Report Manager) have the ability to generate alerts, view alert reports, manage user accounts, and manage distribution lists in the VA EAAS system. The majority of the 500k+ plus accounts in the VA EAAS system are End User users and can only view and update their own contact information within the system.

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.

Contractors will only have access to their own individual accounts through the VA EAAS Self Service Link. The VA EAAS system is hosted in Blackberry AtHoc FISMA Moderate-Impact FedRAMP Approved Cloud Hosting Environment as a SaaS implementation. Only

agreed upon BlackBerry AtHoc and Four Points, Inc. personnel will have access to the system for maintenance and training purposes. BlackBerry personnel who access the system and VA network will complete all VA on-boarding requirements (NDA, PIV issuance, Background Investigation, etc).

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.

Privacy and Information Security Awareness and Rules of Behavior (TMS course # 10176) is required for all Federal and Contractor personnel that require access to the VA Network. New Employees, contractors and affiliates will complete the VA EAAS Employee training in TMS course number, VA 4619494. VA EAAS Operators and administrators also have TMS training to complete prior to gaining access to VA EAAS. Those trainings are TMS Course ID 4563148 (Operator Training) or Course ID 4563149 (Administrator Training).

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

Yes. A full three-year ATO was initially granted on 5/13/2019. The current Enterprise ATO is authorized until October 7, 2023.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 02/14/2023
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 10/07/2022
5. *The Authorization Termination Date:* 10/07/2023
6. *The Risk Review Completion Date:* Please provide response here
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.***

Not applicable.

Section 9 – Technology Usage

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

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

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

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

Yes. The Blackberry AtHoc FISMA Moderate-Impact Cloud Hosting Environment, owned by Blackberry AtHoc is Federal Risk and Authorization Management Program (FedRAMP) Authorized as a SaaS service, in a hybrid cloud deployment model at the moderate impact level, certified per NIST SP 800-53 Rev 4 (at a moderate FIPS 199 classification).

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.*

VA contract NNG15SD22B (fully executed on 02/28/2023) governs all terms associated with ownership of VA data. Contract was executed by and using standard templates of the VA Technology Acquisition Center (TAC).

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.

Yes. VA contract NNG15SD22B (fully executed on 02/28/2023) governs all terms associated with ownership of VA data. Contract was executed by and using standard templates of the VA Technology Acquisition Center (TAC).

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.

Yes. VA contract NNG15SD22B (fully executed on 02/28/2023) governs all terms associated with ownership of VA data. Contract was executed by and using standard templates of the VA Technology Acquisition Center (TAC).

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).

Yes. RPA processes are used by the SaaS to synchronize and validate data. An example of this is the automated synchronization of AD data to the SaaS, and the processes that run to filter the data to ensure that duplicate accounts are not created.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2023.05.16 10:11:25 -06'00'

Privacy Officer, Julie Drake

Joseph A. Guillory 1085540 Digitally signed by Joseph A. Guillory 1085540
Date: 2023.05.22 08:39:35 -07'00'

Information System Security Officer, Joseph Guillory

SHANNON JONES Digitally signed by SHANNON JONES
Date: 2023.05.22 12:29:12 -04'00'

Information System Owner, Shannon E. Jones

APPENDIX A-6.1

Notice of Privacy Practices

As of: December 10, 2018

The VA EAAS website has the statement “UNCLASSIFIED - FOUO Contains Personal Data - Privacy Act of 1974 Applies (5 USC 552a)” at the bottom of the website.
The following Privacy Notice was added as a popup on the splash page.

Authority: Federal Continuity Directive 1 (FCD 1)
Purpose and Routine Use: Information provided to the system is protected by the Privacy Act Statement of 1974 and will ONLY be used for emergency alerts and personnel accountability.
DISCLOSURE: Personal contact information is VOLUNTARY. Employees who opt against providing additional information will not receive alerts and accountability messages on their personal devices from their Safety or Emergency Management staff. less

---

AD Privacy Notice
As of: January 10, 2018

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.

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