SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

*The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).*


Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.
Privacy Impact Assessment for the VA IT System called:

**VistA Adaptive Maintenance (VAM)**

*Name of the Program Office: Enterprise Cloud Solutions Office (ECSO)*

**Date PIA submitted for review:**

July 28, 2020

**System Contacts:**

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Rita Grewal</td>
<td><a href="mailto:Rita.Grewal@va.gov">Rita.Grewal@va.gov</a></td>
<td>202-632-7861</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Albert Estacio</td>
<td><a href="mailto:Albert.Estacio@va.gov">Albert.Estacio@va.gov</a></td>
<td>909-583-6309</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>David Catanoso</td>
<td><a href="mailto:David.Catanoso@va.gov">David.Catanoso@va.gov</a></td>
<td>732-440-9583</td>
</tr>
</tbody>
</table>

Version Date: February 27, 2020
Page 1 of 23
Abstract

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

The VistA Adaptive Maintenance (VAM) system is a comprehensive, commercial Cloud-First/Cloud-Native security solution that provides security for all remote clients, applications, and users of VistA data via monitoring and securing VistA’s Remote Procedure Call (RPC) interface within the VA’s FedRAMP-high Enterprise Cloud (VAEC).

Overview

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

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?
- Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.
• Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
• NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?
• What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?

VistA Adaptive Maintenance (VAM) is a Cloud-Smart / Cloud-Native application deployed in the dedicated U.S. FedRAMP-HIGH, HIPAA-compliant VA Enterprise Cloud (VAEC) leveraging Amazon Web Services (AWS) commercial cloud infrastructure, security, and services. VAM is a passive monitoring system which sends the log of VistA traffic to AWS CloudWatch Logs for security monitoring. Some of this VistA traffic may contain PII. AWS CloudWatch Logs is FedRAMP-high certified and stores all data in encrypted form within the FedRAMP-high, HIPAA-compliant VAEC

VAM provides comprehensive, commercial cloud-based monitoring and security for all remote clients, applications, and users that access VistA data via VistA’s Remote Procedure Call (RPC) interface. VAM is operationalized and scaled for production enterprise’s use in the VAEC leveraging FedRAMP-high approved AWS Kinesis Streams and AWS CloudWatch Logs and provides comprehensive commercial cloud-based VistA RPC Interface monitoring and security for all VistA systems migrated to the VAEC. VAM is 100% Legacy-free, Cloud-Native, and Non-invasive - allowing it to be scaled and deployed enterprise-wide without any change required for any VistA system or any end-user Client or Application.

VAM does not allow for connection or sharing of information in identifiable form with external organizations, websites or applications. VAM will be hosted in production within the VA’s FedRAMP-high / HIPAA-certified Enterprise Cloud (VAEC) using Amazon Web Services (AWS).

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

the text box below:

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Health Insurance Beneficiary Numbers
- Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Other Unique Identifying Number (list below)

VAM application and RPCs do not store or transmit any information outside the VAEC network. The RPC Mirror and RPC Monitor logs, describes and classifies Vista data and migrates (by Executive Order 9397) it to AWS Kinesis Streams and AWS CloudWatch Logs located in AWS VAEC. Other information that will be accessed and processed include:

- Gender
- Guardian name and contact information
- Next of kin name and contact information
- Military and service history
- Employment information
- Veteran dependent information
- Education information
- Research medical statistics
- Service-connected rating and disabilities
- Criminal background information
- Date of death

**PII Mapping of Components**

VAM consists of four key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VAM and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**
### Components of the information system (servers) collecting/storing PII

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS CloudWatch Logs</td>
<td>Yes</td>
<td>Yes</td>
<td>AWS VAEC</td>
<td>Parsing data and classifying it</td>
<td>AWS VAEC</td>
</tr>
<tr>
<td>AWS Kinesis Streams</td>
<td>Yes</td>
<td>No</td>
<td>AWS VAEC</td>
<td>Mirrors Vista traffic</td>
<td>AWS VAEC</td>
</tr>
<tr>
<td>RPC Mirror</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>VAEC</td>
</tr>
<tr>
<td>RPC Monitor</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>VAEC</td>
</tr>
</tbody>
</table>

### 1.2 What are the sources of the information in the system?

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

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.  
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

VistA is the source information. The VAM application / RPC Mirror and RPC Monitor are not an End User based software and there is no GUI (Graphical User Interface). VAM is a passive monitoring system that sends the mirrored client-to-VistA RPC traffic to an alternate, data streaming service (AWS Kinesis), which sends the log of VistA traffic (Data source) to Amazon Web Services (AWS) AWS CloudWatch Logs for security monitoring. VistA traffic contains varying levels of PII. AWS CloudWatch Logs is FedRAMP-high certified and stores all data in encrypted form within the FedRAMP-high, HIPAA-compliant VAEC.

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

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

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

VAM mirrors the traffic from all remote Clients (such as CPRS) that use VistA’s Remote Procedure Call (RPC) interface and stores this traffic log in encrypted form in the FedRAMP-high certified AWS CloudWatch Logs within VAEC. This is a fully automated process. There is no human involvement in the capture or management of any of this data. All information is fully and immediately encrypted within AWS CloudWatch Logs. There is no access to any of the traffic logs outside of the Virtual Private Network (VPN) of the VAEC.

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

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

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

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

Purpose is to provide monitoring for all remote clients, applications, and users that access VistA data via VistA’s Remote Procedure Call (RPC) interface.

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

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.
If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract. This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

All information passing into the VAEC environment has already been through the VA Network’s authentication process. For the VAM Application itself, an RPC (Remote Procedure Call) is an American Standard Code Information Interchange (ascii) encoded message sent by VistA Clients to VistA over TCP connections. RPCs are logged and classified.

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

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

Executive Order 9397 allows Federal agencies to collect and use the SSN. VAM will migrate information collected to support the EHR from legacy systems to a secure, centralized, cloud-based system. All processes in place for the legacy systems will remain in place during migration of data. VAM is hosted in the VAEC environment and at High Assessing, the information that is logged is done so in AWS CloudWatch Logs that also resides in the AWS VAEC, thus the collection of data/data retention is inherited through the Cloud Service Provider (CSP) in accordance of the Customer Responsibility Matrix (CRM).

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?
Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: VAM has been categorized in the Enterprise Program Management Office (EPMO) System Security Categorization as a High impact system based on the sensitive and important nature of the VistA data traffic that the VAM application monitors. The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day to day functions from providers. However, the risk of information exposure is based on the VAEC security maintaining integrity.

Mitigation: There are no connections outside of the VAEC to websites, or systems and does not directly collect information from individuals. VAM provides security monitoring for all remote access clients (CPRS, JLV, CAPRI, …) of all veterans’ health and benefits information in the Veterans Information System and Technology Architecture (VISTA) systems. Additionally, system Log files, sample clinical data that may contain Protected Health Information (PHI) appropriate to the agreements. Veteran, veteran's primary contact and volunteer's service, medical, criminal record, guardian, education and benefit information may be collected as well as contractor and employee personnel and payroll records may be collected and processed.

The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day to day functions from providers. However, the risk of information exposure is based on the VAEC security maintaining integrity.

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.

VAM is meant to plan, develop, design, integrate, test, implement, and manage centralized services to provide comprehensive, real-time, 24/7 monitoring and security for all Veteran data in all VistA systems migrated to VAEC. VAM is a data-driven, minimally invasive, intelligent auditing and alerting classifier system of RPC inquiries into the VistA. As VA continues to strengthen its cybersecurity profile, project VAM will provide the following benefits:

• Reduce the cost and complexity of the maintenance of VistA systems
• Resolve security vulnerabilities of all VistA systems migrated to VAEC
• Full utilization of the scaling and features of VA’s commercial cloud capabilities
• Ensure the safe, secure, and seamless continuity of Veteran care and services as VistA systems are migrated to VAEC

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

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

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

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

VAM is comprised of three major architectural components; the RPC Monitor, the RPC Mirror, and the RPC Definition Models. Because VAM only resides in the VAEC environment, all other tools are inherited through the VAEC and Cloud Service Provider (CSP).

1. The RPC Monitor represents the software pipeline that facilitates RPC parsing, classification, and alert notification functions of the VAM application
2. The RPC Mirror represents the software that mirrors client-to-VistA RPC traffic to an alternate, data streaming service, Amazon Web Services (AWS) Kinesis. AWS Kinesis must make as small an impact as possible, as it sits on the critical network traffic path between VistA clients and VistA.
3. The RPC Definition Models represent the static RPC definition model files, generated by the RPC Definition Toolkit, and the classifier pipeline, resident in the RPC Monitor, that applies the models against RPC traffic to generate classifications and alerts.
4. **NOTE:** All of the VAM architectural components will be managed within a single security boundary in VAEC.

VAM enables VA to transition from VistA systems to a single, secure, commercially managed set of centralized cloud-based services - Veteran Integrated Care Services (VICS) - while maintaining full backwards-compatibility and continuity of care and workflows of the Computerized Patient Record System (CPRS). VAM will be hosted in production within the VA’s Enterprise Cloud (VAEC) using Amazon Web Services (AWS). The result of integration will streamline and improve patient care for Veterans and their dependents. No information is stored or handled outside the VAEC network.
There is no connection outside of the VA to websites, or systems. VAM is not an End User based software and there is no GUI (Graphical User Interface).

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

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

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

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

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

All information in VistA, and in the VAEC is entered and accessed by healthcare professionals, already trained in handling of PHI and PII. This system allows for data transfer and database consolidation. All processes and workflows in place handling PII/PHI, and access to the data, will be maintained as they are for the current systems and the VAEC environment.

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

All clinical and administrative data that passes through the RPC Broker port.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the
information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.

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

All RPC mirrored data is stored in S3 buckets in unstructured format for 15 days.

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

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

No, the data is only being kept for 15 days but a report can be generated manually as needed.

3.4 What are the procedures for the elimination of SPI?

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

Once they reach 15 days they are automatically deleted daily.

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

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

VAM does not have any external connections outside the VAEC environment. All data privacy restrictions are through the VAEC.
3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: VAM has been categorized in the EPMO System Security Categorization as a High impact system based on the sensitive and important nature of the VistA data traffic that the VAM application monitors. The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day to day functions from providers. However, the risk of information exposure is based on the VAEC security maintaining integrity.

Mitigation: VAM is hosted in the VAEC environment. Data retention requirements are inherited from the Cloud Service Provider (CSP) as identified in the Customer Responsibility Matrix (CRM) Per the VA 6500 and 6510, all members are provided required annual security awareness training. All members are required to review and sign a Rules of Behavior form, NDA (Non-disclosure agreement) and conduct TMS based trainings.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.
4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

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

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

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

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

**Data Shared with Internal Organizations**

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>VistA</td>
<td>System integration/centralization</td>
<td>System Log files, sample clinical data that may contain Protected Health Information (PHI) appropriate to the agreements. Veteran, veteran's primary contact and volunteer's service, medical, criminal record, guardian, education and benefit information may be</td>
<td>All clinical and administrative data that passes through the RPC Broker port</td>
</tr>
<tr>
<td>Data Source</td>
<td>Purpose</td>
<td>Information Stored</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>--------------------</td>
<td>-------</td>
</tr>
<tr>
<td>VA Email</td>
<td>Project related communications</td>
<td>Emails, image attachments, Word Documents and PDFs.</td>
<td>VA Enterprise Microsoft Outlook</td>
</tr>
<tr>
<td>eMASS</td>
<td>Project information related for Authorization to Operate (ATO) purposes</td>
<td>Application/system information and descriptions. Evidence of compliance to NIST requirements, which includes screenshots and policies.</td>
<td>VA Enterprise eMASS. Vista Adaptive Maintenance (VAM) Assessing link: <a href="https://va.emass.apps.mil/App/CA/SystemMainDashboard/1030/8541">https://va.emass.apps.mil/App/CA/SystemMainDashboard/1030/8541</a></td>
</tr>
<tr>
<td>GitHub – Public Open source</td>
<td>Code and collaboration management</td>
<td>ATO process. Project status and communication on tasks. Test code (Not active/live) and system components. No sensitive data or PII is maintained on the VAM GitHub</td>
<td>Link: <a href="https://github.com/CloudVistA/cloudvista-TrafficMirrorMonitor">https://github.com/CloudVistA/cloudvista-TrafficMirrorMonitor</a> Information is only transmitted within the GitHub itself and through VA Network email.</td>
</tr>
<tr>
<td>GitHub - VAEC</td>
<td>Code and collaboration management</td>
<td>ATO process. Project status and communication on tasks. Test code (Not active/live) and system components. No sensitive data or PII is maintained on the VAM GitHub</td>
<td><a href="https://github.ec.va.gov/ECSO/TrafficMirror">https://github.ec.va.gov/ECSO/TrafficMirror</a> Information is only transmitted within the GitHub itself and through VA Network email.</td>
</tr>
</tbody>
</table>

### 4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Version Date: February 27, 2020

Page 14 of 23
Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. This question is related to privacy control UL-1, Internal Use.

Follow the format below:

**Privacy Risk:** VAM has been categorized in the EPMO System Security Categorization as a High impact system based on the sensitive and important nature of the VistA data traffic that the VAM application monitors. The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day to day functions from providers.

**Mitigation:** However, the risk of information exposure is based on the VAEC security maintaining integrity. Cloud Service Provider (CSP) will not be affected by intentional or unintentional disclosure of PII, but VA will be affected. This solution supports VISTA data and any disclosure of data will have a harmful effect on the VA and the magnitude will be same as VISTA data being disclosed. Bec All information sharing is done within the VA network, per VA 6500 and 6510 requirements. Contractors working on the VAM Project are required to have PIV cards, Government Furnished Equipment (GFE - Laptops), VPN access to VA network and VA enterprise emails. Additionally, VAM RPCs only reside in the VAEC environment and have no external connections and VAM RPCs are not an End User based software, as well as there is no GUI (Graphical User Interface).

**Section 5. External Sharing/Receiving and Disclosure**

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

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

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

**Note:** This question is #7 in the Privacy Threshold Analysis.

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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

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

N/A. VAM application has no external connection outside of VA. Information sharing only occurs within the VA Network

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:** High

**Mitigation:** VAM has been categorized in the EPMO System Security Categorization as a High impact system based on the sensitive and important nature of the VistA data traffic that the VAM application monitors. The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day to day functions from providers. However, the risk of information exposure is based on the VAEC security maintaining integrity.

VAM application has no external connection outside of VAEC environment. VistA data is protected in the VAEC environment. All information sharing is done within the VA network, per VA 6500 requirements. Contractors working on the VAM Project are required to have PIV cards, Government Furnished Equipment (GFE - Laptops), VPN access to VA network and VA enterprise emails.

**Section 6. Notice**

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

N/A. The VAM application has no external connections outside the VAEC. VAM Application / RPCs are not an End User based software. Moreover, there is no GUI (Graphical User Interface).

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.

N/A. The VAM application has no external connections outside the VAEC. VAM Application / RPCs are not an End User based software. Moreover, there is no GUI (Graphical User Interface).

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.

N/A. The VAM application has no external connections outside the VAEC. VAM Application / RPCs are not an End User based software. Moreover, there is no GUI (Graphical User Interface).

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

**Principle of Use Limitation:** Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

Follow the format below:

**Privacy Risk:** VAM has been categorized in the EPMO System Security Categorization as a High impact system based on the sensitive and important nature of the VistA data traffic that the VAM application monitors. The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day to day functions from providers. However, the risk of information exposure is based on the VAEC security maintaining integrity.

**Mitigation:** The VAM application has no external connections outside the VAEC. VAM RPCs are not an End User based software. Moreover, there is no GUI (Graphical User Interface). CSP will not be affected by intentional or unintentional disclosure of PII, but VA will be affected. This solution
supports VISTA data and any disclosure of data will have a harmful effect on the VA and the magnitude will be same as VISTA data being disclosed.

VAM is hosted in the VAEC environment and at High Assessing. System notices is a requirement inherited from the VA Enterprise as identified in the Customer Responsibility Matrix (CRM) attached under the evidence tab.

Section 7. Access, Redress, and Correction

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

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

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

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

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

N/A. The VAM application has no external connections outside the VAEC. VAM Application / RPCs is not an End User based software. Moreover, there is no GUI (Graphical User Interface).

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. The VAM application has no external connections outside the VAEC. VAM Application / RPCs is not an End User based software. Moreover, there is no GUI (Graphical User Interface).
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. The VAM application has no external connections outside the VAEC. VAM Application / RPCs is not an End User based software. Moreover, there is no GUI (Graphical User Interface).

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

N/A. The VAM application has no external connections outside the VAEC. VAM Application / RPCs is not an End User based software. Moreover, there is no GUI (Graphical User Interface).

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.
Follow the format below:

**Privacy Risk:** VAM has been categorized in the EPMO System Security Categorization as a High impact system based on the sensitive and important nature of the VistA data traffic that the VAM application monitors. The inherent risk from the VAM application is VistA traffic interruption. This can cause delays in day to day functions from providers. However, the risk of information exposure is based on the VAEC security maintaining integrity.

**Mitigation:** The VAM application has no external connections outside the VAEC. VAM Application / RPCs is not an End User based software. Moreover, there is no GUI (Graphical User Interface). VA will be affected by intentional or unintentional disclosure of PII. This solution supports VISTA data and any disclosure of data will have a harmful effect on the VA and the magnitude will be same as VISTA data being disclosed.

VAM provides security monitoring for all remote access clients (CPRS, JLV, CAPRI, …) of all veterans’ health and benefits information in the Veterans Information System and Technology Architecture (VISTA) systems. The resulting issue from system failure is traffic interruption. Issue can be addressed through rescaling.

**Section 8. Technical Access and Security**

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

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

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

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

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

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

The data in the S3 bucket is encrypted at rest and only authorized and authenticated users will have access to the S3 bucket. Date is retained for 15 days and automatically deleted.

**8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?**
If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

VA Contractors must have an approved PIV and an approved VPN access to the VA Network as well as requesting access to the Cloud environment by creating a VAEC Service Desk ticket. VA Contractors do not handle live PII (dummy data) in the Pre-Production environment. Contractors adhere to the requirements for use-privileges (VA 6500 and 6510). Contractors are required to review and/or sign onboarding training and documents, such as Rules of Behavior, NDA (Non-disclosure agreement), TMS training and Security Awareness. Additionally, VAM has no external connections outside the VAEC. VAM is not an End User based software. Moreover, there is no GUI (Graphical User Interface).

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.

VAM Application is not an End User software. However, VA Contractors take and review TMS training, NDA (Non-disclosure agreement) Rules of Behavior, Security Awareness, per the VA 6500 and 6510.

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

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

If No or In Process, provide your Initial Operating Capability (IOC) date.
1. An ATO was granted on 25 Nov 2019
2. Full ATO was granted
3. One Year ATO was granted, due to expire 19 Nov 2020
4. The categorization of the application is, HIGH.
# Section 9. References

## Summary of Privacy Controls by Family

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

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

RITA K GREWAL 114938
Digitally signed by RITA K GREWAL 114938
Date: 2020.07.31 07:56:14 -04'00'

Privacy Officer, Rita Grewal

Albertino M. Estacio 119921
Digitally signed by Albertino M. Estacio 119921
Date: 2020.07.31 13:00:42 -07'00'

Information System Security Officer, Albert Estacio

David Catanoso 337416
Digitally signed by David Catanoso 337416
Date: 2020.07.31 23:21:40 -04'00'

Information System Owner, David Catanoso
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).