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

**January 2020**

Version 1.10

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 01/03/2020 | 1.10 | Updates for December 2019 | AbleVets |
| 12/03/2019 | 1.9 | Updates for November 2019 | AbleVets |
| 11/04/2019 | 1.8 | Updates for October 2019 | AbleVets |
| 10/03/2019 | 1.7 | Updates for September 2019 | AbleVets |
| 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](#_Toc28947600)

[2. Work Completed 1](#_Toc28947601)

[3. Work Planned 2](#_Toc28947602)

[4. Risks and Issues 2](#_Toc28947603)

Table of Tables

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

[Table 2: Acronyms and Abbreviations 2](#_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 December 1 through December 31, 2019 Period of Performance (PoP).

* Started IOC pre-production testing at Valley Costal Band (VCB) and Omaha VISTA.
* Completed IOC Pre-Production testing at VCB VistA and provided the demonstration to the entire team on 12-04-2019.
* Installed the software on Production site and started testing against VCB VistA after the successful completion and demonstration of pre-production testing.
* 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 December 04, 11, and 18, 2019.
* Updated and delivered the following PWS artifacts (Table 1) on December 4, 2019.

Table : PWS Project Deliverables

|  |  |
| --- | --- |
| CLIN | Artifact |
| 0001AA | Contractor Project Management Plan (CPMP) |
| 0001AB | Monthly Progress Report |
| 0003AA | Master Test Plan |

# Work Planned

The following work is planned for the January 1, 2019 to January 31, 2019 PoP.

* Continue the IOC pre-production and production testing.
* Continue updating the test framework.
* Facilitate weekly status meetings.
* Transition the AbleVets PM work from Nilesh Lal to Savio Mendonsa.
* Update project documentation and prepare same for delivery.

# Risks and Issues

There are no known risks and issues currently. After successful ATO approval and access to IOC sites all the risks and issues were resolved. Appendix: Acronyms and Abbreviations

Table 2 lists the acronyms and abbreviations used in this document with their descriptions.

Table 2: 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 |