VistA Adaptive Maintenance VAEC Security (VAM)

Monthly Progress Report



Department of Veterans Affairs

Office of Information & Technology

Contract No: VA118-16-D-1009

Task Order: 36C10B19F10090015

**September 2019**

Version 1.6

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 09/03/2019 | 1.6 | Updates for August 2019 | AbleVets |
| 08/02/2019 | 1.5 | Updates for July 2019 | AbleVets |
| 07/03/2019 | 1.4 | Updates for June 2019 | AbleVets |
| 06/03/2019 | 1.3 | Updates for May 2019 | AbleVets |
| 05/03/2019 | 1.2 | Updates for April 2019 | AbleVets |
| 04/03/2019 | 1.1 | Updates for March 2019 | AbleVets |
| 03/04/2019 | 1.0 | Initial version of the document | AbleVets |

CLIN Satisfaction Statement

This document is submitted in satisfaction of CLIN 0001AB.

Table of Contents

[1. Introduction 1](#_Toc17977964)

[2. Work Completed 1](#_Toc17977965)

[3. Work Planned 2](#_Toc17977966)

[4. Risks and Issues 3](#_Toc17977967)

[A. Appendix: Acronyms and Abbreviations 4](#_Toc17977968)

Table of Tables

[Table 1: PWS Project Deliverables 2](#_Toc17977969)

[Table 2: Risks and Issues 3](#_Toc17977970)

[Table 3: Acronyms and Abbreviations 4](#_Toc17977971)

# Introduction

The Veterans Health Information Systems and Technology Architecture (VistA) Adaptive Maintenance (VAM) System is a cloud-native Platform as a Service (PaaS), deployed entirely and exclusively within the Federal Risk and Authorization Management Program (FedRAMP), Health Insurance Portability and Accountability Act of 1996 (HIPAA)-compliant VA Enterprise Cloud (VAEC), leveraging the Amazon Web Services (AWS) commercial cloud infrastructure and services.

VAM provides comprehensive, commercial cloud-based monitoring and security for all clients, applications, and users of the VistA Remote Procedure Call (RPC) interface. VAM is operationalized and scaled for Enterprise Production use for all VistA systems migrated to the VAEC, leveraging FedRAMP High, VAEC-approved AWS Kinesis and AWS CloudWatch Logs.

VAM is a passive monitoring PaaS that mirrors VistA RPC traffic via AWS Kinesis to the AWS CloudWatch Logs, which is then interpreted by the RPC Monitor. AWS CloudWatch Logs are FedRAMP High certified and store all data in an encrypted form.

VAM is a 100% cloud-native, legacy-free, and non-invasive PaaS. VAM requires no change to any VistA system, nor to any end user client or application, allowing VAM to be safely and reliably deployed and scaled Enterprise-wide with minimal to no risk. Should VAM (RPC Mirror or Monitor) be disabled or deactivated, all RPC traffic flows between VistA and all its clients as usual, only without monitoring.

All of VAM’s functionality is contained exclusively and entirely as a PaaS within the VAEC, thus inheriting all security and compliance controls of the Federal Information Security Management Act of 2002 (FISMA) High VAEC. VAM has neither a connection to, nor does it share any information with, any organization, application, or system outside of the VAEC.

# Work Completed

The work detailed below was completed during the August 1 through August 31, 2019 Period of Performance (PoP).

* Updated Project VAM’s Enterprise Mission Assurance Support Service (eMASS) profile.
* Created an eMASS [migration dashboard](https://github.com/vistadataproject/VAM2ProjectManagement/tree/master/eMASS_Transition) in GitHub.
* Met with Business Owner, System Owner, VA Project Manager (PM), and Information System Security Officer (ISSO) and received their concurrence to fast-track the VAM Authority to Operate (ATO) approval process by seeking a 1-year conditional ATO, given the new timeline for an ATO approval process in eMASS.
* Began the review and update of new controls for the ATO package in eMASS.
* Worked with the VA COMS team to carry over VAM’s classification as PaaS from RiskVision to eMASS.
* Completed the analysis of the version D5 logs and enhancement of definitions.
* Received updated results from the Nessus scan. No critical or high issues found.
* Received the Secure Code review results.
* Continued remediating the issues found in the Secure Code review and submitted a request for a new Secure Code review.
* Received the results of the Quality Code scan.
* Continued remediating the issues found in the Quality Code scan and submitted a request for a new Quality Code scan.
* Facilitated multiple, weekly status meetings to discuss Team AbleVets’ progress. Meeting minutes can be found on the [Project VAM workspace](https://github.com/vistadataproject/VAMProjectManagement/tree/master/Documents/weekly_meeting_minutes) of GitHub.
* Delivered the Weekly Onboarding Status Reports on August 7, 14, 21, and 28, 2019.
* Updated and delivered the PWS artifacts (Table 1) on August 3, 2019.

Table 1: PWS Project Deliverables

|  |  |
| --- | --- |
| CLIN | Artifact |
| 0001AA | Contractor Project Management Plan (CPMP) |
| 0001AB | Monthly Progress Report |
| 0002AA | Comprehensive RPC Interface Audit Report |
| 0002AB | Massachusetts General Hospital Utility Multi-Programming System (MUMPS) RPC to JavaScript Object Notation (JSON) Model Data Definition |
| 0002AC | Version Description Document (VDD) |
| 0002AD | Automated CloudWatch Configuration |
| 0002AE | Security Vulnerability Report |
| 0003AA | Master Test Plan |
| 0003AB | RPC Interface Test Suite |
| 0005AA | Production Operations Manual (POM) |
| 0005AB | Deployment and Installation Guide |
| 0005AC | User Guide |

# Work Planned

The following work is planned for the September 1, 2019 to September 30, 2019 PoP.

* Continue updating Project VAM’s eMASS profile for the Authorizing Official’s (AO) review.
* Submit all relevant information and documentation for the processing of the ATO.
* Continue the analysis of the version D6 change crumbs.
* Continue updating the test framework.
* Obtain all required scans for the VAM environments in AWS.
* Facilitate weekly status meetings.
* Update project documentation and prepare same for delivery.

# Risks and Issues

Table 2 lists the currently known risks and issues. Each item will be resolved prior to the delivery of Build 4 in January of 2020.

Table : Risks and Issues

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Issue Number and Category | Due Date | Issue Description | Risk | Mitigation Plan |
| VAM-R10 (ATO Dashboard) | 10/31/2019 | Receive VA approval for the ATO package by 10/31/2019. | If ATO approval is not received by 10/31/2019, the VAM deployment to IOC Production will be delayed. | Team AbleVets will submit all ATO documentation to eMASS by 9/15/2019, ensuring VA has sufficient time to review and approve the ATO package by 10/31/2019. |
| VAM-R17 (IOC Dashboard)  Technical | 10/31/2019 | Access to the VistA environments in VAEC is required for Build 4. | If Team AbleVets does not obtain access to the VistA environments in VAEC by 9/30/2019, then they cannot deploy or test Build 4 in the IOC PreProduction environment, resulting in a day-for-day schedule slip that will impact the Production deployment date. | Upon completion of the VA migration of VistA environments to VAEC, Team AbleVets will immediately submit access requests and elevate the requests as needed. Once access is granted, Team AbleVets will deploy and test Build 4. |
| VAM-R59 (Administration) | 09/15/2019 | The transition to eMASS will impact the VAM ATO package submission | If the ATO package cannot be submitted for approval by 09/15/2019 due to the multiple new external dependencies at each stage of the eMASS RMF (Risk Management Framework) approval process, receiving an ATO for IOC Production will be impacted. | AbleVets persuaded the Business Owner, System Owner, VA PM, and ISSO to seek a 1-year conditional ATO to fast-track the ATO approval, as the new process for ATO approval in eMASS is lengthier. |

1. Appendix: Acronyms and Abbreviations

Table 3 lists the acronyms and abbreviations used in this document with their descriptions.

Table : Acronyms and Abbreviations

|  |  |
| --- | --- |
| Acronym | Description |
| **ATO** | Authority to Operate |
| **AWS** | Amazon Web Services |
| **BIA** | Business Impact Analysis |
| **CM** | Configuration Management |
| **COMS** | Cloud Operations and Management Services/Cloud Operations and Migration Services |
| **CPMP** | Contractor Project Management Plan |
| **CSOC** | Cybersecurity Operations Center |
| **DRP** | Disaster Recovery Plan |
| **eMASS** | Enterprise Mission Assurance Support Service |
| **FedRAMP** | Federal Risk and Authorization Management Program |
| **FISMA** | Federal Information Security Management Act of 2002 |
| **HIPAA** | Health Insurance Portability and Accountability Act of 1996 |
| **IOC** | Initial Operating Capability |
| **IRP** | Incident Response Plan |
| **ISA** | Independent Safety Assessment |
| **ISCP** | Information Security Contingency Plan |
| **ISSO** | Information System Security Officer |
| **JSON** | JavaScript Object Notation |
| **MOU** | Memorandum of Understanding |
| **MTP** | Master Test Plan |
| **MUMPS** | Massachusetts General Hospital Utility Multi-Programming System |
| **PaaS** | Platform as a Service |
| **PIA** | Privacy Impact Assessment |
| **PM** | Project Manager |
| **POAM** | Plan of Action and Milestones |
| **POM** | Production Operations Manual |
| **PoP** | Period of Performance |
| **PTA** | Privacy Threshold Analysis |
| **PWS** | Performance Work Statement |
| **RMF** | Risk Management Framework |
| **RPC** | Remote Procedure Call |
| **SIA** | Security Impact Analysis |
| **SDD** | System Design Document |
| **SSC** | System Security Categorization Report |
| **SSP** | System Security Plan |
| **VA** | Department of Veterans Affairs |
| **VAEC** | VA Enterprise Cloud |
| **VAM** | VistA Adaptive Maintenance |
| **VDD** | Version Description Document |
| **VistA** | Veterans Health Information Systems and Technology Architecture |
| **WASA** | Web Application Security Assessment |