VistA System Security Assessments

Department of Veterans Affairs

Office of Information and Technology (OIT)

March 2022

Version 1.0

Revision History

Date	Version	Description	Author
03/31/2022	1.0	Initial Version	VistA Office

Table of Contents

VistA System Security Assessments

1. Introduction

The purpose of the Veterans Health Information Systems and Technology Architecture (VistA) System Security Assessment section is to capture the objectives, roles, and responsibilities of key security assessments the VistA System undergoes while operating on the Veterans Administration Network. Identifying the security assessment, along with the security assessor's objectives, roles and responsibilities is the point of convergence for managing the intersection of products created by development teams with the respective system. Applying National Institute of Standards and Technology (NIST) Security Standards, Risk Management Framework (RMF), and security controls are the practical steps used to secure and defend the authorization boundaries of the VistA system.

Each year, the VistA System goes through several Security Assessments to ensure security controls have been effectively applied to reduce material weaknesses within its system boundaries. A few of the more prominent Security Assessments conducted are the Annual Office of Inspector General Inspection, Authority to Operate, Authority-to-Connect, along with independent security and privacy control assessments and validations. One of the tenets of the RMF is applying Continuous Monitoring practices to a System. Strong continuous monitoring practices create an assurance that information security practices are in balance. The Secure Assessment section of this guides reminds all members that read this guide their role in securing and protecting the VistA System.

2. Processes

Enterprise VistA Environment Background Information: Enterprise VistA is comprised of virtual servers; RedHat Linux Operating System, InterSystems Cache, and InterSystems Cache and Inquiry Routing and Information System (IRIS) Database Monitoring Systems (DBMS), the VistA database application and over 100 M-based application modules. Each package is comprised of multiple software programs that includes administrative and clinical data. The VistA Kernel software provides identification and authentication, access control via menu management, and auditing of user actions. VA FileMan, the VistA database management software, in conjunction with the Kernel, provides data access control. Access to the system is controlled by set menus and security keys, which are determined prior to the initial issuance of access codes to new users or users who are changing positions within the organization. VistA is accessed by Secure Shell Layer emulators. In order to access VistA additional access is required via an Active Directory account, which requires two-factor authentication. All medical centers have production and pre-production test environments which are located within four VA data centers (Philadelphia, Austin, Sacramento, and Denver respectively.)

3. References

- Authority to Operate: Authority to Operate (ATO) is an official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations. ATOs are approved through the Authorizing Official System Brief (AOSB) process. The AOSB is a form that captures a summary of information and data provided by the System Owner, and the Information System Security Officer captured following the proper execution of the Risk Management Framework, which essentially, allows the Authorizing Official to approve the system's access to the VA network. AOSB information includes describing and explaining the following:

    - VistA System security posture
    - Remediation task/activities
    - Constraints/Impediments addressing Plan of Action & Milestones

- Office of the Inspector General (OIG): Following the mandates of Federal Information System Controls Audit Manual (FISCAM) and /Federal Information Security Management ACT (FISMA,) the OIG evaluate VA's information security program and practices for compliance with specific federal requirements, standards, and regulations. The objective of the audit is to determine the extent in which the VA is in compliance with multiple organizational and publicized security standards.

- Authority to Connect (ATC): In order for VistA to connect to the Defense Health Agency (DHA,) the VistA system must provide DHA with an Authority to Connect package of artifacts listed in the "Provided by Client" section of this document to allow them to review and authorize the external connection.
- Security and Privacy Control Assessment (SCA): The Security Assessment & Validation Division, the Office of Information Security (OIS) personnel conduct control assessments of information systems managed by or for the U.S. Department of Veterans Affairs (VA) using the guidance in applicable NIST standards, VA directives and handbooks, and other guidance provided by OIS leadership. Security and privacy control assessments determine the extent to which security and privacy controls are implemented correctly, operating as intended, and producing the desired outcome. Security and privacy control assessments are required by the Federal Information Security Modernization Act of 2014.

4. Continuous Monitoring Procedures

The fundamental basics of information security is contingent on protecting the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by VistA.

According to NIST SP 800-37, Confidentiality seeks to preserve authorized restrictions on information access and disclosure; Integrity is preventing improper information modification or destruction, while ensuring information non-repudiation and authenticity; Availability is ensuring timely and reliable access to use of information. The combination of Confidentiality, Integrity, and Availability is known as the CIA triad. Threats to VistA include hardware failure, system and/or service disruptions, human or machine errors, as well as orchestrated attacks that lessen the ability of VistA users to complete their tasks.

Information Assurance personnel focuses on addressing threats and vulnerabilities of an Information System from the CIA triad perspective by using continuous monitoring practices from the risk management framework. Continuous Monitoring involves ongoing assessments along with the analysis of security controls associated with an information system. Below are key assessments, tasks, and practices used to secure Enterprise VistA:

- Authority to Operate:
  - Authority to Operate Memo
  - Boundary and System Design network drawing
  - Hardware and Software List
  - Vulnerability Scans
    - Nessus Scan is a credential discovery vulnerability scan against all VistA instances to identify security flaws
    - BigFix Scans encompasses a continuous monitoring process that run on VistA system endpoints with a focus on VistA DISA STIG baseline configuration file
  - Risk Assessment Report: Identifies, estimates, and prioritizes risk involved with organization operations

- Contingency Plan: Interim measures deployed to recover information system services after a disruption
  - Incident Response Plan: Allows for rapidly detecting incidents, minimizing loss and destruction, mitigating weaknesses that could be exploited, and restoring computing services
  - Information Security Contingency Plan: Documented procedures to recover VistA systems after a disruption

- Plan of Action and Milestones Reports: Captures the description of security weaknesses, while identify parties responsible for resolving weaknesses to include times frames that includes milestones for ongoing security weaknesses, and completion dates for resolved security issues.

- Configuration Management Plan: Identifies configuration management roles and responsibilities, resources, and processes to ensure changes are evaluated and approved before implementation.

- Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA): The PTA is a privacy compliance and risk management tool that determines whether PII/PHI is collected and maintained in an IT system. PTA determines whether a PIA is required,

which identifies the privacy and security risk associated with the use of sensitive, personal of information.

- Interconnection Security Agreements (ISA)/Memorandum of Understanding (MOU): Developed to authorize a connection between information systems that do not share the same Authorizing Official. Also required for all external connections.
- System Security Plan: A report generated in Enterprise Mission Assurance Support Service (eMASS) after all the completion of all assessments to include POA&M items and responses.

5. Contacts

- DevSecOps Information Assurance
  - Coordinates security and risk management within OI&T
  - Manages the ATO process for VA's Authorizing Officials
  - Prepare and reviews ATO security packages
  - Execute Security Assessments
  - Performs System Security Categorizations

- Office of Information Security
  - Manages the VA's Enterprise Cybersecurity Program
  - Enterprise Cybersecurity Strategy Program consist of:
    - Executing VA's cybersecurity and risk management policies
    - Establishment of centralized policy and implementation guidance repository Knowledge Service
    - Implementation of NIST Cybersecurity Framework and Risk Management Framework

- Security Assessment & Validation Division
  - Responsible for conducting independent security and privacy control assessment and validation activities
  - Provides Security Controls Assessment Report along with findings and
  - recommendations after the conclusion of the inspection

- Privacy Service
  - Privacy Service leads the charge in the protection of Veteran and Employee personal information and advocates privacy awareness across the Veterans Administration
  - The Privacy Service collaborates with privacy officers in VHA, VBA, NCA, Field Offices, as well as VA Central Office
  - PS seeks to implement privacy policy, identify, and mitigate privacy risks
  - Informs VA personnel on their roles and responsibilities to safeguard personally identifiable information
  - Privacy Officers work alongside with Information System Security Officers to investigate privacy complaints

- Information Security Operations
  - The ISO sets the direction for the VA's cybersecurity operations and privacy actions
  - ISO synchronizes VA strategic guidance into VA's cybersecurity and privacy efforts through
  - Cybersecurity Operations Center, Information Security Risk Management, and the Data Breach Response Service

- Quality, Performance, and Risk
  - Oversees all aspects of quality and compliance with OI&T
  - The Compliance Readiness division with QPR manages the full OIG Auditing Lifecycle Process
  - OIG Audit Lifecycle Process

- IT Operations and Services
  - End User Operations provides direct technical and information security support to VA staff at every physical location in the enterprise
  - Infrastructure Operations
  - Software Product Management manage acquisitions, budgets and arrange resources to deliver and sustain software products

- Solutions Delivery is responsible for engineering solutions through the following divisions:
  - Business Systems Engineering
  - Infrastructure Engineering
  - Endpoint Engineering
  - Security Engineering