**EPMO System Security Categorization Report**

**VistA Adaptive Maintenance (VAM)**

*April 08th, 2019*

# System Identification

|  |  |
| --- | --- |
| **From Risk Vision** | |
| **System Name** | VistA Adaptive Maintenance |
| **Acronym** | VAM |
| **RV Unique Identifier** | 029-555555302 |
| **Related Data from VASI** | |
| **System Type** | Support System |
| **VA Business Reference Model (BRM) Capabilities** | Provide Health Care Administration Provide Information Technology Services |
| **BRM Functions** | Manage Health Care Costs and Administrative Efficiency Provide and Maintain IT Infrastructure |
| **BRM Business Functions** | Manage Data Center |

For additional information on this information system (IS), see the following sections at the end of this report, as extracted from Risk Vision:

[System Description - Risk Vision](#_bookmark1) [Owners – Risk Vision](#_bookmark2)

# Information System Security Category

As described in FIPS 200, following the high watermark concept, **VistA Adaptive Maintenance (VAM) Assessing** is a **High** impact system.

Using the notation in FIPS 199 the security category of this information system is:

**SC VistA Adaptive Maintenance (VAM) Assessing**: **confidentiality** = HIGH; **integrity** = HIGH; **availability** = HIGH

The system security category is based on the potential impact assessments for loss of each security objective for each identified information type (SP 800-60 Volume 2):

SC Health Care Delivery Services = (**confidentiality** = HIGH), (**integrity** = HIGH), (**availability** = HIGH)

SC Health Care Research and Practitioner Education = (**confidentiality** = HIGH), (**integrity** = HIGH), (**availability** = HIGH)

# Categorization Detail

On 9/26/2018, 1/25/2019, 1/28/2019, 04/09/2019 selected system stakeholders and EPMO IA personnel listed in the [Categorization Review Team](#_bookmark0)s table met to categorize the system using procedures based on VA

Handbook 6500, FIPS 199, and NIST SP 800-60. A member of the EPMO IA team led the discussion, assisting the system stakeholders in identifying information types in accordance with SP 800-60, then defining specific potential results from losing each of the security objectives of confidentiality, integrity, and availability (C-I-A), as defined in FIPS 199. The team used information type definitions and C-I-A descriptions from SP 800-60 Volume 2 and considered whether any Special Factors existed for each information type.

As each results statement was confirmed, the team applied the potential impact level definitions from FIPS 199 and determined the information type potential impact categories for the security objectives.

To save time, if any security objective impact was set to HIGH for one information type, the team did not consider that objective for subsequent information types. The team used this approach because that one HIGH value drives the High Water Mark (FIPS 200) impact category for that objective. As long as the team identified only LOW or MODERATE impacts, they continued to consider all three security objectives for each information type. Using this process ensures that each security objective receives the correct High Water Mark potential impact level, but may not provide analysis for all three objectives for every identified information type.

# Potential Impact Analysis

The system stakeholder identified the following information types as stored or processed in the information system, and described the operational results detailed below for the loss of each security objective. The team then mapped those results to the potential impact level shown.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **800-60**  **Para** | **Information Type** | **Security Objective** | **Result of Loss** | **Impact** |
| **D.14.4** | **Health Care Delivery Services** | Confidentiality | This system has PHI and PII; loss of confidentiality would be a violation of the Privacy Act and HIPAA. Loss of any PHI/PII would cause loss of reputation to the VA if the confidentiality were to be compromised. Such PHI includes highly sensitive information such as mental health data, HIV, cancer, psychiatric history, substance abuse, and criminal history. Any unauthorized disclosure of information would be embarrassing for the patients and could negatively affect the patients' ability to find employment. This could cause severe hardship to veteran and could contribute to or even cause possible suicide. | **HIGH** |
| Integrity | Loss of integrity would cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions. | **HIGH** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **800-60**  **Para** | **Information Type** | **Security Objective** | **Result of Loss** | **Impact** |
|  |  |  | There could be loss of life due to any possible medical errors. For example, an allergy could be listed incorrectly or not be listed, which would result in the patient losing their life. |  |
| Availability | Loss of availability would cause severe or catastrophic adverse effect to the agency's operations and the Veteran. Safe health care delivery would be disrupted greatly. This could cause loss of life as the critical health information would not be available to save patients' lives.  The disaster recovery plan includes a read-only system and read-only access, but there would be no capability to do order entry or any transactions. For example, one would not be able to order medications and lab tests for medications. | **HIGH** |
| **D.14.5** | **Health Care Research and Practitioner Education** | Confidentiality | This system has PHI and PII; loss of confidentiality would be a violation of the Privacy Act and HIPAA. Loss of any PHI/PII would cause loss of reputation to the VA if the confidentiality were to be compromised. Such PHI includes highly sensitive information such as mental health data, HIV, cancer, psychiatric history, substance abuse, and criminal history. Any unauthorized disclosure of information would be embarrassing for the patients and could negatively affect the patients' ability to find employment. This could cause severe hardship to veteran and could contribute to or even cause possible suicide. | **HIGH** |
| Integrity | Loss of integrity would cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions. | **HIGH** |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **800-60**  **Para** | **Information Type** | **Security Objective** | **Result of Loss** | **Impact** |
|  |  |  | There could be loss of life due to any possible medical errors. For example, an allergy could be listed incorrectly or not be listed, which would result in the patient losing their life. |  |
| Availability | Loss of availability would cause severe or catastrophic adverse effect to the agency's operations and the Veteran. Safe health care delivery would be disrupted greatly. This could cause loss of life as the critical health information would not be available to save patients' lives. The disaster recovery plan would be a read- only system to allow read-only access, but there would be no capability to do order entry or any transactions. For example, one would not be able to order medications and lab tests for medications. | **HIGH** |
| **Categorization Revi** | |  | | |

# Categorization Review Teams

***System Stakeholders/Participants***

|  |  |  |
| --- | --- | --- |
| **Name** | **e-Mail** | **Role** |
| Rafael Richards | rafael.richards@va.gov | Business Owner |
| Bobbi Begay | [bobbi.begay@va.gov](mailto:bobbi.begay@va.gov) | ISO |
| Christopher Brown | [christopher.brown1@va.gov](mailto:christopher.brown1@va.gov) | System Owner |

***EPMO IA Team***

|  |  |  |
| --- | --- | --- |
| **Name** | **e-Mail** | **Role** |
| Bayo Iferika | [Bayo.iferika@va.gov](mailto:Bayo.iferika@va.gov) | Team Lead |
| Abbas Ali | [Abbas.Ali3@va.gov](mailto:Abbas.Ali3@va.gov) | IT Specialist |
| Bailey G. Zhang | [Bailey.Zhang@va.gov](mailto:Bailey.Zhang@va.gov) | Statistical Analyst |
| Edmund Addei | [Edmund.Addei@va.gov](mailto:Edmund.Addei@va.gov) | IA Analyst |

**System Description – Risk Vision**

The **VistA Adaptive Maintenance system** is a Cloud-Smart / Cloud-Native application developed and deployed in the dedicated U.S. FedRAMP-HIGH, HIPAA-compliant VA Enterprise Cloud (VAEC) leveraging Amazon Web Services (AWS) commercial cloud infrastructure and services. VAM provides comprehensive, commercial cloud-based monitoring and security for all clients, applications, and users that access VistA data using VistA’s Remote Procedure Call (RPC) interface. VAM is operationalized and scaled for production enterprise’s use in the VAEC leveraging AWS Kinesis and AWS CloudWatch, 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 to any VistA system required.

# Owners – Risk Vision



|  |  |
| --- | --- |
| **Name** | **Role** |
| Rafael Richards | Business Owner (BO) |
| Christopher Brown | System Owner (SO) |
| Bobbi Begay | Information Security Officer (ISO) |
| Bill James | Authorizing Official (AO) |
| EPMO ATO Review Team (3 Members) | CIO |
| EPMO Team (35 Members) | System Steward |
| OCS - CA (9 Members) | Certification Authority (CA) |
| OCS Review Team (5 Members) | OCS |
| OIS ADAS Team (1 Member) | ADAS |
| David Faulkner | System Steward (Security) |
| Nilesh Lal | System Steward |
| William P. McDonough | System Steward |
| Robert Ballon | System Steward |

**EPMO Security Categorization Report:**

**APPROVAL**

VistA Adaptive Maintenance (VAM)

**System Owner**

Name: Christopher Brown

Date: Signature:

**Information Security Officer**

Name: Bobbi Begay

Date: Signature:

**Disposition**

Once all required approvals are recorded on this report, post a copy as a permanent artifact in the system record in the VA Governance, Risk, & Compliance (GRC) system.

**References**

|  |  |
| --- | --- |
| **Document** | **Title** |
| VA Handbook 6500 | Risk Management Framework for VA Information Systems - Tier 3: VA  Information Security Program |
| FIPS 199 | Standards for Security Categorization of Federal Information and Information Systems |
| FIPS 200 | Minimum Security Requirements for Federal Information and  Information Systems |
| NIST SP 800-60, Vol I, Revision 1 | Guide for Mapping Types of Information and Information Systems to Security Categories |
| NIST SP 800-60, Vol II, Revision 1 | Appendices: Guide for Mapping Types of Information and Information  Systems to Security Categories |