DEPARTMENT OF VETERANS AFFAIRS

VistA Adaptive Maintenance (VAM)

029-555555302

SYSTEM SECURITY PLAN

Generated September 12, 2018

Contents

1.0 SYSTEM IDENTIFICATION 4

2.0 SECURITY CONTROL IDENTIFICATION 12

3.0 CONTROL RESULTS 13

- Access Control 13
- Authority and Purpose 42
- Accountability, Audit, and Risk Management 43
- Awareness and Training 48
- Audit and Accountability 51
- Certification, Accreditation, and Security Assessments 68
- Configuration Management 77
- Contingency Planning 97
- Data Quality and Integrity 121
- Data Minimization and Retention 124
- Identification and Authentication 127
- Individual Participation and Redress 144
- Incident Response 147
- Maintenance 157
- Media Protection 165
- Physical and Environmental Protection 172
- Planning 188
- Program Management 193
- Personnel Security 204
- Risk Assessment 210
- System and Services Acquisition 216
- System and Communications Protection 228
- Security 248
- System and Information Integrity 249
- Transparency 268
- Use Limitation 270

Appendix A References 272

Appendix B Acronyms List 273

Appendix C Glossary 275

Change Management

The VistA Adaptive Maintenance (VAM) System Security Plan (SSP) is a formal living document that provides an overview of the security requirements and describes the security controls in place to meet those requirements. The SSP is required for Assessment and Authorization of an information system per FISMA and Federal Regulations. Additionally, the VistA Adaptive Maintenance (VAM) Security Team was given guidance by the VA Office of Cyber Security (OCS) to follow the National Institute of Standards and Technology, NIST 800-37 Guide for the Security Assessment and Authorization of Federal Information Systems methodology for the Assessment and Authorization (A&A) of the VistA Adaptive Maintenance (VAM). Per NIST requirements the VistA Adaptive Maintenance (VAM) Security Team will use NIST 800-18 "Guide for Developing Security Plans for Information Technology Systems", to develop the SSP format which will provide the Veterans Affairs (VA) standardized approach across the VA enterprise.

Per NIST 800-37 the A&A process consists of four distinct phases, with requirements for updating the SSP at the end of each phase. The SSP contains both technical information and policy requirements derived from system vulnerability scans, system design documentation, VA security policies, and the security assessment that will be conducted by the VistA Adaptive Maintenance (VAM) Security Team. The SSP will be used by individuals responsible for IT security at the system level and at the organization level to ensure that the VistA Adaptive Maintenance (VAM) system security requirements are met according to VA and Federal policies and guidelines.

Changes to the SSP will only be performed by the VistA Adaptive Maintenance (VAM) Security Team or VistA Adaptive Maintenance (VAM) System Stewards with ISO approval. This is necessary to preserve the impartial and unbiased nature of the information contained within the SSP. This ensures that the Authorizing Official receives the most objective information possible in order to make accreditation decisions regarding VistA Adaptive Maintenance (VAM).

In addition, the VistA Adaptive Maintenance (VAM) SSP contains Sensitive but Unclassified information and security information and all government employees or government contractor employees are obligated to protect this information from unauthorized disclosure and cannot be distributed outside of the Department of Veterans Affairs.

Executive Summary

The objective of system security planning is to improve protection of information technology (IT) resources. All federal systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan. The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, Computer Security Act of 1987.

The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager. Additional information may be included in the basic plan and the structure and format organized according to agency needs, so long as the major sections described in this document are adequately covered and readily identifiable.

In order for the plans to adequately reflect the protection of the resources, a management official must authorize a system to process information or operate. The authorization of a system to process information, granted by a management official, provides an important quality control. By authorizing processing in a system, the manager accepts its associated risk.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the security plan establishes and documents the security controls, it should form the basis for the authorization, supplemented by more specific studies as needed. In addition, a periodic review of controls should also contribute to future authorizations. If the AO deems the VA-level risk acceptable, an ATO is issued. The AO may issue an ATO with specific terms and conditions associated with the ATO for up to 36 months. The termination date indicates when the security authorization expires. The authorization termination date is not required when the ISCM program provides the AO with the needed information to conduct ongoing risk determination and risk acceptance activities.

1.0 SYSTEM IDENTIFICATION

1.1 System Name/Identifier

System Name: VistA Adaptive Maintenance (VAM)

System Acronym: VAM

Unique Identifier: 029-555555302

System Type: Major Application

1.2 System Categorization

Exhibit 1: Sensitivity Levels and Description

Sensitivity Level	Description of Sensitivity Level
High	*Data stored, processed, or transported by computer or telecommunications resources, the inaccuracy, alteration, disclosure, or unavailability of which:* • Would have an **IRREPARABLE IMPACT** on Major Application or General Support System (GSS), functions, image, or reputation, such that the catastrophic result would not be able to be repaired or set right again, or • Could result in **LOSS OF MAJOR TANGIBLE ASSETS** or resources, including posing a threat to human life
Moderate	*Data stored, processed, or transported by computer or telecommunications resources, the inaccuracy, alteration, disclosure, or unavailability of which:* • Would have an **ADVERSE IMPACT** on Major Application or General Support System (GSS), functions, image, or reputation, such that the impact would place the Major Application at a significant disadvantage, or • Could result in **LOSS OF SIGNIFICANT TANGIBLE ASSETS** or resources.
Low	*Data stored, processed, or transported by computer or telecommunications resources, the inaccuracy, alteration, disclosure, or unavailability of which:* • Would have an **MINIMAL IMPACT** on Major Application or General Support System (GSS), functions, image, or reputation, such that the catastrophic result would not be able to be repaired or set right again, or • Could result in **LOSS OF SOME TANGIBLE ASSETS** or resources. ***Systems that contain Personal Identifiable Information (PII) are automatically either a moderate or high level sensitivity and cannot be low sensitivity.***

General Description of Information Sensitivity

In accordance with Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, information categorization is calculated based on the three basic security objectives: confidentiality, integrity, and availability. NIST Publication 800-60 *Guide for Mapping Types of Information and Information System to Security Categories* provides implementation guidance in completing this activity.

Exhibit 2: Information Categories

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. ***Systems that contain Personal Identifiable Information (PII) may not be low for confidentiality and must be either a moderate or high***	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. ***Systems that contain Personal Identifiable Information (PII) may not be low for integrity and must be either a moderate or high***	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Protection/Certification Requirements

The following table describes the information system categorization. For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information that residents on the information system.

Exhibit 3: Information System Categorization

Security Objective	Ranking
Confidentiality	High
Integrity	High
Availability	High
Security Category (SC) =	**High**

1.3 System Owner

For all phases the responsible System Owner and organizations include:

Dick Rickard

null

Richard.Rickard@va.gov

The responsible organization owns the system, the data it contains, and controls the use of the data

1.4 Authorizing Official

The designated person formally assumes responsibility for the operations of VistA Adaptive Maintenance (VAM) Assessing at an acceptable level of risk to agency operations, agency assets, or individuals:

Bill James

202-632-7390

bill.james@va.gov

1.5 Assignment of Security Responsibility/Other Designated Contacts

The designated person(s) have sufficient knowledge of the system to be able to provide additional information or points of contact regarding the security plan and the system, as needed. Include the designated person(s) responsible for the security of the system that have been assigned responsibility in writing to ensure that the Major Application has adequate security and is knowledgeable of the management, operational, and technical controls used to protect the system.

RiskVision System Role	Name	Email/Phone
Information Security Officer (ISO)	Bobbi Begay	Bobbi.Begay@va.gov 303.331.7837
Information Security Officer (ISO)	Charles Adejumo	Charles.Adejumo@va.gov 703 645-0420
System Owner	Dick Rickard	Richard.Rickard@va.gov
System Steward	Badhan Mandal	badhan.mandal@va.gov
System Steward	Dick Rickard	Richard.Rickard@va.gov
System Steward	John Allen	john.allen4@va.gov 703-407-5437

Table 1: Security Responsibility/Other Designated Contacts

1.6 Information System Operational Status

For each system the status is:

System	Status
VistA Adaptive Maintenance (VAM)	Acquisitions / Development

Table 2: System Status

1.7 Information System Type

Major Application	**[X]**	**General Support System**	**[ ]**	**Program**	**[ ]**	**Unassigned**	**[ ]**

1.8 General Description and Purpose

The purpose of the VistA Adaptive Maintenance (VAM) project is to establish a secure, sustainable, high-performing, cloud-based service to implement provider workflow logic back-end processing and storage. The VAM service will replicate the Remote Procedure Call (RPC) functionality currently provided via VistA in a modern, well-documented platform (i.e., Node.js and NoSQL database). VAM will enable the incremental transition of clinical workflow logic out of VistA into VAM services, while maintaining full compatibility with current VistA clients such as CPRS. VAM will be hosted in production within the VA's Enterprise Cloud (VAEC) using the Amazon Web Services (AWS) service provider.

1.9 System Environment

VISTA Adaptive Maintenance (VAM) VAM will be deployed within the VA's Enterprise Cloud using Amazon Web Services (AWS) and Amazon CloudWatch.

Facility Code	Address	City	State

Table 3a: Facilities

Information System	Operating System	Number of Components

Table 3b: Major Equipment List

1.10 System Interconnections/Information Sharing

Source Name	Relationship Name	Target Name

See CA-3 for a list of ISA/MOUs. A Facility Compliance Report may need to be pulled to see individual facility interconnections

Table 4: System Interconnections

The following System of Record Notices (SORN) have been identified for the VistA Adaptive Maintenance (VAM)

Not Applicable

1.11.1 Risk Summary

The results of the VistA Adaptive Maintenance (VAM) Reporting Risk Assessment indicated that the risks to system resources are as follows:

Summarize risk assessment findings below

• The most significant control related risks include CA-8.1, PM-1.1, PM-2.1, PM-3.1, PM-4.1, PM-5.1, PM-6.1, PM-7.1, PM-8.1, PM-9.1, PM-10.1, PM-11.1, PM-12.1, PM-13.1, PM-14.1, PM-15.1, PM-16.1, RA-5.E4, CM-5.E1, CM-6.1, CM-6.E2, CM-7.1, CM-7.E1, CM-7.E2, CM-7.E5, CP-3.1, CP-3.E1, CP-4.1, CP-4.E1, CP-10.E2, CP-10.E4, SI-2.1, SI-4.E2, SI-7.1, SI-7.E1, SI-7.E2, SI-7.E5, SI-7.E7, SI-11.1, SI-16.1, AC-6.E1, AC-6.E3, AC-7.1, AC-14.1, AC-17.1, AC-17.E1, AC-17.E2, AC-17.E3, AC-17.E4, AC-18.1, AC-18.E4, AC-19.1, AC-19.E5, AC-20.E1, AC-20.E2, AC-22.1, AU-8.1, AU-8.E1, AU-10.1, IA-2.E12, SC-2.1, SC-10.1, SC-12.1, SC-12.E1

Risks in areas such as natural, environmental, human intentional and human unintentional threats were assessed.

1.11.2 Threat Description

A threat is defined as anything or anyone having the potential to negatively affect the security posture of the system or acquire unauthorized access to information contained on the system. Threats can be categorized as intentional or unintentional and initiated by human or natural causes. Threats and vulnerabilities should be considered against the criticality of the general security requirements for the system.

The probable threats to the VistA Adaptive Maintenance (VAM) Reporting, along with the likelihood and impact of the threats, are identified in Table 5.

Threat	Threat Category	Likelihood Rating	Impact Rating	Raw Score	Risk Level

Table 5: Threat Description

1.12 Related Laws, Regulations, and Policies

- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- 17 U.S.C. 106, Exclusive rights in copyrighted works
- 18 U.S.C. 1030 (a) (3), "Fraud and related activity in connection with computers."
- 21 U.S.C., Food and Drugs
- 38 U.S.C. 218, "Security and law enforcement on property under the jurisdiction of the Veterans Administration"
- 38 U.S.C. 3301, "Confidential nature of claims"
- 38 U.S.C. 3305, "Confidentiality of medical quality assurance records"
- 38 U.S.C. Section 44132 covers Drug and Alcohol treatment and scheduling records
- PL 100-322 covers the confidentiality of AIDS patients data
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- Government Paperwork Elimination Act (GPEA), PL 105-277
- OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- Executive Order 13103, Computer Software Piracy
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- FIPS 201-1, Personal Identity Verification of Federal Employees and Contractors
- FIPS 140-2, Security Requirements for Cryptographic Module

2.0 SECURITY CONTROL IDENTIFICATION

This section summarizes the management, operational and technical control requirements for the system and shows their status (in place, planned or in place and planned and type of control).

Control Status Summary Table

NIST SP800-53 Rev4	In Place (Pass)	Planned (Fail)	Common	Hybrid (*)	System Specific (*)	Unknown Type (*)
Access Control	27	16	0	28	15	0
Accountability, Audit, and Risk Management	0	0	0	8	0	0
Audit and Accountability	25	3	0	11	17	0
Authority and Purpose	0	0	0	2	0	0
Awareness and Training	5	0	0	5	0	0
Certification, Accreditation, and Security Assessments	11	1	0	12	0	0
Configuration Management	24	7	0	21	11	0
Contingency Planning	29	6	0	25	11	0
Data Minimization and Retention	0	0	0	6	0	0
Data Quality and Integrity	0	0	0	5	0	0
Identification and Authentication	23	1	0	23	1	0
Incident Response	16	0	0	16	1	0
Individual Participation and Redress	0	0	0	6	0	0
Information Security Programs	0	16	16	0	0	0
Maintenance	13	0	0	12	2	0
Media Protection	12	0	0	8	4	0
Personnel Security	9	0	0	7	3	0
Physical and Environmental Protection	26	0	0	12	16	0
Planning	6	0	0	5	2	0
Risk Assessment	7	1	0	5	4	0
Security	0	0	0	2	0	0
System and Communications Protection	26	4	0	23	7	0
System and Information Integrity	18	9	0	17	12	0
System and Services Acquisition	18	0	0	12	6	0
Transparency	0	0	0	5	0	0
Use Limitation	0	0	0	2	0	0

Table 6: Control Status Summary Table

3.0 CONTROL RESULTS

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-01.1 Access Control Policy And Procedures	**AC-01.1 Access Control Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from OI&T. OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Access Control Policy is reviewed every five (5) years.
OI&T:
a. Develops, documents, and disseminates to defined personnel or roles (See Attachment 2):
1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
b. Reviews and updates the current:
1. Access control policy ; and
2. Access control procedures

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-02.1 Account Management	**AC-02.1 Account Management** The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	**Status** In Place (Pass): X Planned or In Place and Planned (Fail): **Type** Common: Hybrid: X System Specific:

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High Assessing and Enterprise Operations (EO).
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-02.E01 Account Management | Automated System Account Management	**AC-02.E01 Account Management | Automated System Account Management** The organization employs automated mechanisms to support the management of information system accounts.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and VAEC AWS GovCloud High
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-02.E02 Account Management | Removal Of Temporary / Emergency Accounts	**AC-02.E02 Account Management | Removal Of Temporary / Emergency Accounts** The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and VAEC AWS GovCloud High Assessing .
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-02.E03 Account Management | Disable Inactive Accounts	**AC-02.E03 Account Management | Disable Inactive Accounts** The information system automatically disables inactive accounts after [Assignment: organization-defined time period].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and VAEC AWS GovCloud High Assessing.
Inactive accounts are automatically disabled after 90 days of inactivity, in accordance with VA Handbook 6500. This is implemented by VA Microsoft Active Directory (AD) Group Policy (GPO). AD services are controlled and managed by VA AD Team.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-02.E04 Account Management | Automated Audit Actions	**AC-02.E04 Account Management | Automated Audit Actions** The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and NSOC.
SIEM Splunk is managed by the NSOC that alerts and notifies requisite personnel, such as the ISO, of abnormalities. VAEC utilizes VA Active Directory services for authentication, and as such, the account creation, modification, disabling, enabling and removal of accounts are managed by the VA AD team.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-02.E05 Account Management | Inactivity Logout	**AC-02.E05 Account Management | Inactivity Logout** The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and VAEC AWS GovCloud High Assessing. VA requires that users log out when a time period of expected inactivity has occurred or describes when to log out.

User sessions are disconnected after 15 minutes of inactivity. This is implemented by Microsoft AD GPO. AD services are controlled and managed by VA AD Team. In accordance with VA Handbook 6500, users should actively lock/log off their sessions once they are finished with their work.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-02.E11 Account Management | Usage Conditions	**AC-02.E11 Account Management | Usage Conditions** The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].	Status: In Place (Pass): X; Planned or In Place and Planned (Fail): Type: Common: ; Hybrid: ; System Specific: X

Status		Type	
In Place (Pass)	X	Common	
Planned or In Place and Planned (Fail)		Hybrid	
		System Specific	X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
Inherited from VAEC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-02.E12 Account Management | Account Monitoring / Atypical Usage	**AC-02.E12 Account Management | Account Monitoring / Atypical Usage** The organization: (a) Monitors information system accounts for [Assignment: organization-defined atypical usage]; and (b) Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and NSOC. VAEC AWS GovCloud High sends all event logs to VA SIEM Splunk for real-time monitoring. Monitoring is performed by the VA NSOC 24x7/365, and they identify abnormalities. Splunk is controlled and managed by the VA NSOC. The VA NSOC notifies the VA Incident Response team in the event of any abnormalities.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-02.E13 Account Management | Disable Accounts For High-Risk Individuals	**AC-02.E13 Account Management | Disable Accounts For High-Risk Individuals** The organization disables accounts of users posing a significant risk within [Assignment: organization-defined time period] of discovery of the risk.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and VAEC AWS GovCloud High Assessing.
The VAEC AWS GovCloud High disables accounts of users posing a significant risk immediately upon discovery of the risk.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-03.1 Access Enforcement	**AC-03.1 Access Enforcement** The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and VAEC AWS GovCloud High Assessing.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-04.1 Information Flow Enforcement	**AC-04.1 Information Flow Enforcement** The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:

This control is inherited from the VAEC AWS and VA NSOC. In accordance with VA Handbook 6500, the VAEC AWS GovCloud High system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on VA-NSOC flow control policy.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-05.1 Separation Of Duties	**AC-05.1 Separation Of Duties** The organization: a. Separates [Assignment: organization-defined duties of individuals]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and VAEC AWS GovCloud High Assessing.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-06.1 Least Privilege	**AC-06.1 Least Privilege** The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and VAEC AWS GovCloud High Assessing.
OI&T employs the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with VA missions and business functions.
In accordance with VA Handbook 6500, VAEC AWS GovCloud High employs least privilege. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Additionally, VAEC Microsoft AWS GovCloud High applies least privilege to the development, implementation, and operation of organizational information systems.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-06.E01 Least Privilege | Authorize Access To Security Functions	**AC-06.E01 Least Privilege | Authorize Access To Security Functions** The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].	**Status**: In Place (Pass) — ; Planned or In Place and Planned (Fail) — X **Type**: Common — ; Hybrid — ; System Specific — X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
OI&T explicitly authorizes access to security functions and security-relevant information.
In accordance with the VA Handbook 6500, VAM explicity authorizes access to system security files, system management/configuration files, and creation of system accounts and shared drives or other protected files. Initial configuration of these resources are based on approved baselines and all changes must follow the change management process. Authorized access to security functions are listed in the VA NSOC SOP.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-06.E02 Least Privilege | Non-Privileged Access For Nonsecurity Functions	**AC-06.E02 Least Privilege | Non-Privileged Access For Nonsecurity Functions** The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.	**Status**: In Place (Pass) — X; Planned or In Place and Planned (Fail) — **Type**: Common — ; Hybrid — ; System Specific — X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations. In accordance with VA Handbook 6500, VAM requires users accessing security functions or security relevant information to authenticate with a non-privileged account or role, when accessing nonsecurity function.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-06.E03 Least Privilege | Network Access To Privileged Commands	**AC-06.E03 Least Privilege | Network Access To Privileged Commands** The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.	**Status** In Place (Pass): Planned or In Place and Planned (Fail): X **Type** Common: Hybrid: System Specific: X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations.
OI&T authorizes network access to privileged commands only for compelling operational needs and documents the rationale for such access in the security plan for the information system.
In accordance with VA Handbook 6500, VAM authorizes network access to the Information System Owner/Delegate determines the network accessed privileged commands and operational needs are documented in the Account Management Plan, All privileged access must go through ePAS.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-06.E05 Least Privilege | Privileged Accounts	**AC-06.E05 Least Privilege | Privileged Accounts** The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and VAEC AWS GovCloud. In accordance with VA Handbook 6500, VAEC AWS GovCloud High reviews all accounts at a minimum, semiannually. The
review identifies when accounts are no longer required, users that are terminated or transferred, and when users' information system usage or need-to-know changes. A report is submitted to the requisite account manager for review and verification. VAEC AWS GovCloud High reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-06.E09 Least Privilege | Auditing Use Of Privileged Functions	**AC-06.E09 Least Privilege | Auditing Use Of Privileged Functions** The information system audits the execution of privileged functions.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and NSOC.
VA NSOC operates and manages Splunk. The VA NSOC audits the execution of privileged functions
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-06.E10 Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions	**AC-06.E10 Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions** The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA Enterprise Operations and OI&T.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-07.1 Unsuccessful Logon Attempts	**AC-07.1 Unsuccessful Logon Attempts** The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
a. In accordance with VA Handbook 6500, VAM enforces a limit of five unsuccessful attempts during a one day (24 hour) period.
b. In accordance with VA Handbook 6500, VAM automatically locks the account until released by Administrator when the maximum number of unsuccessful attempts is exceeded.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-08.1 System Use Notification	**AC-08.1 System Use Notification** The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information [Assignment: organization-defined conditions], before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems	**Status**: In Place (Pass) [X]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VAEC.
a. In accordance with VA Handbook 6500, VAM displays to users a system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The banner message includes the information that users are accessing a U.S. Government information system, information system usage may be monitored, recorded, and subject to audit, unauthorized use of the information system is prohibited and subject to criminal and civil penalties, and use of the information system indicates consent to monitoring and recording.
b. VAM retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.
c. In accordance with VA Handbook 6500, VAM displays system use information for publicly accessible systems displays system use information conditions, before granting further access. The VAM Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities and includes a description of the authorized uses of the system.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-10.1 Concurrent Session Control	**AC-10.1 Concurrent Session Control** The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].	

Status		Type	
In Place (Pass)	X	Common	
Planned or In Place and Planned (Fail)		Hybrid	
		System Specific	X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
In accordance with VA Handbook 6500, VAM limits the number of concurrent sessions for each account to three sessions for general users and five sessions for users with elevated privileges. Additionally, nonprivileged user concurrent sessions are defined by the Information System Owner/Delegate.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-11.1 Session Lock	**AC-11.1 Session Lock** The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
a. In accordance with VA Handbook 6500, the VAM prevents further access to the system by initiating a session lock after a maximum of fifteen minutes of inactivity or upon receiving a request from a user. Requests for increased time for specific individuals will be approved by the Information System Owner/Delegate, local CIO or designee.
b. In accordance with VA Handbook 6500, the VAM Retains the session lock until released by Administrator.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-11.E01 Session Lock | Pattern-Hiding Displays	**AC-11.E01 Session Lock | Pattern-Hiding Displays** The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM conceals, via the session lock, information previously visible on the display with a publicly viewable image
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-12.1 Session Termination	**AC-12.1 Session Termination** The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
In accordance with the VA Handbook 6500, termination of user sessions and conditions or trigger evets requiring session disconnect are documented in the Account Management Plan. Termination of the user session occurs after 15 minutes.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-14.1 Permitted Actions Without Identification Or Authentication	**AC-14.1 Permitted Actions Without Identification Or Authentication** The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.	**Status** / **Type** In Place (Pass): ☐ — Common: ☐ Planned or In Place and Planned (Fail): X — Hybrid: ☐ System Specific: X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
a. VAM requires all applications/systems to be authenticated prior to access.
b. VAM prohibits all activities that do not require identification and authentication to the system.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

CP-2, IA-2.

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-17.1 Remote Access	**AC-17.1 Remote Access** The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
a. To obtain access to VAM, users must be within the VA network. Remote users are required to VPN into the VA network to gain connectivity. VPN is controlled and managed by the VA NSOC. VAM utilizes PIV (certificate) and/or token-based authentication for multifactor authentication. User restrictions are documented within the Account Management Plan.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-17.E01 Remote Access | Automated Monitoring / Control	**AC-17.E01 Remote Access | Automated Monitoring / Control** The information system monitors and controls remote access methods.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO and VAEC. All logs are forwarded to the VA NSOC SIEM Splunk. Splunk is controlled and managed by the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-17.E02 Remote Access | Protection Of Confidentiality / Integrity Using Encryption	**AC-17.E02 Remote Access | Protection Of Confidentiality / Integrity Using Encryption** The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from VAEC.
Remote access to and within VAEC is protected by using secure protocols.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-17.E03 Remote Access | Managed Access Control Points	**AC-17.E03 Remote Access | Managed Access Control Points** The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] Type: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and NSOC. Access to VAM traverses the VA Trusted Internet Connection (TIC). TIC connections are monitored
and controlled by the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-17.E04 Remote Access | Privileged Commands / Access	**AC-17.E04 Remote Access | Privileged Commands / Access** The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and (b) Documents the rationale for such access in the security plan for the information system.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] Type: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
a. In accordance with VA Handbook 6500 VAM requires execution of privileged commands and
access to security-relevant information via remote access only. Users accessing security functions or security relevant information to authenticate with a non-privileged account or role, when accessing nonsecurity function. Users must have two accounts on all these boxes.

For VAM, all account requests are submitted via the VA Service Desk Manager (SDM) ticketing system rationale/justification for such access.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

AC-6.

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-18.1 Wireless Access	**AC-18.1 Wireless Access** The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is N/A
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-18.E01 Wireless Access | Authentication And Encryption	**AC-18.E01 Wireless Access | Authentication And Encryption** The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is N/A.

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-18.E04 Wireless Access | Restrict Configurations By Users	**AC-18.E04 Wireless Access | Restrict Configurations By Users** The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.	Status: In Place (Pass); Planned or In Place and Planned (Fail) X Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:

This control is N/A

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-18.E05 Wireless Access | Antennas / Transmission Power Levels	**AC-18.E05 Wireless Access | Antennas / Transmission Power Levels** The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is N/A
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-19.1 Access Control For Mobile Devices	**AC-19.1 Access Control For Mobile Devices** The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.	**Status**: In Place (Pass); Planned or In Place and Planned (Fail) X **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is N/A.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-19.E05 Access Control For Mobile Devices | Full Device / Container-Based Encryption	**AC-19.E05 Access Control For Mobile Devices | Full Device / Container-Based Encryption** The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is N/A.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-20.1 Use Of External Information Systems	**AC-20.1 Use Of External Information Systems** The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
In accordance with VA Handbook 6500, external system access, and any storage, processing, or transmission of information requires an interconnection agreement that must define terms and conditions consistent with any trust relationship. Additionally, agreements with external parties must be approved by the Authorizing Official (AO).
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-20.E01 Use Of External Information Systems | Limits On Authorized Use	**AC-20.E01 Use Of External Information Systems | Limits On Authorized Use** The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.	**Status**: In Place (Pass); Planned or In Place and Planned (Fail) X **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
In accordance with VA Handbook 6500, external system access, and any storage, processing, or transmission of information requires an interconnection agreement that must define terms and conditions consistent with any trust relationship. Additionally, agreements with external parties must be approved by the Authorizing Official (AO).
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-20.E02 Use Of External Information Systems | Portable Storage Devices	**AC-20.E02 Use Of External Information Systems | Portable Storage Devices** The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
In accordance with VA Handbook 6500, VAM restricts or prohibits the use of VA-controlled portable storage devices by authorized individuals on external information systems.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-21.1 Information Sharing	**AC-21.1 Information Sharing** The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM complies with VA Handbook 6500.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AC-22.1 Publicly Accessible Content	**AC-22.1 Publicly Accessible Content** The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.	**Status**: In Place (Pass); Planned or In Place and Planned (Fail) X **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC.
The VAEC does not have any publicly accessible content.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AP-01.1 Authority To Collect	**AP-01.1 Authority To Collect** The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AP-02.1 Purpose Specification	**AP-02.1 Purpose Specification** The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AR-01.1 Governance And Privacy Program	**AR-01.1 Governance And Privacy Program** The organization: a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems; b. Monitors federal privacy laws and policy for changes that affect the privacy program; c. Allocates[Assignment: organization-defined allocation of budget and staffing] sufficient resources to implement and operate the organization-wide privacy program; d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and f. Updates privacy plan, policies, and procedures [Assignment: organization-defined frequency,at least biennially].	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AR-02.1 Privacy Impact And Risk Assessment	**AR-02.1 Privacy Impact And Risk Assessment** The organization: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AR-03.1 Privacy Requirements For Contractors And Service Providers	**AR-03.1 Privacy Requirements For Contractors And Service Providers** The organization: a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and b. Includes privacy requirements in contracts and other acquisition-related documents	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

AR-1, AR-5, SA-4.

Control (*)	Description of Control (*)	Control Status/Type (*)
AR-04.1 Privacy Monitoring And Auditing	**AR-04.1 Privacy Monitoring And Auditing** The organization monitors and audits privacy controls and internal privacy policy [Assignment: organization-defined frequency] to ensure effective implementation.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

AR-6, AR-7, AU-1, AU-2,
AU-3, AU-6, AU-12, CA-7, TR-1, UL-2.

Control (*)	Description of Control (*)	Control Status/Type (*)
AR-05.1 Privacy Awareness And Training	**AR-05.1 Privacy Awareness And Training** The organization: a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; b. Administers basic privacy training [Assignment: organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [Assignment: organization-defined frequency, at least annually]; and c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

[Assignment: organization-defined frequency, at least annually].

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

AR-3, AT-2, AT-3, TR-1.

Control (*)	Description of Control (*)	Control Status/Type (*)
AR-06.1 Privacy Reporting	**AR-06.1 Privacy Reporting** The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.	**Status**: In Place (Pass) ☐; Planned or In Place and Planned (Fail) ☐ **Type**: Common ☐; Hybrid X; System Specific ☐

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AR-07.1 Privacy-Enhanced System Design And Development	**AR-07.1 Privacy-Enhanced System Design And Development** The organization designs information systems to support privacy by automating privacy controls.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

AC-6, AR-4, AR-5, DM-2, TR-1.

Control (*)	Description of Control (*)	Control Status/Type (*)
AR-08.1 Accounting Of Disclosures	**AR-08.1 Accounting Of Disclosures** The organization: a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made; b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and c. Makes the accounting of disclosures available to the person named in the record upon request.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

IP-2.

Control (*)	Description of Control (*)	Control Status/Type (*)
AT-01.1 Security Awareness And Training Policy And Procedures	**AT-01.1 Security Awareness And Training Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy [Assignment: organization-defined frequency]; and 2. Security awareness and training procedures [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA Enterprise Operations. The OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Awareness and Training Policy is reviewed every five (5) years.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AT-02.1 Security Awareness Training	**AT-02.1 Security Awareness Training** The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The OI&T provides basic security awareness training to all users (including managers, senior executives, and contractors) of VA Information systems or VA information on an annual basis.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AT-02.E02 Practical Exercises | Insider Threat	**AT-02.E02 Practical Exercises | Insider Threat** The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA Enterprise Operations. The OI&T includes security awareness training on recognizing and reporting potential indicators of insider threat.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AT-03.1 Role-Based Security Training	**AT-03.1 Role-Based Security Training** The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA Enterprise Operations.
Role-Based Training is given through the Talent Management System (TMS) in VA. Information Technology Workforce Development has developed IT competency modeling for the workforce. Information Assurance is a core competency across the Department (includes annual awareness training and on-going training through such modalities as the Information Security Focus Campaign, Information Protection Week, etc.). Through competency modeling, higher proficiencies (higher level of training) are identified for the Information Assurance competency. These higher levels of required knowledge/skill are added to the identified staff's (e.g., System Administrators, Network Administrators, Database Administrators) competency profiles and role-based training for "those with significant responsibilities" are incorporated IT Workforce Development Portal for Role-Based Training.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AT-04.1 Security Training Records	**AT-04.1 Security Training Records** The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [Assignment: organization-defined time period].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA Enterprise Operations.
All required security related training is documented and tracked in the VA Talent Management System (TMS). TMS reports can be pulled at any time via the user or TMS manager access. TMS will send timely notifications to remind users of upcoming required training due. Additionally SDE maintains a listing of compliant/non-compliant OIT staff and contractors (see evidence) Per VA Handbook 6500 individual

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-01.1 Audit And Accountability Policy And Procedures	**AU-01.1 Audit And Accountability Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy [Assignment: organization-defined frequency]; and 2. Audit and accountability procedures [Assignment: organization-defined frequency].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA Enterprise Operations. OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Audit Control Policy is reviewed every five (5) years.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-02.1 Audit Events	**AU-02.1 Audit Events** The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High Assessing and VA NSOC.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-02.E03 Audit Events | Reviews And Updates	**AU-02.E03 Audit Events | Reviews And Updates** The organization reviews and updates the audited events [Assignment: organization-defined frequency].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High Assessing.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-03.1 Content Of Audit Records	**AU-03.1 Content Of Audit Records** The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High Assessing.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-03.E01 Content Of Audit Records | Additional Audit Information	**AU-03.E01 Content Of Audit Records | Additional Audit Information** The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High Assessing
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-03.E02 Content Of Audit Records | Centralized Management Of Planned Audit Record Content	**AU-03.E02 Content Of Audit Records | Centralized Management Of Planned Audit Record Content** The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High Assessing and VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-04.1 Audit Storage Capacity	**AU-04.1 Audit Storage Capacity** The information system off-loads audit records [Assignment: organization-defined frequency] onto a different system or media than the system being audited.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) — **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-05.1 Response To Audit Processing Failures	**AU-05.1 Response To Audit Processing Failures** The information system: a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-05.E01 Response To Audit Processing Failures | Audit Storage Capacity	**AU-05.E01 Response To Audit Processing Failures | Audit Storage Capacity** The information system provides a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit record storage capacity.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-05.E02 Response To Audit Processing Failures | Real-Time Alerts	**AU-05.E02 Response To Audit Processing Failures | Real-Time Alerts** The information system provides an alert in [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-06.1 Audit Review	**AU-06.1 Audit Review** The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and b. Reports findings to [Assignment: organization-defined personnel or roles].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-06.E01 Audit Review | Process Integration	**AU-06.E01 Audit Review | Process Integration** The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-06.E03 Audit Review | Correlate Audit Repositories	**AU-06.E03 Audit Review | Correlate Audit Repositories** The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-06.E05 Audit Review | Integration / Scanning And Monitoring Capabilities	**AU-06.E05 Audit Review | Integration / Scanning And Monitoring Capabilities** The organization integrates analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-06.E06 Audit Review | Correlation With Physical Monitoring	**AU-06.E06 Audit Review | Correlation With Physical Monitoring** The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-07.1 Audit Reduction And Report Generation	**AU-07.1 Audit Reduction And Report Generation** The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-07.E01 Audit And Accountability | Automatic Processing	**AU-07.E01 Audit And Accountability | Automatic Processing** The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-08.1 Time Stamps	**AU-08.1 Time Stamps** The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-08.E01 Time Stamps | Synchronization With Authoritative Time Source	**AU-08.E01 Time Stamps | Synchronization With Authoritative Time Source** The information system: (a) Compares the internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and (b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-09.1 Protection Of Audit Information	**AU-09.1 Protection Of Audit Information** The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is a VA core service. This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-09.E02 Protection Of Audit Information | Audit Backup On Separate Physical Systems / Components	**AU-09.E02 Protection Of Audit Information | Audit Backup On Separate Physical Systems / Components** The information system backs up audit records [Assignment: organization-defined frequency] onto a physically different system or system component than the system or component being audited.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-09.E03 Protection Of Audit Information | Cryptographic Protection	**AU-09.E03 Protection Of Audit Information | Cryptographic Protection** The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-09.E04 Protection Of Audit Information | Access By Subset Of Privileged Users	**AU-09.E04 Protection Of Audit Information | Access By Subset Of Privileged Users** The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-10.1 Non-Repudiation	**AU-10.1 Non-Repudiation** The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].	**Status**: In Place (Pass); Planned or In Place and Planned (Fail) X **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and NSOC
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-11.1 Audit Record Retention	**AU-11.1 Audit Record Retention** The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-12.1 Audit Generation	**AU-12.1 Audit Generation** The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-12.E01 Audit Generation | System-Wide / Time-Correlated Audit Trail	**AU-12.E01 Audit Generation | System-Wide / Time-Correlated Audit Trail** The information system compiles audit records from [Assignment: organization-defined information system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
AU-12.E03 Audit Generation | Changes By Authorized Individuals	**AU-12.E03 Audit Generation | Changes By Authorized Individuals** The information system provides the capability for [Assignment: organization-defined individuals or roles] to change the auditing to be performed on [Assignment: organization-defined information system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CA-01.1 Security Assessment And Authorization Policy And Procedures	**CA-01.1 Security Assessment And Authorization Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and 2. Security assessment and authorization procedures [Assignment: organization-defined frequency].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from OI&T. The OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Security Assessment and Authorization Policy is reviewed every five (5) years. The VAEC AWS GovCloud High develops and maintains SOPs as needed.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CA-02.1 Security Assessments	**CA-02.1 Security Assessments** The organization: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from Enterprise Operations. The GRC RiskVision Tool generates the SSP. This System Security plan follows NIST 800-53, revision 4 and addresses each applicable control and enhancement for HIGH systems. The Office of Cyber Security puts out an annual assessment each year for systems to complete that have not had a full SCA within the prior 12 months. This annual assessment consists of approximately 1/3 of the total required controls. This serves as continuous monitoring.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CA-02.E01 Security Assessments | Independent Assessors	**CA-02.E01 Security Assessments | Independent Assessors** The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from OCS and OCS employs independent assessors or assessment teams to conduct SCAs. These are external assessors or internal assessors outside of OIS.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CA-02.E02 Security Assessments | Specialized Assessments	**CA-02.E02 Security Assessments | Specialized Assessments** The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is partially inherited from OCS as they provide control assessment services to the VA at large. Testing may be included as part of SCAs, other types of testing as part of initial security authorizations and the continuous monitoring process where the frequency is determined by the Information Security Continuous Monitoring program. OCS, in conjunction with VAEC, performs in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessments; performance/load testing as needed.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CA-03.1 System Interconnections	**CA-03.1 System Interconnections** The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM will be hosted in production within the VA's Enterprise Cloud (VAEC) using Amazon Web Services (AWS) and leverage the AWS CloudWatch service.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CA-03.E05 System Interconnections | Restrictions On External System Connections	**CA-03.E05 System Interconnections | Restrictions On External System Connections** The organization employs [Selection: allow-all, deny-by-exception; deny-all, permit-by-exception] policy for allowing [Assignment: organization-defined information systems] to connect to external information systems.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM will be hosted in production within the VA's Enterprise Cloud (VAEC) using Amazon Web Services (AWS) and leverage the AWS CloudWatch service.
a. VAEC AWS GovCloud authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements (ISA)/Memorandums of Understanding (MOU);
b. VAEC AWS GovCloud High documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. VAEC AWS GovCloud High reviews and updates Interconnection Security Agreements (ISA)/Memorandums of Understanding (MOU) annually.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CA-05.1 Plan Of Action And Milestones	**CA-05.1 Plan Of Action And Milestones** The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM develops POA&Ms for the information system to document the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. POA&Ms are documented, tracked, and managed using RiskVison.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CA-06.1 Security Authorization	**CA-06.1 Security Authorization** The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VA:
a. Assigns a senior-level executive or manager to the role of AO for the information system;
b. Ensures that the AO authorizes the information system for processing before commencing operations; and
c. Ongoing security authorization through implementation of the Information Security Continuous Monitoring program and when a significant change in the system or major change in the data occurs.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CA-07.1 Continuous Monitoring	**CA-07.1 Continuous Monitoring** The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].	<table><tr><th>Status</th><th></th><th>Type</th><th></th></tr><tr><td>In Place (Pass)</td><td>X</td><td>Common</td><td></td></tr><tr><td rowspan="2">Planned or In Place and Planned (Fail)</td><td rowspan="2"></td><td>Hybrid</td><td>X</td></tr><tr><td>System Specific</td><td></td></tr></table>

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from Enterprise Operations (EO). The OI&T develops a continuous monitoring strategy and implements a continuous monitoring program that includes:
a. Establishing metrics to be monitored, which is determined by the Information Security Continuous Monitoring program.
b. Establishment of risk-based tiers of security controls tested on the frequency outlined in VA's Information Security Continuous Monitoring Security Control Evaluation Plan created and maintained by OCS;
c. Ongoing SCAs in accordance with VA’s continuous monitoring strategy; and
d. Ongoing security status monitoring of organization-defined metrics in accordance with VA’s continuous monitoring strategy;
e. Correlation and analysis of security-related information generated by assessments and monitoring;
f. Response actions to address results of the analysis of security-related information; and
g. Reporting the security status of VA and the
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CA-07.E01 Continuous Monitoring | Independent Assessment	**CA-07.E01 Continuous Monitoring | Independent Assessment** The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA Enterprise Operations (EO). The OIS employs assessors or assessment teams to monitor the security controls in the information system on an ongoing basis. The AO determines the required degree of independence for assessors for continuous monitoring.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CA-08.1 Penetration Testing	**CA-08.1 Penetration Testing** The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].	Status: In Place (Pass); Planned or In Place and Planned (Fail) X Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The OI&T conducts penetration testing quarterly on one-fourth of the total number of VA High systems.
VAM conducts penetration testing every 3 months.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CA-09.1 Internal System Connections	**CA-09.1 Internal System Connections** The organization: a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM is comprised of 4 major architectural components:
Veteran Integrated Care Services (VICS) Server – Software component that comprises the individual Node.js-based services that comprise the overall suite of VAM services (called VICS). Service requests and associated data are sent from the client (e.g. CPRS, other) to the RPC Router and/or directly to VICS Server.
RPC Router – implemented in Node.js, the Router received RPC requests from the client (e.g. CPRS, other) and forwards the RPC call to either the legacy VistA endpoint or to the cloud-based VICS Server for processing. The RPC Router is only used for client applications that leverage the legacy CPRS/VistA RPC calling format.
Traffic between the RPC router and VICS and between new clients and VICS over REST will be encrypted, and the effectiveness of that encryption will be tested. If Veteran Affairs add traffic encryption into and out of CPRS, VAM will add support to the router and test that encryption as well. Additionally, the RPC Router provides an auditing capability for all RPC traffic.
RPC Router Manager – Manages configuration and auditing of the RPC Router.
NoSQL JSON Datastore – Stores PII/PHI and non-PII/PHI electronic health record (EHR) data within FIPS 140-2 cryptographic modules for processing by the VICS services.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-01.1 Configuration Management Policy And Procedures	**CM-01.1 Configuration Management Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy [Assignment: organization-defined frequency]; and 2. Configuration management procedures [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VAEC AWS GovCloud High inherits this control from OI&T. OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Configuration Management Policy is reviewed every five (5) years.
VAM Configuration Management Plan has been developed to follow OI&T.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-02.1 Baseline Configuration	**CM-02.1 Baseline Configuration** The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM develops, documents, and maintains configuration control, a current baseline configuration of the information system. Baseline configurations are developed and documented in the VAM Configuration Management Plan (CMP).
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-02.E01 Baseline Configuration | Reviews And Updates	**CM-02.E01 Baseline Configuration | Reviews And Updates** The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency]; (b) When required due to [Assignment organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM reviews and updates the baseline configurations at least annually or when any change occurs that affects the baseline configurations.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-02.E02 Baseline Configuration | Automation Support For Accuracy / Currency	**CM-02.E02 Baseline Configuration | Automation Support For Accuracy / Currency** The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM uses Jazz/Rational to employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-02.E03 Baseline Configuration | Retention Of Previous Configurations	**CM-02.E03 Baseline Configuration | Retention Of Previous Configurations** The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM retains previous versions of baseline configurations of the information system to support rollback.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-02.E07 Baseline Configuration | Configure Systems	**CM-02.E07 Baseline Configuration | Configure Systems** The organization: (a) Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and (b) Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM is a cloud-based system; therefore, this control enhancement is not applicable.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-03.1 Configuration Change Control	**CM-03.1 Configuration Change Control** The organization: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; f. Audits and reviews activities associated with configuration-controlled changes to the	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

information system; and g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM uses the SCM approved tools such as Jazz/Rational for configuration change control.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-03.E01 Configuration Change Control | Automated Document / Notification / Prohibition Of Changes	**CM-03.E01 Configuration Change Control | Automated Document / Notification / Prohibition Of Changes** The organization employs automated mechanisms to: (a) Document proposed changes to the information system; (b) Notify [Assignment: organized-defined approval authorities] of proposed changes to the information system and request change approval; (c) Highlight proposed changes to the information system that have not been approved or disapproved by [Assignment: organization-defined time period]; (d) Prohibit changes to the information system until designated approvals are received; (e) Document all changes to the information system; and (f) Notify [Assignment: organization-defined personnel] when approved changes to the information system are completed.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM utilizes SCM approved tools such as Jazz/Rationaldocument changes, notify individuals of
changes to be reviewed and approved, highlights changes that are pending approval/disapproval and notifies requisite personnel when approved changes are completed.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-03.E02 Configuration Change Control | Test / Validate / Document Changes	**CM-03.E02 Configuration Change Control | Test / Validate / Document Changes** The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	**Status** In Place (Pass): X Planned or In Place and Planned (Fail): **Type** Common: Hybrid: X System Specific:

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM tests, validates, and documents changes to the information system before implementing the changes on the operational system.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-04.1 Security Impact Analysis	**CM-04.1 Security Impact Analysis** The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM analyzes changes to the information system to determine potential security impacts prior to change implementation.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-04.E01 Security Impact Analysis | Separate Test Environments	**CM-04.E01 Security Impact Analysis | Separate Test Environments** The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM analyzes changes to the information system in a separate test environment such as the Dev environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-05.1 Access Restrictions For Change	**CM-05.1 Access Restrictions For Change** The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM utilizes a work flow change management process through the Jazz/Rational tools that defines, documents, approves all proposed changes prior to implementation. Only system engineers with privileged access have logical access to make changes to the operational environment.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-05.E01 Access Restrictions For Change | Automated Access Enforcement / Auditing	**CM-05.E01 Access Restrictions For Change | Automated Access Enforcement / Auditing** The information system enforces access restrictions and supports auditing of the enforcement actions.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM enforces access to only approved VA PIV owners who will support sustainment/maintenance work for VAM.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-05.E02 Access Restrictions For Change | Review System Changes	**CM-05.E02 Access Restrictions For Change | Review System Changes** The organization reviews information system changes [Assignment: organization-defined frequency] and [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.	**Status**: In Place (Pass) [X]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM utilizes Jazz/Rational for identifying changes. Changes are reviewed monthly per the VA 6500 Handbook.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-05.E03 Access Restrictions For Change | Signed Components	**CM-05.E03 Access Restrictions For Change | Signed Components** The information system prevents the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM prevents the installation of unauthorized software without verification that the software has been digitally signed using a certificate (administrator token) that is recognized and approved by the organization. Changes to the operational environment must go through the change management process that verifies the integrity of the software/code to be installed. VAM only installs software in accordance with the TRM list that is vetted and approved by the VA.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-06.1 Configuration Settings	**CM-06.1 Configuration Settings** The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM submits tickets through ESCCB for changes to configuration settings. The Process consists of the following:
1. Enter the BPE Connection ID.
2. Enter the name of the Business Partner.
3. Enter the name of the VA Program the access will support.
4. List the communications.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-06.E01 Configuration Settings | Automated Central Management / Application / Verification	**CM-06.E01 Configuration Settings | Automated Central Management / Application / Verification** The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components].	**Status**: In Place (Pass) [X]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM employs Jazz/Rational to centrally manage, apply, and verify configuration settings.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-06.E02 Configuration Settings | Respond To Unauthorized Changes	**CM-06.E02 Configuration Settings | Respond To Unauthorized Changes** The organization employs [Assignment: organization-defined security safeguards] to respond to unauthorized changes to [Assignment: organization-defined configuration settings].	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from OI&T.
OI&T employs security safeguards to respond to unauthorized changes to VA-defined configuration settings. VAM submits tickets through ESCCB for changes to configuration settings. The Process consists of the following:
1. Enter the BPE Connection ID.
2. Enter the name of the Business Partner.
3. Enter the name of the VA Program the access will support.
4. List the communications.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-07.1 Least Functionality	**CM-07.1 Least Functionality** The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VAM Information System Owner configures VAM to provide only essential capabilities and prohibits or restricts the use of other identified functions, ports, protocols, and/or services.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-07.E01 Least Functionality | Periodic Review	**CM-07.E01 Least Functionality | Periodic Review** The organization: (a) Reviews the information system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and (b) Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure].	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VAM Information System Owner:
a. Reviews VAM to identify unnecessary and/or non-secure functions, ports, protocols, and services and
b. Disables functions, ports, protocols, and services within VAM deemed to be unneccesary and/or non-secure
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-07.E02 Least Functionality | Prevent Program Execution	**CM-07.E02 Least Functionality | Prevent Program Execution** The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].	**Status**: In Place (Pass) — ; Planned or In Place and Planned (Fail) — X **Type**: Common — ; Hybrid — ; System Specific — X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VAM Information System Owner prevents program execution in accordance with one or more of the following specifications: VA policies regarding software usage and restrictions and/or rules authorizing the terms and conditions of software program usage.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-07.E05 Least Functionality | Authorized Software / Whitelisting	**CM-07.E05 Least Functionality | Authorized Software / Whitelisting** The organization: (a) Identifies [Assignment: organization-defined software programs authorized to execute on the information system]; (b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and (c) Reviews and updates the list of authorized software programs [Assignment: organization-defined frequency].	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM follows VAEC policy.
The Information System Owner:
a. Identifies software programs authorized to execute on the information system and reviews and updates the list of authorized software programs
b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and
c. Reviews and updates the list of authorized software programs
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-08.1 Information System Component Inventory	**CM-08.1 Information System Component Inventory** The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].	**Status**: In Place (Pass) [X]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC .
VAM also has it's own boundaries which uses VAEC.
OI&T:
a. Develops and documents an inventory of information system components that:
1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes information necessary for effective information system component accountability
b. Reviews and updates the information system component inventory
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-08.E01 Information System Component Inventory | Updates During Installations / Removals	**CM-08.E01 Information System Component Inventory | Updates During Installations / Removals** The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	**Status** In Place (Pass): X Planned or In Place and Planned (Fail): **Type** Common: Hybrid: X System Specific:

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC.
OI&T updates the inventory of information system components as an integral part of component installations, removals, and information system updates.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-08.E02 Information System Component Inventory | Automated Maintenance	**CM-08.E02 Information System Component Inventory | Automated Maintenance** The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High Assessing.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-08.E03 Information System Component Inventory | Automated Unauthorized Component Detection	**CM-08.E03 Information System Component Inventory | Automated Unauthorized Component Detection** The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and (b) Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO. VA OI&T SDE and the NSOC employs automated mechanisms (SCCM, BigFix, etc.) to continuously detect the presence of unauthorized hardware, software, and firmware components within the information system (as a series of dashboards). These dashboards provide updates on software versioning, hardware specifications (age, model number, etc) and if unauthorized will indicate in the report and unauthorized devices OI&T personnel can run reports to check for unapproved software.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-08.E04 Information System Component Inventory | Accountability Information	**CM-08.E04 Information System Component Inventory | Accountability Information** The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible/accountable for administering those components.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VAM System Owner is responsible for maintaining an accurate and complete inventory listing of components within the VAM and VAEC AWS GovCloud High system boundary.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-08.E05 Information System Component Inventory | No Duplicate Accounting Of Components	**CM-08.E05 Information System Component Inventory | No Duplicate Accounting Of Components** The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VAM System Owner is responsible for verifying that all components within the authorization boundary of the information system are not duplicated in other information system inventories.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-09.1 Configuration Management Plan	**CM-09.1 Configuration Management Plan** The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM develops, documents, and implements a configuration management plan for the information system that:
a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the information system and places the configuration items under configuration management; and
d. Protects the configuration management plan from unauthorized disclosure and modification.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-10.1 Software Usage Restrictions	**CM-10.1 Software Usage Restrictions** The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
Only authorized software is allowed to be used within the environment. An approved list can be found within TRM. In addition, SCM is used to track versioning, software and licensing. OI&T has the ability to run remove software or take other action if needed.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CM-11.1 User-Installed Software	**CM-11.1 User-Installed Software** The organization: a. Establishes [Assignment: organization-defined policies] governing the installation of software by users; b. Enforces software installation policies through [Assignment: organization-defined methods]; and c. Monitors policy compliance at [Assignment: organization-defined frequency].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
Users are restricted from installing software if elevated privileges (EP) are not assigned. EP is assigned to those with a valid need. OI&T or designated individuals may only install software that is listed in TRM and must comply with licensing. Software compliancy can be verified via BigFix, SCCM, and other tools the VA may see fit.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-01.1 Contingency Planning Policy And Procedures	**CP-01.1 Contingency Planning Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy [Assignment: organization-defined frequency]; and 2. Contingency planning procedures [Assignment: organization-defined frequency].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM inherits this control from OI&T. OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Contingency Planning Policy is reviewed every five (5) years.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-02.1 Contingency Plan	**CP-02.1 Contingency Plan** The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification.	**Status** In Place (Pass): X Planned or In Place and Planned (Fail): **Type** Common: Hybrid: X System Specific: X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
a. The VAM contingency plan for the information system identifies core essential missions and business functions and associated contingency requirements. These essential services are:
Server Configuration Management Service, Code Configuration and Release Management Services, Authentication Services, Auditing Service, Monitoring Service, Vulnerability Scanning Service, JumpBox Service Recovery objectives, restoration priorities, and metrics are defined in the VAM contingency plan. The contingency plan also addresses contingency roles, responsibilities, assigned individuals with contact information, missions/business functions in the case of system disruption/compromise/failure, and full system restoration - without deterioration of the security safeguards originally planned and implemented. The contingency plan is reviewed and approved by the VAM system owner.
b. The VAM distribution list is documented in the contingency management plan. The contingency plan is distributed using a shared web portal.
c. VAM coordinates contingency planning activities with incident handling activities with the VA NSOC.

d. VAM reviews the contingency plan for the information system annually and when one or more significant changes are made.
e. The VAM updates the contingency plan on an annual basis or as needed to address changes to the information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing
f. The VAM distribution list is documented in the contingency management plan. The contingency plan is shared using a shared web portal.
g. The portal that is used to distribute and share the contingency plan is restricted to on the requisite personnel.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-02.E01 Contingency Plan | Coordinate With Related Plans	**CP-02.E01 Contingency Plan | Coordinate With Related Plans** The organization coordinates contingency plan development with organizational elements responsible for related plans.	

Status		Type	
In Place (Pass)	X	Common	
Planned or In Place and Planned (Fail)		Hybrid	X
		System Specific	

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-02.E02 Contingency Plan | Capacity Planning	**CP-02.E02 Contingency Plan | Capacity Planning** The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM conducts capacity planning annually, or as new systems are added to the environment, or if there are any significant changes to the environment.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-02.E03 Contingency Plan | Resume Essential Missions / Business Functions	**CP-02.E03 Contingency Plan | Resume Essential Missions / Business Functions** The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM plans for the resumption of essential missions and business functions is based on the RPO and RTO documented in the contingency plan.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-02.E04 Contingency Plan | Resume All Missions / Business Functions	**CP-02.E04 Contingency Plan | Resume All Missions / Business Functions** The organization plans for the resumption of all missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM plans for the resumption of all missions and business functions is based on the RPO and RTO documented in the contingency plan.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-02.E05 Contingency Plan | Continue Essential Missions / Business Functions	**CP-02.E05 Contingency Plan | Continue Essential Missions / Business Functions** The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM plans for the continuance of essential missions and business functions based on the RPO, RTO, and MTD requirements of the VAEC AWS GovCloud High core services or hosted applications. The continuance of missions and functions anticipate little or no loss of operational continuity and sustain that continuity until full information system restoration at primary processing and/or storage sites.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-02.E08 Contingency Plan | Identify Critical Assets	**CP-02.E08 Contingency Plan | Identify Critical Assets** The organization identifies critical information system assets supporting essential missions and business functions.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM identifies and documents critical information system assets supporting essential missions and business functions for core services and hosted applications in the contingency plan.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-03.1 Contingency Training	**CP-03.1 Contingency Training** The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
In accordance with VA Handbook 6500, VAM provides contingency training to information system
users with assigned contingency planning roles and responsibilities. On an annual basis, additional training is provided during ISCP testing.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-03.E01 Contingency Training | Simulated Events	**CP-03.E01 Contingency Training | Simulated Events** The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] Type: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM annually incorporates simulated events on core services and hosted applications into contingency training exercises to facilitate effective response by personnel in crisis situations.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-04.1 Contingency Plan Testing	**CP-04.1 Contingency Plan Testing** The organization: a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] Type: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM conducts an annual functional exercise to determine the effectiveness of the current contingency plan and to identify weaknesses. Test results are analyzed and reviewed to identify shortcomings. Corrective actions are developed and implented per lessons learned.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-04.E01 Contingency Plan Testing | Coordinate With Related Plans	**CP-04.E01 Contingency Plan Testing | Coordinate With Related Plans** The organization coordinates contingency plan testing with organizational elements responsible for related plans.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM coordinates contingency plan testing with the system owner and Information Security.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-04.E02 Contingency Plan Testing | Alternate Processing Site	**CP-04.E02 Contingency Plan Testing | Alternate Processing Site** The organization tests the contingency plan at the alternate processing site: (a) To familiarize contingency personnel with the facility and available resources; and (b) To evaluate the capabilities of the alternate processing site to support contingency operations.	**Status**: In Place (Pass) [X]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-06.1 Alternate Storage Site	**CP-06.1 Alternate Storage Site** The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-06.E01 Alternate Storage Site | Separation From Primary Site	**CP-06.E01 Alternate Storage Site | Separation From Primary Site** The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-06.E02 Alternate Storage Site | Recovery Time / Point Objectives	**CP-06.E02 Alternate Storage Site | Recovery Time / Point Objectives** The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-06.E03 Alternate Storage Site | Accessibility	**CP-06.E03 Alternate Storage Site | Accessibility** The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-07.1 Alternate Processing Site	**CP-07.1 Alternate Processing Site** The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-07.E01 Alternate Processing Site | Separation From Primary Site	**CP-07.E01 Alternate Processing Site | Separation From Primary Site** The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-07.E02 Alternate Processing Site | Accessibility	**CP-07.E02 Alternate Processing Site | Accessibility** The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-07.E03 Alternate Processing Site | Priority Of Service	**CP-07.E03 Alternate Processing Site | Priority Of Service** The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-07.E04 Alternate Processing Site | Preparation For Use	**CP-07.E04 Alternate Processing Site | Preparation For Use** The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-08.1 Telecommunications Services	**CP-08.1 Telecommunications Services** The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High and VA EO. The VAEC AWS GovCloud High is designed for High-Availability (HA) with duplicate AWS direct connect and a backup VPN
connection. All connections flow traverse VA TIC and is managed by VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-08.E01 Telecommunications Services | Priority Of Service Provisions	**CP-08.E01 Telecommunications Services | Priority Of Service Provisions** The organization: (a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and (b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High and VA EO. The VAEC AWS GovCloud High is designed for High-Availability (HA) with duplicate AWS direct connect and a backup VPN
connection. All connections flow traverse VA TIC and is managed by VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-08.E02 Telecommunications Services | Single Points Of Failure	**CP-08.E02 Telecommunications Services | Single Points Of Failure** The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High and VA EO. The VAEC AWS GovCloud High is designed for High-Availability (HA) with duplicate AWS direct connect and a backup VPN
connection. All connections flow traverse VA TIC and is managed by VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-08.E03 Telecommunications Services | Separation Of Primary / Alternate Providers	**CP-08.E03 Telecommunications Services | Separation Of Primary / Alternate Providers** The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High and VA EO. The VAEC AWS GovCloud High is designed for High-Availability (HA) with duplicate AWS direct connect and a backup VPN
connection. All connections flow traverse VA TIC and is managed by VA NSOC
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-08.E04 Telecommunications Services | Provider Contingency Plan	**CP-08.E04 Telecommunications Services | Provider Contingency Plan** The organization: (a) Requires primary and alternate telecommunications service providers to have contingency plans; (b) Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and (c) Obtains evidence of contingency testing/training by providers [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High and VA EO. The VAEC AWS GovCloud High is designed for High-Availability (HA) with duplicate AWS direct connect and a backup VPN
connection. All connections flow traverse VA TIC and is managed by VA NSOC
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-09.1 Information System Backup	**CP-09.1 Information System Backup** The organization: a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-09.E01 Information System Backup | Testing For Reliability / Integrity	**CP-09.E01 Information System Backup | Testing For Reliability / Integrity** The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
The VAEC AWS GovCloud High tests backup information annually or as needed to verify media reliability and information integrity.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-09.E02 Information System Backup | Test Restoration Using Sampling	**CP-09.E02 Information System Backup | Test Restoration Using Sampling** The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
The VAEC AWS GovCloud High uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-09.E03 Information System Backup | Separate Storage For Critical Information	**CP-09.E03 Information System Backup | Separate Storage For Critical Information** The organization stores backup copies of [Assignment: organization-defined critical information system software and other security-related information] in a separate facility or in a fire-rated container that is not collocated with the operational system.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
The VAEC AWS GovCloud High stores backup copies of all data in separate alternative AWS availability zones (AZ1 and AZ2).
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-09.E05 Information System Backup | Transfer To Alternate Storage Site	**CP-09.E05 Information System Backup | Transfer To Alternate Storage Site** The organization transfers information system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-10.1 Information System Recovery And Reconstitution	**CP-10.1 Information System Recovery And Reconstitution** The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
The VAEC AWS GovCloud High provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery and reconstitution procedures are documented in the contingency plan.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-10.E02 Information System Recovery And Reconstitution | Transaction Recovery	**CP-10.E02 Information System Recovery And Reconstitution | Transaction Recovery** The information system implements transaction recovery for systems that are transaction-based.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
CP-10.E04 Information System Recovery And Reconstitution | Restore Within Time Period	**CP-10.E04 Information System Recovery And Reconstitution | Restore Within Time Period** The organization provides the capability to restore information system components within [Assignment: organization-defined restoration time-periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
DI-01.1 Data Quality	**DI-01.1 Data Quality** The organization: a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; b. Collects PII directly from the individual to the greatest extent practicable; c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems[Assignment: organization-defined frequency]; and d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
DI-01.E01 Data Quality | Validate Pii	**DI-01.E01 Data Quality | Validate Pii** The organization requests that the individual or individual's authorized representative validate PII during the collection process.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
DI-01.E02 Data Quality | Re-Validate Pii	**DI-01.E02 Data Quality | Re-Validate Pii** The organization requests that the individual or individual's authorized representative revalidate that PII collected is still accurate [Assignment: organization-defined frequency].	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
DI-02.1 Data Integrity And Data Integrity Board	**DI-02.1 Data Integrity And Data Integrity Board** The organization: a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements123 and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
DI-02.E01 Data Integrity And Data Integrity Board | Publish Agreements On Website	**DI-02.E01 Data Integrity And Data Integrity Board | Publish Agreements On Website** The organization publishes Computer Matching Agreements on its public website.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
DM-01.1 Minimization Of Personally Identifiable Information	**DM-01.1 Minimization Of Personally Identifiable Information** The organization: a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose	**Status** / **Type** In Place (Pass) — Common Planned or In Place and Planned (Fail) — Hybrid: X System Specific

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
DM-01.E01 Minimization Of Personally Identifiable Information | Locate / Remove / Redact / Anonymize Pii	**DM-01.E01 Minimization Of Personally Identifiable Information | Locate / Remove / Redact / Anonymize Pii** The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
DM-02.1 Data Retention And Disposal	**DM-02.1 Data Retention And Disposal** The organization: a. Retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
DM-02.E01 Data Retention And Disposal | System Configuration	**DM-02.E01 Data Retention And Disposal | System Configuration** The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
DM-03.1 Minimization Of Pii Used In Testing, Training, And Research	**DM-03.1 Minimization Of Pii Used In Testing, Training, And Research** The organization: a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and b. Implements controls to protect PII used for testing, training, and research.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
DM-03.E01 Minimization Of Pii Used In Testing, Training, And Research | Risk Minimization Techniques	**DM-03.E01 Minimization Of Pii Used In Testing, Training, And Research | Risk Minimization Techniques** The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-01.1 Identification And Authentication Policy And Procedures	**IA-01.1 Identification And Authentication Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: 1. Identification and authentication policy [Assignment: organization-defined frequency]; and 2. Identification and authentication procedures [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA OI&T. The OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Identification and Authentication Policy is reviewed every five (5) years.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-02.1 Identification And Authentication (Organizational Users)	**IA-02.1 Identification And Authentication (Organizational Users)** The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The RPC protocol is connection-oriented and synchronous with clients opening a connection to VistA and only making new RPC calls after receiving a reply from a previous call.
Connection establishment and ending define a “client session” in the RPC engine and all RPC traffic on that connection is identified with that session.
Clients log into VistA in different ways – there are Connection Proxies, CAPRI tokens, BSE tokens, Access Verify, SAML tokens. Each method is recognized by the Router and allows it to associate a client’s identity with the session. It is important to note that the Router doesn’t implement authentication – it merely notes how VistA responds to different sign on options and changes the client session appropriately.
Session identity and details are passed into RPC Handlers along with a parsed version of an RPC
An RPC Handler may signal the Router engine to end a session

The VAEC AWS GovCloud High requires all users to uniquely authenticate to the system prior to performing any actions. Users connect to the system using VA-issued two-factor authentication and service accounts also use unique IDs.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-02.E01 Identification And Authentication (Organizational Users) | Network Access To Privileged Accounts	**IA-02.E01 Identification And Authentication (Organizational Users) | Network Access To Privileged Accounts** The information system implements multifactor authentication for network access to privileged accounts.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO and managed by VA NSOC.

To obtain access to the VAEC AWS GovCloud High environment, users must be within the VA network. Remote users are required to VPN into the VA network to gain connectivity. VAEC AWS GovCloud High utilizes PIV (certificate) and/or token-based authentication for multifactor authentication.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-02.E02 Identification And Authentication (Organizational Users) | Network Access To Non-Privileged Accounts	**IA-02.E02 Identification And Authentication (Organizational Users) | Network Access To Non-Privileged Accounts** The information system implements multifactor authentication for network access to non-privileged accounts.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is not applicable since the VAEC system has no "non-privileged users".
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-02.E03 Identification And Authentication (Organizational Users) | Local Access To Privileged Accounts	**IA-02.E03 Identification And Authentication (Organizational Users) | Local Access To Privileged Accounts** The information system implements multifactor authentication for local access to privileged accounts.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-02.E04 Identification And Authentication (Organizational Users) | Local Access To Non-Privileged Accounts	**IA-02.E04 Identification And Authentication (Organizational Users) | Local Access To Non-Privileged Accounts** The information system implements multifactor authentication for local access to non-privileged accounts.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-02.E08 Identification And Authentication (Organizational Users) | Network Access To Privileged Accounts - Replay Resistant	**IA-02.E08 Identification And Authentication (Organizational Users) | Network Access To Privileged Accounts - Replay Resistant** The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VAEC AWS GovCloud High utilizes VA PIV cards for authentication, which utilizes replay-resistant technologies.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-02.E09 Identification And Authentication (Organizational Users) | Network Access To Non-Privileged Accounts - Replay Resistant	**IA-02.E09 Identification And Authentication (Organizational Users) | Network Access To Non-Privileged Accounts - Replay Resistant** The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VAEC AWS GovCloud High only has privileged accounts accessing the environment. Therefore, this control enhancement is not applicable.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-02.E11 Identification And Authentication (Organizational Users) | Remote Access - Separate Device	**IA-02.E11 Identification And Authentication (Organizational Users) | Remote Access - Separate Device** The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is partially inherited from VA NSOC.
VAM components will be managed within a single security boundary, within VAEC.
VAM and its associated components (VICS Server, RPC Router, Router Manager, and Datastore) are all contained within a single security boundary within the VAEC using the AWS GovCloud High environment.
To obtain access to the VAEC AWS GovCloud High environment, users must be within the VA network. Remote users are

required to VPN into the VA network to gain connectivity. VPN is controlled and managed by the VA NSOC. VAEC AWS GovCloud High utilizes PIV (certificate) and/or token-based authentication for multifactor authentication.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-02.E12 Identification And Authentication (Organizational Users) | Acceptance Of Piv Credentials	**IA-02.E12 Identification And Authentication (Organizational Users) | Acceptance Of Piv Credentials** The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM plans to accept and verify PIV credentials using a centralized server managed by VA AD. AD services are controlled and managed by the VA AD Team.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-03.1 Device Identification And Authentication	**IA-03.1 Device Identification And Authentication** The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited fromo VAEC.
VAM follows the VAEC AWS GovCloud High which uniquely identifies all systems in the environment via unique identifier (UID). Devices are authenticated for network access based off the IP range of the environment.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-04.1 Identifier Management	**IA-04.1 Identifier Management** The organization manages information system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and e. Disabling the identifier after [Assignment: organization-defined time period of inactivity].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO and VAEC.
a. In accordance with VA Handbook 6500, the VAEC AWS GovCloud High accepts and verifies PIV credentials using a centralized server managed by VA AD. AD services are controlled and managed by the VA AD Team. The VAEC AWS GovCloud High requires all users to uniquely identify and authenticate to the system prior to establishing remote connections.

Access to all systems are entered into the SDM/CMDB system and the account manager authorizes access based on a valid need, intended system usage, and mission/business function.
b. VA AD team selects PIV cards that uniquely identify users. VAEC AWS GovCloud High uses IP addresses to identify cloudbased network access points/devices.
c. VA AD team assigns PIV cards that uniquely identify users. VAEC AWS GovCloud High uses IP addresses to identify cloudbased network access points/devices.
d. In accordance with VA Handbook 6500, the VAEC AWS GovCloud High prevents the reuse of identifiers for at least two years.
e. In accordance with VA Handbook 6500, the VAEC AWS GovCloud High manages information system identifiers for users and devices by disabling the identifier after ninety days of inactivity.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-05.1 Authenticator Management	**IA-05.1 Authenticator Management** The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
a. To obtain access VAM users must be within the VA network. Remote users are required to VPN into the VA network to gain connectivity. VPN is controlled and managed by the VA NSOC. Users connect to the system using VA-issued PIV cards managed by the OI&T. The AD team manages the underlying Microsoft AD infrastructure.
The OI&T verifies, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.
b. The OI&T establishes authenticator content for authenticators.

c. The OI&T ensures that authenticators have sufficient strength of mechanism for their intended use. Two-factor authentication is used for FIPS 140-2 compliant algorithms. The following setting are in place for all systems: Enforce password history - 24 passwords remembered, Maximum password age 90 days, Minimum password age 1 days, Minimum password length 8 characters, Password must meet complexity requirements.
d. The OI&T establishes and implements administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
e. The OI&T requires the changing of default content of authenticators prior to information system installation.
f. The OI&T establishes minimum (1 day) and maximum (90 days) lifetime restrictions and reuse conditions (24-password history) for authenticators.
G: The OI&T manages information system authenticators by changing/refreshing authenticators for single-factor authentication, user accounts will be changed every 90 days. For single-factor authentication, administrator accounts should be changed at a maximum of every 30 days and will be changed at a minimum of every 90 days. Service accounts will be changed at a minimum every 3 years.
h. The OI&T protects authenticator content from unauthorized disclosure and modification.
i. The OI&T requires individuals to take, and having devices implement, specific security safeguards to protect authenticators.
j. The OI&T changes authenticators for group/role accounts when membership to those accounts changes.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-05.E01 Authenticator Management | Password-Based Authentication	**IA-05.E01 Authenticator Management | Password-Based Authentication** The information system, for password-based authentication: (a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]; (b) Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number]; (c) Stores and transmits only cryptographically-protected passwords; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; (e) Prohibits password reuse for [Assignment: organization-defined number] generations; and (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
a. In accordance with VA Handbook 6500, the VAM users' passwords must contain at least 8 non-blank characters. Those 8 characters must contain characters from 3 of the following categories: English upper case letters, English lower case letters, Base 10 digits, and non-alphanumeric special characters. Six of the characters must not occur more than once in the password.

System administrator and service account passwords must contain at least 12 non-blank characters and use 3 of the 4 categories as outlined above.
b. When a user wants to change their password, VAM, in accordance with VA Handbook 6500, forces a user to change 4 characters from the old password to the new password.
c. VAM hashes all passwords using FIPS 140-2 compliant algorithms prior to storage and transmission.
d. VAM utilizes GPOs to enforce minimum (1 day) and maximum (90 days) lifetime restrictions and reuse conditions (24-password history) for authenticators.
e. In accordance with VA Handbook 6500, VAM prohibits the same password being used if it was used within the past 2 years. Additionally, the VAM prohibits the reuse of a password that has been used within the last 3 times the password has been changed - regardless of time frame.
f. VAM allows the use of a one-time password that must be reset upon initial login.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-05.E02 Authenticator Management | Pki-Based Authentication	**IA-05.E02 Authenticator Management | Pki-Based Authentication** The information system, for PKI-based authentication: (a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; (b) Enforces authorized access to the corresponding private key; (c) Maps the authenticated identity to the account of the individual or group; and (d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO. Two-factor authentication is configured and managed through OI&T.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-05.E03 Authenticator Management | In-Person Or Trusted Third-Party Registration	**IA-05.E03 Authenticator Management | In-Person Or Trusted Third-Party Registration** The organization requires that the registration process to receive [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection: in person; by a trusted third party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO. The OI&T requires that the registration process for issuance of VA identity credentials, and the verification and provisioning process for acceptance for use in VA systems of credentials issued by third parties, shall follow the procedures defined in NIST SP 800-63 for the level of assurance applicable to that credential or token.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-05.E11 Authenticator Management | Hardware Token-Based Authentication	**IA-05.E11 Authenticator Management | Hardware Token-Based Authentication** The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
OIT requires that the registration process for issuance of VA identity credentials, and the verification and provisioning process for acceptance for use in VA systems of credentials issued by third parties, shall follow the procedures defined in NIST SP 800-63 for the level of assurance applicable to that credential or token.
For VAM Clients log into VistA in different ways – there are Connection Proxies, CAPRI tokens, BSE tokens, Access Verify,

SAML tokens. Each method is recognized by the Router and allows it to associate a client's identity with the session. It is important to note that the Router doesn't implement authentication – it merely notes how VistA responds to different sign on options and changes the client session appropriately.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-06.1 Authenticator Feedback	**IA-06.1 Authenticator Feedback** The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is partially inherited from VAEC AWS and VA EO.
VAM uses RPC for authentication. The RPC protocol is connection-oriented and synchronous with clients opening a connection to VistA and only making new RPC calls after receiving a reply from a previous call.
Clients log into VistA in different ways – there are Connection Proxies, CAPRI tokens, BSE tokens, Access Verify, SAML tokens. Each method is recognized by the Router and allows it to associate a client's identity with the session. It is important to note that the Router doesn't implement authentication – it merely notes how VistA responds to different sign on options and changes the client session appropriately. Authentication is provided by VA EO.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-07.1 Cryptographic Module Authentication	**IA-07.1 Cryptographic Module Authentication** The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO and VAEC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-08.1 Identification And Authentication (Non-Organizational Users)	**IA-08.1 Identification And Authentication (Non-Organizational Users)** The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is not applicable due to the VAM system not granting acccess to non-organizational users.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-08.E01 Identification And Authentication (Non-Organizational Users) | Acceptance Of Piv Credentials From Other Agencies	**IA-08.E01 Identification And Authentication (Non-Organizational Users) | Acceptance Of Piv Credentials From Other Agencies** The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-08.E02 Identification And Authentication (Non-Organizational Users) | Acceptance Of Third-Party Credentials	**IA-08.E02 Identification And Authentication (Non-Organizational Users) | Acceptance Of Third-Party Credentials** The information system accepts only FICAM-approved third-party credentials.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA and VAEC AWS GovCloud High Assessing. This control is partially inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-08.E03 Identification And Authentication (Non-Organizational Users) | Use Of Ficam-Approved Products	**IA-08.E03 Identification And Authentication (Non-Organizational Users) | Use Of Ficam-Approved Products** The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IA-08.E04 Identification And Authentication (Non-Organizational Users) | Use Of Ficam-Issued Profiles	**IA-08.E04 Identification And Authentication (Non-Organizational Users) | Use Of Ficam-Issued Profiles** The information system conforms to FICAM-issued profiles.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Status		Type	
In Place (Pass)	X	Common	
Planned or In Place and Planned (Fail)		Hybrid	X
		System Specific	

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IP-01.1 Consent	**IP-01.1 Consent** The organization: a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII notinitially described in the public notice that was in effect at the time the organization collected the PII.	Status: In Place (Pass); Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Status		Type	
In Place (Pass)		Common	
Planned or In Place and Planned (Fail)		Hybrid	X
		System Specific	

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IP-01.E01 Consent | Mechanisms Supporting Itemized Or Tiered Consent	**IP-01.E01 Consent | Mechanisms Supporting Itemized Or Tiered Consent** The organization implements mechanisms to support itemized or tiered consent for specific uses of data.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IP-02.1 Individual Access	**IP-02.1 Individual Access** The organization: a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records; b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; c. Publishes access procedures in System of Records Notices (SORNs); and d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IP-03.1 Redress	**IP-03.1 Redress** The organization: a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected oramended.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IP-04.1 Complaint Management	**IP-04.1 Complaint Management** The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] Type: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IP-04.E01 Complaint Management | Response Times	**IP-04.E01 Complaint Management | Response Times** The organization responds to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] Type: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-01.1 Incident Response Policy And Procedures	**IR-01.1 Incident Response Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy [Assignment: organization-defined frequency]; and 2. Incident response procedures [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-02.1 Incident Response Training	**IR-02.1 Incident Response Training** The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is partially inherited from the VA NSOC. Additionally, Incident Response training is required for each new user as a component of the VA User Awareness Training. This training is done annually.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-02.E01 Incident Response Training | Simulated Events	**IR-02.E01 Incident Response Training | Simulated Events** The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-02.E02 Incident Response Training | Automated Training Environments	**IR-02.E02 Incident Response Training | Automated Training Environments** The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-03.1 Incident Response Testing	**IR-03.1 Incident Response Testing** The organization tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-03.E02 Incident Response Testing | Coordination With Related Plans	**IR-03.E02 Incident Response Testing | Coordination With Related Plans** The organization coordinates incident response testing with organizational elements responsible for related plans.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-04.1 Incident Handling	**IR-04.1 Incident Handling** The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-04.E01 Incident Handling | Automated Incident Handling Processes	**IR-04.E01 Incident Handling | Automated Incident Handling Processes** The organization employs automated mechanisms to support the incident handling process.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-04.E04 Incident Handling | Information Correlation	**IR-04.E04 Incident Handling | Information Correlation** The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-05.1 Incident Monitoring	**IR-05.1 Incident Monitoring** The organization tracks and documents information system security incidents.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-05.E01 Incident Monitoring | Automated Tracking / Data Collection / Analysis	**IR-05.E01 Incident Monitoring | Automated Tracking / Data Collection / Analysis** The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-06.1 Incident Reporting	**IR-06.1 Incident Reporting** The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Reports security incident information to [Assignment: organization-defined authorities].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-06.E01 Incident Reporting | Automated Reporting	**IR-06.E01 Incident Reporting | Automated Reporting** The organization employs automated mechanisms to assist in the reporting of security incidents.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-07.1 Incident Response Assistance	**IR-07.1 Incident Response Assistance** The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-07.E01 Incident Response Assistance | Automation Support For Availability Of Information / Support	**IR-07.E01 Incident Response Assistance | Automation Support For Availability Of Information / Support** The organization employs automated mechanisms to increase the availability of incident response-related information and support.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
IR-08.1 Incident Response Plan	**IR-08.1 Incident Response Plan** The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification.	**Status** In Place (Pass): X Planned or In Place and Planned (Fail): **Type** Common: Hybrid: X System Specific: X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-01.1 System Maintenance Policy And Procedures	**MA-01.1 System Maintenance Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy [Assignment: organization-defined frequency]; and 2. System maintenance procedures [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA Enterprise Operations. OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the System Maintenance Policy is reviewed every five (5) years.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-02.1 Controlled Maintenance	**MA-02.1 Controlled Maintenance** The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High Assessing and OI&T.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-02.E02 Controlled Maintenance | Automated Maintenance Activities	**MA-02.E02 Controlled Maintenance | Automated Maintenance Activities** The organization: (a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and (b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed. Related to: CA-7, MA-3	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-03.1 Maintenance Tools	**MA-03.1 Maintenance Tools** The organization approves, controls, and monitors information system maintenance tools.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-03.E01 Maintenance Tools | Inspect Tools	**MA-03.E01 Maintenance Tools | Inspect Tools** The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-03.E02 Maintenance Tools | Inspect Media	**MA-03.E02 Maintenance Tools | Inspect Media** The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-03.E03 Maintenance Tools | Prevent Unauthorized Removal	**MA-03.E03 Maintenance Tools | Prevent Unauthorized Removal** The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-04.1 Nonlocal Maintenance	**MA-04.1 Nonlocal Maintenance** The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-04.E02 Nonlocal Maintenance | Document Nonlocal Maintenance	**MA-04.E02 Nonlocal Maintenance | Document Nonlocal Maintenance** The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from OI&T.
OI&T documents, in the security plan for the information system, the policies and procedures for establishment and use of non-local maintenance and diagnostic connections.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-04.E03 Nonlocal Maintenance | Comparable Security / Sanitization	**MA-04.E03 Nonlocal Maintenance | Comparable Security / Sanitization** The organization: (a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or (b) Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from OI&T.
OI&T documents, in the security plan for the information system, the policies and procedures for establishment and use of non-local maintenance and diagnostic connections.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-05.1 Maintenance Personnel	**MA-05.1 Maintenance Personnel** The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-05.E01 Maintenance Personnel | Individuals Without Appropriate Access	**MA-05.E01 Maintenance Personnel | Individuals Without Appropriate Access** The organization: (a) Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: (b) Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MA-06.1 Timely Maintenance	**MA-06.1 Timely Maintenance** The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MP-01.1 Media Protection Policy And Procedures	**MP-01.1 Media Protection Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy [Assignment: organization-defined frequency]; and 2. Media protection procedures [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA Enterprise Operations. OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Media Protection Policy is reviewed every five (5) years.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MP-02.1 Media Access	**MP-02.1 Media Access** The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MP-03.1 Media Marking	**MP-03.1 Media Marking** The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [Assignment: organization-defined controlled areas].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MP-04.1 Media Storage	**MP-04.1 Media Storage** The organization: a. Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MP-05.1 Media Transport	**MP-05.1 Media Transport** The organization: a. Protects and controls [Assignment: organization-defined types of information system media] during transport outside of controlled areas using [Assignment: organization-defined security safeguards]; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MP-05.E04 Media Transport | Cryptographic Protection	**MP-05.E04 Media Transport | Cryptographic Protection** The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MP-06.1 Media Sanitization	**MP-06.1 Media Sanitization** The organization: a. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MP-06.E01 Media Sanitization | Review / Approve / Track / Document / Verify	**MP-06.E01 Media Sanitization | Review / Approve / Track / Document / Verify** The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MP-06.E02 Media Sanitization | Equipment Testing	**MP-06.E02 Media Sanitization | Equipment Testing** The organization tests sanitization equipment and procedures [Assignment: organization-defined frequency] to verify that the intended sanitization is being achieved.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MP-06.E03 Media Sanitization | Nondestructive Techniques	**MP-06.E03 Media Sanitization | Nondestructive Techniques** The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MP-07.1 Media Use	**MP-07.1 Media Use** The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
MP-07.E01 Media Use | Prohibit Use Without Owner	**MP-07.E01 Media Use | Prohibit Use Without Owner** The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-01.1 Physical And Environmental Protection Policy And Procedures	**PE-01.1 Physical And Environmental Protection Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and 2. Physical and environmental protection procedures [Assignment: organization-defined frequency].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA Enterprise Operations. OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Physical and Environment Protection Policy is reviewed every five (5) years.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-02.1 Physical Access Authorizations	**PE-02.1 Physical Access Authorizations** The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and d. Removes individuals from the facility access list when access is no longer required.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-03.1 Physical Access Control	**PE-03.1 Physical Access Control** The organization: a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards]; b. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points]; c. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring]; e. Secures keys, combinations, and other physical access devices; f. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and g. Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-03.E01 Physical Access Control | Information System Access	**PE-03.E01 Physical Access Control | Information System Access** The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the information system].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-04.1 Access Control For Transmission Medium	**PE-04.1 Access Control For Transmission Medium** The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-05.1 Access Control For Output Devices	**PE-05.1 Access Control For Output Devices** The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-06.1 Monitoring Physical Access	**PE-06.1 Monitoring Physical Access** The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinates results of reviews and investigations with the organizational incident response capability.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-06.E01 Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment	**PE-06.E01 Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment** The organization monitors physical intrusion alarms and surveillance equipment.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-06.E04 Monitoring Physical Access | Monitoring Physical Access To Information Systems	**PE-06.E04 Monitoring Physical Access | Monitoring Physical Access To Information Systems** The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [Assignment: organization-defined physical spaces containing one or more components of the information system].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-08.1 Visitor Access Records	**PE-08.1 Visitor Access Records** The organization: a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and b. Reviews visitor access records [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-08.E01 Visitor Access Records | Automated Records Maintenance / Review	**PE-08.E01 Visitor Access Records | Automated Records Maintenance / Review** The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-09.1 Power Equipment And Cabling	**PE-09.1 Power Equipment And Cabling** The organization protects power equipment and power cabling for the information system from damage and destruction.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-10.1 Emergency Shutoff	**PE-10.1 Emergency Shutoff** The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-11.1 Emergency Power	**PE-11.1 Emergency Power** The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-11.E01 Emergency Power | Long-Term Alternate Power Supply - Minimal Operational Capability	**PE-11.E01 Emergency Power | Long-Term Alternate Power Supply - Minimal Operational Capability** The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-12.1 Emergency Lighting	**PE-12.1 Emergency Lighting** The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-13.1 Fire Protection	**PE-13.1 Fire Protection** The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-13.E01 Fire Protection | Detection Devices / Systems	**PE-13.E01 Fire Protection | Detection Devices / Systems** The organization employs fire detection devices/systems for the information system that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-13.E02 Fire Protection | Suppression Devices / Systems	**PE-13.E02 Fire Protection | Suppression Devices / Systems** The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-13.E03 Fire Protection | Automatic Fire Suppression	**PE-13.E03 Fire Protection | Automatic Fire Suppression** The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-14.1 Temperature And Humidity Controls	**PE-14.1 Temperature And Humidity Controls** The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and b. Monitors temperature and humidity levels [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-15.1 Water Damage Protection	**PE-15.1 Water Damage Protection** The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-15.E01 Water Damage Protection | Automation Support	**PE-15.E01 Water Damage Protection | Automation Support** The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [Assignment: organization-defined personnel or roles].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-16.1 Delivery And Removal	**PE-16.1 Delivery And Removal** The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-17.1 Alternate Work Site	**PE-17.1 Alternate Work Site** The organization: a. Employs [Assignment: organization-defined security controls] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	**Status** / **Type** In Place (Pass): X — Common: Planned or In Place and Planned (Fail): — Hybrid: System Specific: X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PE-18.1 Location Of Information System Components	**PE-18.1 Location Of Information System Components** The organization positions information system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PL-01.1 Security Planning Policy And Procedures	**PL-01.1 Security Planning Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy [Assignment: organization-defined frequency]; and 2. Security planning procedures [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM inherits this control from OI&T. OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Security Planning Policy is reviewed every five (5) years.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PL-02.1 System Security Plan	**PL-02.1 System Security Plan** The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles]; c. Reviews the security plan for the information system [Assignment: organization-defined frequency]; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is partially inherited from the VA. The System Security Plan (SSP) is generated using RiskVision and is updated annually. Requisite personnel have access to RiskVision to view the SSP as needed.
VAM ISO and System Stewards will generate the SSP using RiskVision and will update annually.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PL-02.E03 System Security Plan | Plan / Coordinate With Other Organizational Entities	**PL-02.E03 System Security Plan | Plan / Coordinate With Other Organizational Entities** The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAEC plans and coordinates security-related activities affecting hosted information system with Continuous Readiness Information Security Program (CRISP) and National Service Desk (NSD) before conducting such activities in order to reduce the impact on other organizational entities. Notification for CBS scan activities such as database scans or WASA are handled by an email notification process. Email notification goes from Application/Build Managers to the Information Owner and then out to all CBS users.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PL-04.1 Rules Of Behavior	**PL-04.1 Rules Of Behavior** The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM inherits the following process from the VA:
(a) Establishes and makes readily available to all VA staff, contractors and volunteers, the Rules of Behavior (ROB) that describe their responsibilities and the expected behavior with regard to information and information system usage; the ROB must be signed on an annual basis, is part of the annual Information Security Briefing and Security Awareness Training, and is available at the following URL: https://www.tms.va.gov/plateau/user/login.jsp This is done through the Talent Management System (TMS).
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PL-04.E01 Rules Of Behavior | Social Media And Networking Restrictions	**PL-04.E01 Rules Of Behavior | Social Media And Networking Restrictions** The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM inherits the following process from the VA:
(a) Establishes and makes readily available to all VA staff, contractors and volunteers, the Rules of Behavior (ROB) that describe their responsibilities and the expected behavior with regard to information and information system usage; the ROB must be signed on an annual basis, is part of the annual Information Security Briefing and Security Awareness Training, and is available at the following URL: https://www.tms.va.gov/plateau/user/login.jsp This is done through the Talent Management System (TMS).
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PL-08.1 Information Security Architecture	**PL-08.1 Information Security Architecture** The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.	**Status** In Place (Pass): X Planned or In Place and Planned (Fail): **Type** Common: Hybrid: X System Specific:

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM has developed and maintains a security plan that: Is consistent with OIT enterprise architecture; Explicitly defines the authorization boundary; Describes the operational context in terms of missions and business processes; Provides the security category and impact level including supporting rationale; Describes the operational environment; Describes relationships with, or connections to, internal and external information systems; Provides an overview of the security requirements; Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and Is reviewed and approved by the authorizing official (AO) or designated approving authority (DAA) prior to plan implementation. b) Reviews the security plan annually; after an SCA has been executed; and after a significant change; and c) Updates the plan to address changes to the service line or environment of operation; or problems identified during plan implementation, scan, or security control assessment. The SSP is considered a living document and is reviewed and updated at least annually or whenever a significant change occurs affecting the security posture. The SSP provides a detailed overview of security requirements and describes the continuous monitoring activities associated with the security controls implemented to meet those requirements. The SSP is a security artifact for the Assessment & Authorization (A&A) of reportable information systems in accordance with the Federal Information Security Management Act (FISMA). DCO implements guidance from NIST SP 800-18 Guide for Developing Security Plans for Information Technology Systems to develop the SSP using OIT and EO approved processes and the VA standardized approach to A&A.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-01.1 Information Security Program Plan	**PM-01.1 Information Security Program Plan** The organization: a. Develops and disseminates an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [Assignment: organization-defined frequency]; c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and d. Protects the information security program plan from unauthorized disclosure and modification.	**Status** In Place (Pass): Planned or In Place and Planned (Fail): X **Type** Common: X Hybrid: System Specific:

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO.
VAM inherits this control from OI&T. OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Program Management Policy is reviewed every five (5) years.
Evidence: YES

Control Provider

DAS for the Office of Information Security (005R2)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-02.1 Senior Information Security Officer	**PM-02.1 Senior Information Security Officer** The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] Type: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, the VA CIO has appointed a CISO with the mission and resources to coordinate, develop, implement, and maintain a VA-wide information security program.
Evidence: YES

Control Provider

Assistant Secretary for OIT (005)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-03.1 Information Security Resources	**PM-03.1 Information Security Resources** The organization: a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] Type: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inhIn accordance with VA Handbook 6500, VA OI&T ensures that all capital planning and investment requests include the resources necessary to implement the information security program and documents all exceptions to this requirement. This includes employing a business case/Exhibit 300/Exhibit 53 to record the resources required and ensuring that information security resources are available for expenditure as planned.erited from the VA EO.

Evidence: YES

Control Provider

OIT Resource Management (005F)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-04.1 Plan Of Action And Milestones Process	**PM-04.1 Plan Of Action And Milestones Process** The organization: a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems: 1. Are developed and maintained; 2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and 3. Are reported in accordance with OMB FISMA reporting requirements. b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
a. In accordance with VA Handbook 6500, VA OI&T has implemented a standardized process for ensuring that POA&Ms for the security program and the associated VA information systems: (i) are developed and maintained; (ii) document the remedial information security actions to adequately respond to risk to VA operations and assets, individuals, other organizations, and the Nation; and (iii) are reported in accordance with OMB FISMA reporting requirements.
b. In accordance with VA Handbook 6500, VA OI&T reviews POA&Ms for consistency with the VA risk management strategy and VA-wide priorities for risk response actions.
Evidence: YES

Control Provider

OIT OCS Certification Program Office (005R2)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-05.1 Information System Inventory	**PM-05.1 Information System Inventory** The organization develops and maintains an inventory of its information systems.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] Type: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, OI&T will develop and maintain an inventory of its information systems. Inventory will comply with current OMB and FISMA guidance, and include data points to identify physical location, logical location (MAC and IP address), ownership/assignment, tracking number, operating system type and version number, serial number, and model number. Service Delivery and Engineering will provide the field with the procedures for conducting and maintaining the inventory of IT systems within VA.
Evidence: YES

Control Provider

OIT Service Delivery and Engineering (005OP) OIT OCS Certification Program Offic

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-06.1 Information Security Measures Of Performance	**PM-06.1 Information Security Measures Of Performance** The organization develops, monitors, and reports on the results of information security measures of performance.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] Type: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, VA OI&T will develop, monitor, and report on the results of information security measures of performance. This is accomplished by determining and establishing outcome based performance metrics and tracking the performance and providing feedback to the field to improve performance.
Evidence: YES

Control Provider

OIT Information Security Office (005R)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-07.1 Enterprise Architecture	**PM-07.1 Enterprise Architecture** The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, OI&T's EA organization:
(a) Aligns VA information system EA with Federal EA design;
(b) Integrates enterprise architectural design with security requirements early in the SDLC;
(c) Ensures security considerations and requirements are directly and explicitly related to VA's mission/business processes;
(d) Effectively uses VA's RMF along with supporting security standards and guidelines to effectively address security requirements; and
(e) Follows Federal Segment Architecture Methodology.
Evidence: YES

Control Provider

OIT Architecture, Strategy, and Design (005E)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-08.1 Critical Infrastructure Plan	**PM-08.1 Critical Infrastructure Plan** The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] Type: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, VA OI&T addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan. This is done by defining: the critical infrastructure for VA information systems, key critical infrastructure resources, and key critical infrastructure personnel.
Evidence: YES

Control Provider

OIT Service Delivery and Engineering (005OP) OIT Business Continuity (005R4)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-09.1 Risk Management Strategy	**PM-09.1 Risk Management Strategy** The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; b. Implements the risk management strategy consistently across the organization; and c. Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] Type: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, VA OI&T has a comprehensive strategy to manage risk to VA operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems. VA implements

the risk management strategy consistently across the organization and reviews and updates the strategy as required to address VA changes.
Evidence: YES

Control Provider

OIT Director Enterprise Risk Management

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-10.1 Security Authorization Process	**PM-10.1 Security Authorization Process** The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, OI&T has developed a security authorization process to manage and control VA information system security posture.
Evidence: YES

Control Provider

OIT OCS Certification Program Office (005R2)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-11.1 Mission/Business Process Definition	**PM-11.1 Mission/Business Process Definition** The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, VA OI&T is continually defining VA mission/business processes with consideration for information security and the resulting risk to VA operations and assets, individuals, other organizations, and the Nation and will revise the processes as necessary until achievable protection needs are obtained. OI&T works closely with VHA, VBA, and NCA to determine their missions and their security requirements and needs and to ensure they are involved in evaluating the impact of security controls on mission and business processes.
Evidence: YES

Control Provider

VHA, VBA and NCA with OIT, Service Delivery and Engineering (005OP)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-12.1 Insider Threat Program	**PM-12.1 Insider Threat Program** The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, the VA OI&T has an insider threat program that includes a cross-discipline insider threat incident handling team. The cross-discipline insider threat incident handling team includes representation from major departments across VA and meets on a regular basis to discuss the current level of organizational preparedness in addressing insider threat. The insider threat program includes controls to detect malicious insider activity and the correlation of both technical and nontechnical information.
Evidence: YES

Control Provider

VA-NSOC, OCS, and Enterprise Risk Management

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-13.1 Information Security Workforce	**PM-13.1 Information Security Workforce** The organization establishes an information security workforce development and improvement program.	Status: In Place (Pass): ; Planned or In Place and Planned (Fail): X Type: Common: X; Hybrid: ; System Specific:

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, VA OI&T has an information security workforce development and improvement plan. The VA information security workforce development and improvement program includes, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions.
Evidence: YES

Control Provider

OI&T Resource Management

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-14.1 Testing	**PM-14.1 Testing** The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: 1. Are developed and maintained; and 2. Continue to be executed in a timely manner; b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, VA OI&T implements a process for ensuring that VA plans for conducting security testing, training, and monitoring activities associated with VA information systems: (i) are developed and maintained; and (ii) continue to be executed in a timely manner. VA OI&T reviews testing, training, and monitoring plans for consistency with VA risk management strategy and VA-wide priorities for risk response actions.
Evidence: YES

Control Provider

OIS

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-15.1 Contacts With Security Groups And Associations	**PM-15.1 Contacts With Security Groups And Associations** The organization establishes and institutionalizes contact with selected groups and associations within the security community: a. To facilitate ongoing security education and training for organizational personnel; b. To maintain currency with recommended security practices, techniques, and technologies; and c. To share current security-related information including threats, vulnerabilities, and incidents.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, VA OI&T establishes and institutionalizes contact with selected groups and associations within the security community:
1. To facilitate ongoing security education and training for VA personnel;
2. To maintain currency with recommended security practices, techniques, and technologies; and
3. To share current security-related information including threats, vulnerabilities, and incidents.
Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. VA selects groups and associations based on VA missions/business functions. VA shares threat, vulnerability, and incident information consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
Evidence: YES

Control Provider

DAS for OIS

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PM-16.1 Threat Awareness Program	**PM-16.1 Threat Awareness Program** The organization implements a threat awareness program that includes a cross-organization information-sharing capability.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [X]; Hybrid [ ]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This is inherited from the VA EO.
In accordance with VA Handbook 6500, VA OI&T has a threat awareness program that includes a cross-VA information-sharing capability.
VA will share threat information as one technique to address the concern of constantly changing and increasingly sophisticated adversaries. Threat information sharing includes, for example, sharing threat events (i.e., tactics, techniques, and procedures) that VA has experienced, mitigations that VA has found are effective against certain types of threats, or threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., governmentcommercial
cooperatives, government-government cooperatives), or multilateral (e.g., VA taking part in threat-sharing
consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely

shared.
Evidence: YES

Control Provider

VA-NSOC

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PS-01.1 Personnel Security Policy And Procedures	**PS-01.1 Personnel Security Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy [Assignment: organization-defined frequency]; and 2. Personnel security procedures [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA Enterprise Operations. OI&T develops, documents, and disseminates policies and procedures enterprise-wide.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

PM-9.

Control (*)	Description of Control (*)	Control Status/Type (*)
PS-02.1 Position Risk Designation	**PS-02.1 Position Risk Designation** The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA per VA Handbook and Directive 0710.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PS-03.1 Personnel Screening	**PS-03.1 Personnel Screening** The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA per VA Handbook and Directive 0710.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PS-04.1 Personnel Termination	**PS-04.1 Personnel Termination** The organization, upon termination of individual employment: a. Disables information system access within [Assignment: organization-defined time period]; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA and VAEC AWS GovCloud High Assessing.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PS-04.E02 Personnel Termination | Automated Notification	**PS-04.E02 Personnel Termination | Automated Notification** The organization employs automated mechanisms to notify [Assignment: organization-defined personnel or roles] upon termination of an individual.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PS-05.1 Personnel Transfer	**PS-05.1 Personnel Transfer** The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA and VAEC AWS GovCloud High Assessing.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PS-06.1 Access Agreements	**PS-06.1 Access Agreements** The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA and VAEC AWS GovCloud High Assessing.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PS-07.1 Third-Party Personnel Security	**PS-07.1 Third-Party Personnel Security** The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and e. Monitors provider compliance.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
PS-08.1 Personnel Sanctions	**PS-08.1 Personnel Sanctions** The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is partially inherited from FedRAMP JAB authorized package ID F1603047866 for Amazon Web Services GovCloud High and VA EO.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
RA-01.1 Risk Assessment Policy And Procedures	**RA-01.1 Risk Assessment Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy [Assignment: organization-defined frequency]; and 2. Risk assessment procedures [Assignment: organization-defined frequency].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM inherits this control from OI&T. OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the Risk Assessment Policy is reviewed every five (5) years.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
RA-02.1 Security Categorization	**RA-02.1 Security Categorization** The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
a. In accordance with VA Handbook 6500, the VAM conducts security categorization in accordance with FIPS 199 and current companion publication, NIST SP 800-60 and OMB Circular A-130.
b. VAM documents the security categorization results in the VAM FIPS 199 and the SSP. Overall system is a High baseline. The Confidentiality, Availability, and Integrity are also rated as High.
c. In accordance with VA Handbook 6500, the VAM AO or designee will review and approve an information system's security

categorization as part of the review and approval of the SSP in accordance with the RMF described in the current version of NIST SP 800-37.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
RA-03.1 Risk Assessment	**RA-03.1 Risk Assessment** The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High Assessing.
a. In accordance with VA Handbook 6500, the VAEC AWS GovCloud High conducts a annnual risk assessment to determine the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.
b. The VAEC AWS GovCloud High documents risk assessment results in the SSP.
c. The VAEC AWS GovCloud High reviews risk assessment results annually or as needed.
d. The VAEC AWS GovCloud High system owner disseminates risk assessment results to personnel or roles that should receive risk assessment results.
e. The VAEC AWS GovCloud High updates the risk assessment at least annually or whenever there are significant changes to the information system or environment of operation.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
RA-05.1 Vulnerability Scanning	**RA-05.1 Vulnerability Scanning** The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is partially inherited from the VA WASA and VAEC.
a. In accordance with VA Handbook 6500, VAM scans for vulnerabilities in the VICS server monthly and/or randomly in accordance with OI&T approved process and when new vulnerabilities
potentially affecting the system/applications are identified and reported.
b. VAM utilizes Tenable Nessus for host-based vulnerability scanning. VA WASA utilizes AppScan and BurpSuite for web application and HP Fortify for static code scanning. These scanning tools incorporates functionality that facilitates interoperability and allows for automated scan management. The tools have the capability to enumerating platforms, software flaws, and improper configurations, formatting checklists and test procedures, and measuring vulnerability impact. Systems are scanned every month during the enterprise predictive scan
c. The VAM team incoordination with VA WASA team analyzes vulnerability scan reports and results from
security control assessments.
d. In accordance with VA Handbook 6500, VAM remediates legitimate vulnerabilities in accordance
with OI&T established response times. Critical: patches will be tested and applied within 30 days. High: patches will be tested and applied within 60 days. Moderate: patches will be tested and applied within 90 days. Low: the Information System Owner will determine the patching timeframe. Emergent: patches will be tested ad applied as soon as possible.
e. In accordance with VA Handbook 6500, VAM shares information obtained from the vulnerability
scanning process and security control assessments with OCS and VAM security team to facilitate similar

vulnerabilities information with other systems.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
RA-05.E01 Vulnerability Scanning | Update Tool Capability	**RA-05.E01 Vulnerability Scanning | Update Tool Capability** The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA WASA and VAEC.

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
RA-05.E02 Vulnerability Scanning | Update By Frequency / Prior To New Scan / When Identified	**RA-05.E02 Vulnerability Scanning | Update By Frequency / Prior To New Scan / When Identified** The organization updates the information system vulnerabilities scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA WASA and VAEC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
RA-05.E04 Vulnerability Scanning | Discoverable Information	**RA-05.E04 Vulnerability Scanning | Discoverable Information** The organization determines what information about the information system is discoverable by adversaries and subsequently takes [Assignment: organization-defined corrective actions].	**Status**: In Place (Pass); Planned or In Place and Planned (Fail) X **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA WASA and VAEC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
RA-05.E05 Vulnerability Scanning | Privileged Access	**RA-05.E05 Vulnerability Scanning | Privileged Access** The information system implements privileged access authorization to [Assignment: organization-identified information system components] for selected [Assignment: organization-defined vulnerability scanning activities].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA WASA and VAEC. VAEC AWS GovCloud High utilizes Tenable Nessus for host-based vulnerability scanning. VA WASA utilizes AppScan and BurpSuite for web application and HP Fortify for static code scanning. These tools conduct scans using privileged access authorization for all vulnerability scan activities.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-01.1 System And Services Acquisition Policy And Procedures	**SA-01.1 System And Services Acquisition Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy [Assignment: organization-defined frequency]; and 2. System and services acquisition procedures [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is partially inherited from VA EO.
OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the System and Services Acquisition Policy is reviewed every five (5) years.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-02.1 Allocation Of Resources	**SA-02.1 Allocation Of Resources** The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
a. VAM determines information security requirements for the information system or information system service in mission/business process planning
b. VAM determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process
c. VAM establishes a discrete line item for information security in organizational programming and budgeting documentation.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-03.1 System Development Life Cycle	**SA-03.1 System Development Life Cycle** The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
a.VAM manages the information system using SDLC guidance provided by Project Management Accountability system.
b. VAM defines and documents information security roles and responsibilities throughout the system development life cycle
c. VAM identifies individuals having information security roles and responsibilities
d. VAM integrates the organizational information security risk management process into system development life cycle activities."
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-04.1 Acquisition Process	**SA-04.1 Acquisition Process** The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria.	<table><tr><th>Status</th><th></th><th>Type</th><th></th></tr><tr><td>In Place (Pass)</td><td>X</td><td>Common</td><td></td></tr><tr><td rowspan="2">Planned or In Place and Planned (Fail)</td><td rowspan="2"></td><td>Hybrid</td><td>X</td></tr><tr><td>System Specific</td><td></td></tr></table>

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VA includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and VA mission/business needs:
a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Requirements for protecting security-related documentation;
f. Description of the information system developmental environment and environment in which the system is intended to operate; and
g. Acceptance criteria.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-04.E01 Acquisition Process | Functional Properties Of Security Controls	**SA-04.E01 Acquisition Process | Functional Properties Of Security Controls** The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM follows the VA requirement for the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-04.E02 Acquisition Process | Design / Implementation Information For Security Controls	**SA-04.E02 Acquisition Process | Design / Implementation Information For Security Controls** The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
Per guidance provided by the VA, VAM has implemented detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-04.E09 Acquisition Process | Functions / Ports / Protocols / Services In Use	**SA-04.E09 Acquisition Process | Functions / Ports / Protocols / Services In Use** The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VAM developers have identified early in the system development life cycle (SDLC), the functions, ports, protocols, and services intended for organizational use. VAM uses the IBM Jazz/Rational tools.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-04.E10 Acquisition Process | Use Of Approved Piv Products	**SA-04.E10 Acquisition Process | Use Of Approved Piv Products** The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VA employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems. OIS reviews all procurements to ensure guidelines are met.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-05.1 Information System Documentation	**SA-05.1 Information System Documentation** The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response; d. Protects documentation as required, in accordance with the risk	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid; System Specific X

management strategy; and e. Distributes documentation to [Assignment: organization-defined personnel or roles].

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM stores all associated system documentation in a secure online portal repositories. Only requisite personnel have access to the VAM documentation repositories.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-08.1 Security Engineering Principles	**SA-08.1 Security Engineering Principles** The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system per NIST SP 800-27 Rev A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security) dated June 2004.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-09.1 External Information System Services	**SA-09.1 External Information System Services** The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
All connectivity comes in through VPN. In the future if an interconnection exists, we will update the policy/evidence.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-09.E02 External Information System Services | Identification Of Functions / Ports / Protocols / Services	**SA-09.E02 External Information System Services | Identification Of Functions / Ports / Protocols / Services** The organization requires providers of [Assignment: organization-defined external information system services] to identify the functions, ports, protocols, and other services required for the use of such services.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
All connectivity comes in through VPN. In the future if an interconnection exists, we will update the policy/evidence.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-10.1 Developer Configuration Management	**SA-10.1 Developer Configuration Management** The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM's configuration management plan document outlines the requirements for developer configuration management.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-11.1 Developer Security Testing And Evaluation	**SA-11.1 Developer Security Testing And Evaluation** The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM conducts developer security testing and evaluation in accordance with VA policies and procedures.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-12.1 Supply Chain Protection	**SA-12.1 Supply Chain Protection** The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VA uses the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain and (ii) protect information systems and information system components, prior to taking delivery of such systems/components.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-15.1 Development Process	**SA-15.1 Development Process** The organization: a. Requires the developer of the information system, system component, or information system service to follow a documented development process that: 1. Explicitly addresses security requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Reviews the development process, standards, tools, and tool options/configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [Assignment: organization-defined security requirements].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VA requires the developers of VAM to follow a documented development process (referenced in the Configuration Management Plan) that:
1. Explicitly addresses security requirements;
2. Identifies the standards and tools used in the development process;
3. Documents the specific tool options and tool configurations used in the development process; and
4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
Reviews the development process, standards, tools, and tool options/configurations annually or as deemed necessary to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy the Release Management Plan located in the Configuration Management Plan.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-16.1 Developer-Provided Training	**SA-16.1 Developer-Provided Training** The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is partially inherited. The VA requires the developer of the VAM to provide training on the correct use and operation of the implemented security functions, controls, and/or mechanisms. For example, the Talent Management System (TMS) has a training for Information Assurance for Software Developers (WBT) (ID#: 1016925)
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SA-17.1 Developer Security Architecture And Design	**SA-17.1 Developer Security Architecture And Design** The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VA requires the developer of the VAM to produce a design specification and security architecture that:
a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;

b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-01.1 System And Communications Protection Policy And Procedures	**SC-01.1 System And Communications Protection Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy [Assignment: organization-defined frequency]; and 2. System and communications protection procedures [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO. OI&T develops, documents, and disseminates policies and procedures enterprise-wide.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-02.1 Application Partitioning	**SC-02.1 Application Partitioning** The information system separates user functionality (including user interface services) from information system management functionality.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] Type: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAEC only utilizes applications that are VA TRM-approved that separate user functionality from security functionality. These include Windows, Linux, Splunk, BigFix, McAfee, etc.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-03.1 Security Function Isolation	**SC-03.1 Security Function Isolation** The information system isolates security functions from nonsecurity functions.	Status: In Place (Pass) [X]; Planned or In Place and Planned (Fail) [ ] Type: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM utilizes only approved software that separates security, administrative, and user functionalities.
These include Windows and Linux operating systems, Splunk, GitHub Enterprise, etc. Hosted applications within the environment are responsible for security function isolation within their application.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-04.1 Information In Shared Resources	**SC-04.1 Information In Shared Resources** The information system prevents unauthorized and unintended information transfer via shared system resources.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO and VAEC AWS GovCloud High.
VAEC AWS GovCloud High partially implements this control from the Amazon Web Services (AWS) GovCloud High Package # F1603047866 for multi-tenant services. Unauthorized/unintended information transfer of shared system resources is preventedat the hypervisor level managed by AWS.
VAEC does not implement shared resources within the environment. However, hosted applications that utilize shared resources are responsible for preventing unauthorized and untintended information transfer via shared system resources within the hosted systems' applications.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-05.1 Denial Of Service Protection	**SC-05.1 Denial Of Service Protection** The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-07.1 Boundary Protection	**SC-07.1 Boundary Protection** The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
VAM has 3 system and security boundaries.
Client Boundary: The client application, CPRS in the case of the IOC, will be installed on a machine within end-user's segment of the VA network. It will directly connect to the VAM Boundary through the VAECs Business Partner Extranet (BPE) ExpressRoute connection.
VAM (AWS) Boundary: VAM and its associated components (VICS Server, RPC Router, Router Manager, and Datastore) are all

contained within a single security boundary within the VAEC using the AWS VA GSS. AWS VA General Support System (GSS) that is already documented within Risk Vision. All Security controls that are already documented in Risk Vision for AWA GSS cloud will be inherit within our System Security Plan (SSP). VAM will connect directly to the Client Boundary and the VistA Boundary through the BPE.
VistA Boundary: In the IOC/Figure 1 configuration, a VistA instance deployed within VA's network will connect directly to the Client Boundary (to pass data to/from CPRS) as well to the VAM Boundary (to pass data to the Router and to support metadata sync) through the BPE.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-07.E03 Boundary Protection | Access Points	**SC-07.E03 Boundary Protection | Access Points** The organization limits the number of external network connections to the information system.	

Status		Type	
In Place (Pass)	X	Common	
Planned or In Place and Planned (Fail)		Hybrid	X
		System Specific	

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
All external network traffic connections traverse the VA TICs.
OI&T limits the number of external network connections to the information system.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-07.E04 Boundary Protection | External Telecommunications Services	**SC-07.E04 Boundary Protection | External Telecommunications Services** The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
OI&T:
a. Implements a managed interface for each external telecommunication service;
b. Establishes a traffic flow policy for each managed interface;
c. Protects the confidentiality and integrity of the information being transmitted across each interface;
d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
e. Reviews exceptions to the traffic flow policy (See Attachment 2); and
f. Removes exceptions that are no longer supported by an explicit mission/business need.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-07.E05 Boundary Protection | Deny By Default / Allow By Exception	**SC-07.E05 Boundary Protection | Deny By Default / Allow By Exception** The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-07.E07 Boundary Protection | Prevent Split Tunneling For Remote Devices	**SC-07.E07 Boundary Protection | Prevent Split Tunneling For Remote Devices** The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
To gain access to the environment,
users must be connected to the VA network. Remote users are required to VPN into the VA environment prior to granting access. The VA VPN restricts split-tunneling for remote user access.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-07.E08 Boundary Protection | Route Traffic To Authenticated Proxy Servers	**SC-07.E08 Boundary Protection | Route Traffic To Authenticated Proxy Servers** The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
VAM routes all traffic through the TIC gateway. Authentication proxies are managed by the VA TIC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-07.E18 Boundary Protection | Fail Secure	**SC-07.E18 Boundary Protection | Fail Secure** The information system fails securely in the event of an operational failure of a boundary protection device.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-07.E21 Boundary Protection | Isolation Of Information System Components	**SC-07.E21 Boundary Protection | Isolation Of Information System Components** The organization employs boundary protection mechanisms to separate [Assignment: organization-defined information system components] supporting [Assignment: organization-defined missions and/or business functions].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
OI&T employs boundary protection mechanisms to separate information system components supporting missions and/or business functions
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-08.1 Transmission Confidentiality And Integrity	**SC-08.1 Transmission Confidentiality And Integrity** The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
All network connections to the environment traverses the VA TICs.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-08.E01 Transmission Confidentiality And Integrity | Cryptographic Or Alternate Physical Protection	**SC-08.E01 Transmission Confidentiality And Integrity | Cryptographic Or Alternate Physical Protection** The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-10.1 Network Disconnect	**SC-10.1 Network Disconnect** The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
VAM follows VAEC procedures.
VAM terminates the network connection associated with a communications session at the end of the session or after a period of inactivity
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-12.1 Cryptographic Key Establishment And Management	**SC-12.1 Cryptographic Key Establishment And Management** The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC. The VA establishes and manages cryptographic keys for required cryptography employed within the information system in
accordance with requirements for the key generation, distribution, storage, access, and destruction. Federal law mandating FIPS 140-2 (or its successor) validated encryption for all Federal government systems.
- Public certificates are established and managed by public Certificate Authorities (CA) and the Department of Defense (DoD).
- User access certificates/keys are stored on the PIV cards are managed and established by the VA.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-12.E01 Cryptographic Key Establishment And Management | Availability	**SC-12.E01 Cryptographic Key Establishment And Management | Availability** The organization maintains availability of information in the event of the loss of cryptographic keys by users.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
OI&T maintains availability of information in the event of the loss of cryptographic keys by users.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-13.1 Cryptographic Protection	**SC-13.1 Cryptographic Protection** The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC. In accordance with VA Handbook 6500, VAM utilizes FIPS 140-2 validated encryption (or its
successor) for VA sensitive information during transmissions and at rest.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-15.1 Collaborative Computing Devices	**SC-15.1 Collaborative Computing Devices** The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b. Provides an explicit indication of use to users physically present at the devices.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is not applicable.
OI&T:
a. Prohibits remote activation of collaborative computing devices unless an exception is defined where remote activation is to be; and
b. Provides an explicit indication of use to users physically present at the devices.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-17.1 Public Key Infrastructure Certificates	**SC-17.1 Public Key Infrastructure Certificates** The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
VA issues public key certificates under an appropriate certificate policy or obtains public key certificates from an approved service provider
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-18.1 Mobile Code	**SC-18.1 Mobile Code** The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is N/A to VAM.
OI&T:
a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-19.1 Voice Over Internet Protocol	**SC-19.1 Voice Over Internet Protocol** The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is N/A to VAM.
OI&T:
a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; and
b. Authorizes, monitors, and
controls the use of VoIP within the information system.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-20.1 Secure Name / Address Resolution Service (Authoritative Source)	**SC-20.1 Secure Name / Address Resolution Service (Authoritative Source)** The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
OI&T:
a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-21.1 Secure Name / Address Resolution Service (Recursive Or Caching Resolver)	**SC-21.1 Secure Name / Address Resolution Service (Recursive Or Caching Resolver)** The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
All name resolution data is resolved by VA internal DNS servers.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-22.1 Architecture And Provisioning For Name / Address Resolution Service	**SC-22.1 Architecture And Provisioning For Name / Address Resolution Service** The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
All name resolution data is resolved by VA internal DNS servers.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-23.1 Session Authenticity	**SC-23.1 Session Authenticity** The information system protects the authenticity of communications sessions.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC.
VAM also utilizes the RPC protocol. The RPC protocol is connection-oriented and synchronous with clients opening a connection to VistA and only making new RPC calls after receiving a reply from a previous call.
• Connection establishment and ending define a “client session” in the RPC engine and all RPC traffic on that connection is identified with that session.

- Clients log into VistA in different ways – there are Connection Proxies, CAPRI tokens, BSE tokens, Access Verify, SAML tokens. Each method is recognized by the Router and allows it to associate a client's identity with the session. It is important to note that the Router doesn't implement authentication – it merely notes how VistA responds to different sign on options and changes the client session appropriately.
- Session identity and details are passed into RPC Handlers along with a parsed version of an RPC
- An RPC Handler may signal the Router engine to end a session

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-24.1 Fail In Known State	**SC-24.1 Fail In Known State** The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-28.1 Protection Of Information At Rest	**SC-28.1 Protection Of Information At Rest** The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC. VAEC has a POA&M is in place to address this control.
The VA protects the confidentiality and integrity of sensitive and confidential data while at rest. All sensitive and confidential data is encrypted using FIPS 140-2 compliant algorithms. The VAEC AWS GovCloud High system only utilizes products from the TRM that has the capability to ensure protection of information at rest.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SC-39.1 Process Isolation	**SC-39.1 Process Isolation** The information system maintains a separate execution domain for each executing process.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC and VAEC AWS GovCloud High.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SE-01.1 Inventory Of Personally Identifiable Information	**SE-01.1 Inventory Of Personally Identifiable Information** The organization: a. Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and b. Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

AR-1, AR-4, AR-5, AT-1, DM-1, PM-5.

Control (*)	Description of Control (*)	Control Status/Type (*)
SE-02.1 Privacy Incident Response	**SE-02.1 Privacy Incident Response** The organization: a. Develops and implements a Privacy Incident Response Plan; and b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

AR-1, AR-4, AR-5, AR-6, AU-1 through 14, IR-1 through IR-8, RA-1.

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-01.1 System And Information Integrity Policy And Procedures	**SI-01.1 System And Information Integrity Policy And Procedures** The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy [Assignment: organization-defined frequency]; and 2. System and information integrity procedures [Assignment: organization-defined frequency].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO. OI&T develops, documents, and disseminates policies and procedures enterprise-wide. In accordance with VA Directive and Handbook 6330, the System and Information Integrity Policy is reviewed every five (5) years.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-02.1 Flaw Remediation	**SI-02.1 Flaw Remediation** The organization centrally manages the flaw remediation process.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] Type: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
INHERITED FROM VA EO.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-02.E01 Flaw Remediation | Central Management	**SI-02.E01 Flaw Remediation | Central Management** The organization centrally manages the flaw remediation process.	Status: In Place (Pass) [X]; Planned or In Place and Planned (Fail) [ ] Type: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO. The VA centrally manages the flaw remediation process utilizing the SDM and CMDB for tracking activities, and Ansible, SCCM,
and GitHub Enterprise for release and patch deployment.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-02.E02 Flaw Remediation | Automated Flaw Remediation Status	**SI-02.E02 Flaw Remediation | Automated Flaw Remediation Status** The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO. The VA employs automated mechanisms to determine the state of information system components with regard to flaw remediation. Scans are performed on demand, on a monthly basis, and for new deployments.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-03.1 Malicious Code Protection	**SI-03.1 Malicious Code Protection** The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	<table><tr><th>Status</th><th></th><th>Type</th><th></th></tr><tr><td>In Place (Pass)</td><td>X</td><td>Common</td><td></td></tr><tr><td rowspan="2">Planned or In Place and Planned (Fail)</td><td rowspan="2"></td><td>Hybrid</td><td>X</td></tr><tr><td>System Specific</td><td></td></tr></table>

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC AWS GovCloud High. a. The VAEC AWS GovCloud High deploys McAfee ePolicy Orchestrator (ePO) for malicious code protection and endpoint protection.
b. McAfee ePO agents installed on servers poll the management server on a daily basis. Management servers check for signature updates from McAFee ePO on a daily basis.
c. McAfee ePO is configured to perform daily scans on all server drives and network endpoints. McAfee ePO attempts to delete malicious code first; in the event the malicious code cannot be deleted/removed, then it quarantines the malicious file. Alerts are sent to the management servers for action by the system administrator.
d. Files identified to be malicious are validated by the system administrator for false positives. In the event a false positive is identified, McAfee ePO policies are updated with an exclusion for identified files.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-03.E01 Malicious Code Protection | Central Management	**SI-03.E01 Malicious Code Protection | Central Management** The organization centrally manages malicious code protection mechanisms.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO. The McAfee ePO agents installed on servers poll the management server on a daily basis. Management servers check for
signature updates from McAfee ePO on a daily basis.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-03.E02 Malicious Code Protection | Automatic Updates	**SI-03.E02 Malicious Code Protection | Automatic Updates** The information system automatically updates malicious code protection mechanisms.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO. The McAfee ePO agents installed on servers poll the management server on a daily basis. Management servers check for
signature updates from McAfee ePO on a daily basis.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-04.1 Information System Monitoring	**SI-04.1 Information System Monitoring** The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c. Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO and VAEC AWS GovCloud High.
a. VAM utilizes McAfee ePO, VA SIEM Splunk, and AWS WAFs to monitor information systems for attacks and unauthorized local and remote connections.
b. Identifies unauthorized use of the information system through monitoring security tools.
c. The VA deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization.
d. The AWS WAFs defends information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

e. Logging and monitoring levels are elevated once an increase in threat level is identified by VA internal and external sources.
f. The VA obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
g. VAM relies on the VA NSOC for real-time information system monitoring.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-04.E02 Information System Monitoring | Automated Tools For Real-Time Analysis	**SI-04.E02 Information System Monitoring | Automated Tools For Real-Time Analysis** The organization employs automated tools to support near real-time analysis of events.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from the VA EO. The VA NSOC to employs the VA SIEM Splunk and McAfee ePO as the automated tools that support near real-time analysis of events.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-04.E04 Information System Monitoring | Inbound And Outbound Communications Traffic	**SI-04.E04 Information System Monitoring | Inbound And Outbound Communications Traffic** The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-04.E05 Information System Monitoring | System-Generated Alerts	**SI-04.E05 Information System Monitoring | System-Generated Alerts** The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
The VA NSOC utilizes dashboards and alerts in the VA SIEM Splunk to identify possible compromise. VAM forwards all logs to the VA SIEM Splunk.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-05.1 Security Alerts	**SI-05.1 Security Alerts** The organization: a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This cotrol is inherited from VA EO. VAM leverages the following from VA:
US-CERT: Provides flow and signature-based visibility and alerting into malicious traffic sourced from or destined to VA through the use of Einstein sensors.
Other Government Agencies: VA maintains an intelligence and technique sharing relationship with other government agencies.
Open source research: VA leverages a number of publicly available resources to supplement their security and threat awareness.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-05.E01 Security Alerts | Automated Alerts And Advisories	**SI-05.E01 Security Alerts | Automated Alerts And Advisories** The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This cotrol is inherited from VA EO. VAM leverages the following from VA:
US-CERT: Provides flow and signature-based visibility and alerting into malicious traffic sourced from or destined to VA through the use of Einstein sensors.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-06.1 Security Function Verification	**SI-06.1 Security Function Verification** The information system: a. Verifies the correct operation of [Assignment: organization-defined security functions]; b. Performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]; c. Notifies [Assignment: organization-defined personnel or roles] of failed security verification tests; and d. [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This cotrol is inherited from VA EO and VAEC. VAM forwards all logs to VAEC CLOUDWATCH.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-07.1 Software	**SI-07.1 Software** The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
Inherited from VA EO and VAEC. Access is not authorized for non VAEC users.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-07.E01 Software | Integrity Checks	**SI-07.E01 Software | Integrity Checks** The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
Inherited from VA EO and VAEC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-07.E02 Software | Automated Notifications Of Integrity Violations	**SI-07.E02 Software | Automated Notifications Of Integrity Violations** The organization employs automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.	**Status**: In Place (Pass) — ; Planned or In Place and Planned (Fail) — X **Type**: Common — ; Hybrid — ; System Specific — X

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-07.E05 Software | Automated Response To Integrity Violations	**SI-07.E05 Software | Automated Response To Integrity Violations** The information system automatically [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards]] when integrity violations are discovered.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
Inherited from VA EO and VAEC.

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-07.E07 Software | Integration Of Detection And Response	**SI-07.E07 Software | Integration Of Detection And Response** The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [X] **Type**: Common [ ]; Hybrid [ ]; System Specific [X]

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:

Inherited from VA EO and VAEC.

Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-07.E14 Software | Binary Or Machine Executable Code	**SI-07.E14 Software | Binary Or Machine Executable Code** The organization: (a) Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and (b) Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO. OI&T assesses software products without accompanying source code from sources with limited or no warranty for potential
security impacts. This is accomplished through the VA TRM process. The assessments address the fact that these types of software products may be very difficult to review, repair, or extend given that VA, in most cases, does not have access to the original source code and there may be no owners who could make such repairs on VA’s behalf.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-08.1 Spam Protection	**SI-08.1 Spam Protection** The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO. All email traffic is monitored by VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-08.E01 Spam Protection | Central Management	**SI-08.E01 Spam Protection | Central Management** The organization centrally manages spam protection mechanisms.	**Status**: In Place (Pass) X; Planned or In Place and Planned (Fail) **Type**: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VA EO. All email traffic is monitored by VA NSOC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-08.E02 Spam Protection | Automatic Updates	**SI-08.E02 Spam Protection | Automatic Updates** The information system automatically updates spam protection mechanisms.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-10.1 Information Input Validation	**SI-10.1 Information Input Validation** The information system checks the validity of [Assignment: organization-defined information inputs].	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-11.1 Error Handling	**SI-11.1 Error Handling** The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defined personnel or roles].	**Status** / **Type** In Place (Pass): — Common: Planned or In Place and Planned (Fail): X — Hybrid: System Specific: X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC. The VA only utilizes software that displays error message information that cannot be exploited. Debugging information is stored
in a secure repository and only authorized personnel have access to this information. Hosted applications are required to ensure appropriate error handling in accordance with VA policy.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-12.1 Information Handling And Retention	**SI-12.1 Information Handling And Retention** The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	Status: In Place (Pass) X; Planned or In Place and Planned (Fail) Type: Common; Hybrid X; System Specific

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC. VAM handles and retains information within the information system and information output from the system in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
Evidence: YES

Control Provider

Dick Rickard

Related Controls

MP-2, MP-4.

Control (*)	Description of Control (*)	Control Status/Type (*)
SI-16.1 Memory Protection	**SI-16.1 Memory Protection** The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.	Status: In Place (Pass); Planned or In Place and Planned (Fail) X Type: Common; Hybrid; System Specific X

Implementation

System: *VistA Adaptive Maintenance (VAM) Assessing*:
Responsibility: Badhan Mandal:
Implementation Details:
This control is inherited from VAEC
Evidence: YES

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
TR-01.1 Privacy Notice	**TR-01.1 Privacy Notice** The organization: a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary; b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.	**Status** In Place (Pass): Planned or In Place and Planned (Fail): **Type** Common: Hybrid: X System Specific:

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
TR-01.E01 Privacy Notice | Real-Time Or Layered Notice	**TR-01.E01 Privacy Notice | Real-Time Or Layered Notice** The organization provides real-time and/or layered notice when it collects PII.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] Type: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
TR-02.1 System Of Records Notices And Privacy Act Statements	**TR-02.1 System Of Records Notices And Privacy Act Statements** The organization: a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII); b. Keeps SORNs current; and c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] Type: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
TR-02.E01 System Of Records Notices And Privacy Act Statements | Public Website Publication	**TR-02.E01 System Of Records Notices And Privacy Act Statements | Public Website Publication** The organization publishes SORNs on its public website.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] Type: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
TR-03.1 Dissemination of Privacy Program Information	**TR-03.1 Dissemination of Privacy Program Information** The organization: a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.	Status: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] Type: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

VA Privacy Office (005R1)

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
UL-01.1 Internal Use	**UL-01.1 Internal Use** The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.	**Status**: In Place (Pass) [ ]; Planned or In Place and Planned (Fail) [ ] **Type**: Common [ ]; Hybrid [X]; System Specific [ ]

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Control (*)	Description of Control (*)	Control Status/Type (*)
UL-02.1 Information Sharing With Third Parties	**UL-02.1 Information Sharing With Third Parties** The organization: a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.	**Status** In Place (Pass) ☐ Planned or In Place and Planned (Fail) ☐ **Type** Common ☐ Hybrid X System Specific ☐

Implementation

Control Provider

Dick Rickard

Related Controls

NONE

Appendix A References

VA Directive 6500, “Information Security Program”
VA Directive and Handbook 0710, “Personnel Suitability and Security Program”
VA Directive and Handbook 0730, “Security and Law Enforcement”
VA Directive 6100, “Telecommunications”
VA Directive and Handbook 6102, “Internet/Intranet Services”
VA Directive 6502, “Privacy Program”
NIST SP 800-12, “An Introduction to Computer Security: The NIST Handbook”
NIST SP 800-18, Revision 1 “Guide for Developing System Security Plans”
NIST SP 800-23, “Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products”
NIST SP 800-26, “Security Self-Assessment Guide for Information Technology Systems”
NIST SP 800-27, Rev A, “Engineering Principles for Information Technology Security (A Baseline for Achieving Security)”
NIST SP 800-28, “Guidelines on Active Content and Mobile Code”
NIST SP 800-30, “Risk Management Guide for Information Technology Systems”
NIST SP 800-34, “Contingency Planning Guide for Information Technology Systems”
NIST SP 800-35, “Guide to Information Technology Security Services”
NIST SP 800-36, “Guide to Selecting Information Security Products”
NIST SP 800-37, Revision 1, “Guide for the Security Certification and Accreditation of Federal Information Systems”
NIST SP 800-40, “Procedures for Handling Security Patches”
NIST SP 800-42, “Guideline on Network Security Testing”
NIST SP 800-46, “Security for Telecommuting and Broadband Communications”
NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems”
NIST SP 800-48, “Wireless Network Security: 802.11, Bluetooth, and Handheld Devices”
NIST SP 800-50, “Building an Information Technology Security Awareness and Training Program”
NIST SP 800-53, Revision 4 Final, “Security and Privacy Controls for Federal Information Systems and Organizations”
NIST SP 800-53A, Revision 4 Final, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations."
NIST SP 800-56A, “Recommendation on Key Establishment Schemes”
NIST SP 800-57, “Recommendation on Key Management”
NIST SP 800-60, “Guide for Mapping Types of Information and Information Systems to Security Categories”
NIST SP 800-61, “Computer Security Incident Handling Guide”
NIST SP 800-63, “Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology”
NIST SP 800-64, “Security Considerations in the Information System Development Life Cycle”

Appendix B Acronyms List

3DES Triple Data Encryption Standard (168 Bit)
ACIO Associate Chief Information Officer
ACL Access Control List
ADPAC Automated Data Processing Applications Coordinator
AES Advanced Encryption Services
AHMIA American Health Information Management Association
AIS Automated Information System(s)
AISO Alternate Information Security Officer
ANSI American National Standards Institute
AO Authorizing Official
ATO Authority to Operate
C&A Certification & Accreditation
CBOC Community Based Outpatient Clinic
CEO Chief Executive Officer
CIO Chief Information Officer
CIRT Computer Incident Response Team
CMT Cryptographic Module Testing (lab)
CMVP Cryptographic Module Validation Program
COOP Continuity of Operation Plan
COTS Commercial Off-The- Shelf
CSE Communications Security Establishment
CSP Critical Security Parameters
DES Data Encryption Standard
DNS Domain Name Systems
DOD Department of Defense
DRP Disaster Recovery Plan
DSA Digital Signature Algorithm
DSS Digital Signature Standard
DTR Derived Test Requirement
ECDSA Elliptic Curve Digital Signature Algorithm
EDC Error Detection Code
EFP Environmental Failure Protection
EFT Environmental Failure Testing
E-MAIL Electronic Mail
EMC Electromagnetic Compatibility
EMI Electromagnetic Interference
FAX Facsimile
FC Fibre Channel
FIPS Federal Information Processing Standard
FISMA Federal Information Security Management Act of 2002
FOIA Freedom of Information Act
FOUO For Official Use Only
FSM Finite State Machine
GAO General Accounting Office
GD Government Division
GISRA Government Information Security Reform Act
GSA General Services Administration
HIPAA Health Insurance Portability and Accountability Act of 1996
HMAC Keyed-hash Message Authentication Code
I&A Identification and Authentication
IATO Interim Authority to Operate
IDS Intrusion Detection System

IG Inspector General
IP Internet Protocol
IRM Information Resources Management
IPSEC Internet Protocol Security
IMRB Internet Management Review Board
IP Internet Protocol
IRM Information Resources Management
IRS Internal Revenue Service
ISO Information Security Officer
IT Information Technology
JCAHO Joint Commission on Accreditation of Healthcare Organizations
KAT Known Answer Test
LAN Local Area Network
LEC Local Exchange Company
MISS Medical Information Security Service
MOU Memorandum Of Understanding
MUMPS Multi-User MEMS Processes
NIST National Institute of Standards and Technology
NVLAP National Voluntary Laboratory Accreditation Program
OI Office of Information
OIG Office of Inspector General
OMB Office of Management and Budget
PBX Private Branch Exchange
PFSS Patient Financial Services System
PIN Personal Identification Number
PIX Private Internet Exchange (Cisco)
PKCS #1 Public Key Cryptography Standards
PPD Port Protection Device
RISO Regional Information Security Officer
RNG Random Number Generator
SAM Security Account Manager
SBU Sensitive But Unclassified
SHA Secure Hash Algorithm
SSA Social Security Administration
SSAA System Security Authorization Agreement
SSH Secure Shell
SSL Secure Sockets Layer
ST&E Security Test & Evaluation
TE Test Evidence
VA Veterans Affairs
VAOIG Veterans Affairs Office of Inspector General
VE Vendor Evidence
VHA Veterans Health Administration
VISN Veterans Integrated Service Network
VISTA Veterans Health Information Systems and Technology
VMS Virtual Memory System
VPN Virtual Private Network
WAN Wide Area Network

Appendix C Glossary

Authorization	See Accreditation.
Authorize Processing	See Accrediation.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Authorizing Official Designated Representative	Individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.
Automated Information System(s) (AIS)	An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Certifaction	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Certification Agent	The individual, group, or organization responsible for conducting a security certification.
Chief Information Officer	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Ciphertext	Form of cryptography in which the plaintext is made unintelligible to anyone who intercepts it by a transformation of the information itself, based on some key.

Common Security Control	Security controls designated as common controls within the VA serve the protection needs of the entire VA, and must have management responsibility assigned at an organizational level by the appropriate group and officials instead of the Information System Owner. This centralized management is instrumental in creating cost-effective security protection. Common controls are designed to be "inherited" by information systems. These are designated as VA common controls and are identified in Appendix F, Attachment 1.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control [CNSS Inst. 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.
COTS Software	Commercial Off The Shelf Software - software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.
Countermeasures [CNSS Inst. 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Default	A value or setting that a device or program automatically selects if you do not specify a substitute.
Designated Approving (Accrediting) Authority	See Authorizing Official.
Dial-up	The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.
Encryption	The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to

Facsimile	A document that has been sent, or is about to be sent, via a fax machine.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
Firewall	A system or combination of systems that enforces a boundary between two or more networks.
Gateway	A bridge between two networks.
General Support System [OMB Circular A-130, Appendix III]	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Hardware	Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips.
Hybrid Control	A combination of common and system-specific controls known as a hybrid control. All other controls in Appendix F, including those in Appendix F.
IATO	Interim Authority to Operate. A temporary ATO, valid for a limited time until ATO can be achieved.
Identification	The process that enables recognition of a user described to an AIS.
Information [FIPS 199]	An instance of an information type.
Information Owner [CNSS Inst. 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy [CNSS Inst. 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information System [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner (or Program Manager) [CNSS Inst.4009, Adapted]	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Officer [CNSS Inst. 4009, Adapted]	Individual responsible to the senior agency information security officer, authorizing official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.

Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Internet	A global network connecting millions of computers. As of 1999, the Internet has more than 200 million users worldwide, and that number is growing rapidly.
Intranet	A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.
Intrusion Detection	Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.
LDAP	Short for Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. An unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access.
Least Privilege	The process of granting users only those accesses they need to perform their official duties.

Local Area Network	A short-haul data communications systems that connects AIS devices in a building or group of buildings within a few square miles, including (but not limited to) workstations, front end processors, controllers, switches, and gateways.
Major Application [OMB Circular A-130, Appendix III]	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.
Major Information System [FISMA]	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.
Management Controls	Security methods that focus on the management of the computer security system and the management of risk for a system.
Management Controls [NIST SP 800-18]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Minor Application	An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.
Modem	An electronic device that allows a microcomputer or a computer terminal to be connected to another computer via a telephone line.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency- (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specificallyauthorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of

Network	Two or more systems connected by a communications medium; a network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.
Non-repudiation [CNSS Inst. 4009]	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Operating System	The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.
Operational Controls	Security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).
Operational Controls [NIST SP 800-18]	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
Parity	The quality of being either odd or even. The fact that all numbers have a parity is commonly used in data communication to ensure the validity of data. This is called parity checking.
Password	Protected/private character string used to authenticate an identity or to authorize access to data.
PBX	Short for private branch exchange, a private telephone network used within an enterprise. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.
Peripheral Device	Any external device attached to a computer. Examples of peripherals include printers, disk drives, display monitors, keyboards, and mice.
PFSS	Patient Financial Services
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Port	An interface on a computer to which you can connect a device.
Port Protection Device	A device that authorizes access to the port itself, often based on a separate authentication independent of the computer's own access control functions.

Potential Impact [FIPS 199]	Low: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Moderate: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. High: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
RADIUS	Short for Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUM server, which checks that the information is correct, and then authorizes access to the ISP system.
Real Time	Occurring immediately. Real time can refer to events simulated by a computer at the same speed that they would occur in real life.
Remote Access	The hookup of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information.
Risk [NIST SP 800-30]	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment [NIST SP 800-30]	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Risk Management [NIST SP 800-30]	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
Router	An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link

Safeguards **[CNSS Inst. 4009, Adapted]**	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Security Accreditation	See Accreditation.
Security Authorization	See Accreditation.
Security Category **[FIPS 199]**	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Controls **[FIPS 199]**	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Impact Analysis	The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.
Security Incident	An adverse event in a computer system or the threat of such an event occurring.
Security Objective	Confidentiality, integrity, or availability.
Security Plan	See System Security Plan.
Security Requirements **[CNSS Inst. 4009, Adapted]**	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet laws, Executive Orders, directives, policies, or regulations.
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.
Separation of Duties	A process that divides roles and responsibilities so that a single individual cannot subvert a critical process.
Server	The control computer on a local area network that controls software access to workstations, printers, and other parts of the network.
Smart Card	A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.
Software	Computer instructions or data. Anything that can be stored electronically is software.

Software Copyright	The right of the copyright owner to prohibit copying and/or issue permission for a customer to employ a particular computer program.
SPAM	To crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
System	See Information System.
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
System-specific Security Control	A security control for an information system that has not been designated as a common security control.
TCP/IP	Transmission Control Protocol/Internet Protocol. The suite of protocols the Internet is based on.
Technical Controls	Security methods consisting of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the operating system and applications.
Technical Controls [NIST SP 800-18, Adapted]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Technical Security Policy	Specific protection conditions and/or protection philosophy that express the boundaries and responsibilities of the AIS product in supporting the information protection policy control objectives and countering expected threats.
Telecommunications	Any transmission, emission, or reception of signals, writing, images, sound or other data by cable, telephone lines, radio, visual or any electromagnetic system.
Threat [CNSS Inst. 4009, Adapted]	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Agent	See Threat Source.
Threat Assessment[CNSS Inst.4009]	Formal description and evaluation of threat to an information system.
Threat Source [NIST SP800-30]	Either: (i) intent and method targeted at the intentionalm exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
Trojan Horse	Any program designed to do things that the user of the program did not intend to do or that disguises its harmful intent. A program that installs itself while the user is making an authorized entry; and, then are used to break-in and exploit the system.

User	Any person who is granted access privileges to a a given AIS.
User Interface	The part of an application that the user works with. User interfaces can be text-driven, such as DOS, or graphical, such as Windows.
User Representative	An individual that represents the operational interests of the user community and serves as the liaison for that community throughout the system development life cycle of the information system.
VHA Facilities	As used in this document, refers to those VA elements under the administrative control of the Veterans Health Administration. These elements include the VHA component of VA CIO, Health Care facilities, and the Office of Information Field Offices. Any other elements under the administrative control of the VHA are also included in this definition.
Virus	A self-propagating Trojan horse (a program that surreptitiously exploits the security/integrity of a program), composed of a mission component, a trigger component, and a self-propagating component.
VistA	The VistA name replaced DHCP in 1996 and encompasses the complete information environment at VA medical facilities. This environment includes workstations and personal computers with graphical user interfaces (GUI) and local software developed by VA employees. It also encompasses the links that allow commercial-off-the-shelf software and products such as office automation, Internet browsers, intensive care, and telemedicine systems , to be used with existing and future technologies.
Vulnerability	A weakness in automated system security procedures, technical controls, environmental controls, administrative controls, internal controls, etc., that could be used as a threat to gain unauthorized access to information or disrupt critical processing.
Vulnerability [CNSS Inst.4009, Adapted]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment [CNSS Inst. 4009]	Formal description and evaluation of the vulnerabilities in an information system.
Wide Area Network	A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.