VistA Reference Guide

TMS Training ID - VA 4645511
May 1, 2025 | VistA Office
Version 3.3

U.S. Department of Veterans Affairs
Office of Information and Technology

Document Change Control Table

Version	Release Date	Description	Author
3.3	05/01/2025	• Updated VistA Office (VO) Change Control Board (VOCCB) VistA Patch Decision (VPD) dashboard link in section 7.11.3. • Updated the Process Asset Library (PAL) link in section 7.4.3 References and section 9 Additional References. • Added new Section 7.2 VistA Software Document Library (VDL). • Added "Commercial-off-the-Shelf (COTS) Interface representative(s)" to 4th bullet in Section 7.3 VistA Office Review Board (VORB). • Added a single sentence of process descriptive text to Section 7.5.2 VistA Package Namespace Setup Guide - Processes. • Monograph link updated in document to point to new SharePoint site. • Added ICR Lookup link to section 7.6 References.	VistA Office
3.2	11/08/2024	Updated VistA Office Background section 4, VistA Authorization Boundary Data Flow Diagram Figure 6-1, VORB section 7.2, VistA System Security Assessment section 7.11.2	VistA Office
3.1	10/10/2023	New, updated content has been added to section 7.4 VistA Package Namespace Setup Guide. New linked references have been added to: • Monograph References section 7.1.3 - VA Systems Inventory (VASI), • HL7 References section 7.7.3 (along with brief explanatory text) - Examples - HL7 Interface Documents and Resource Emails folder, and • Additional References section 9: ▪ Software Product Management (SPM) Health Intake Training, ▪ VistA Monograph – New Item Form Entry, ▪ VASI Registration Form – VA | Enterprise Architecture, and ▪ VistA Office - VDL Service Request Form.	VistA Office
3.0	6/27/2023	Three additional sections have been added: • VistA Monograph (Section 7.1), • VistA HL7 (Section 7.7), and • Veterans Data Integration and Federation – Enterprise Platform (VDIF-EP) (Section 7.8). Figure 6-1: VistA Authorization Boundary Data Flow has been updated. For purposes of greater accessibility, the alt-text description for Figure 6-1 has also been rewritten to achieve greater clarity for those sight-impaired, with color-coding references removed and a more detailed description of diagram structure and content provided.	VistA Office
2.0	10/31/2022	Added two new sections: section 7.1 The VistA Office Review Board (VORB) and section 7.2 Standards and Conventions (SAC).	VistA Office

Version	Release Date	Description	Author
		Implemented formatting, structural, and readability enhancements in accordance with OIT Style Guide, VA Product Guide, and Plain Language guidelines.	
1.0	03/31/2022	Initial Version	VistA Office

Table of Contents

Tables

Figures

New TMS VA 4645511 Self-Certification Training Recommendation:
The VistA Reference Guide and its supporting documents are now recommended TMS training for VistA Developers. TMS Training ID is **VA 4645511**.

1. Purpose

The Veterans Health Information Systems and Technology Architecture (VistA) Reference Guide was created by the VistA Office (VO) to provide product teams with a valuable reference document which must be followed to ensure the success of internal and external products interfacing with VistA. The VistA Reference Guide is intended for product team members, including Developers, Product Line Managers, and Stakeholders who make design decisions for the product being developed.

The VistA Reference Guide (VRG) provides interface reference information to ensure product teams adhere to:

- Authorized systems/application boundaries
- Product namespace boundaries for all product software components
- VistA provisioning, authentication, and authorization requirements
- Obtaining approval for interfaces which deviate from the authorized boundaries and Identity Access Management (IAM)/Kernel guidance
- Receiving approvals for interface agreements between two products before going to production testing in the development lifecycle
- M Programming Standards

Additionally, the VistA Reference Guide provides reference information related to:

- National Patch release requirements to facilitate VistA Change Management
- Periodic security assessments

The guidance provided in this document has previously been available from sources such as the Process Asset Library (PAL) and VA Software Document Library (VDL) and has now been combined to create a consolidated artifact. This artifact can be used to ensure products abide by authorized boundaries, interfaces, security, and processes.

2. Assumptions

The following are baseline assumptions defining the intentions, boundaries, and scope of this document:

- The immediate focus of the VistA Reference Guide is addressing authorization boundary and interface reference materials for internal and external products interfacing with and within VistA.
- The VistA Reference Guide is not intended to address the VistA Development Life Cycle and Agile development methodology used within VA.
- The VistA Reference Guide is a living, iterative document and will be updated as the VistA Office expands the references to additional guidance, processes, and standards for product team awareness.
- The Massachusetts General Hospital Utility Multi-Programming System (MUMPS) programming language will be referred to as M code in this document.

3. Target Audience

The target audience is any product team developing, enhancing, supporting, or maintaining a product which interfaces with VistA, to include:

- VA Office of Information and Technology (OIT) Class 1 product teams
- VA OIT field offices (Class 2 and 3), and field product teams
- Business-partners external to VA (Class 2 and 3) product teams

This document will refer to product teams, a term encompassing Developers, Product Line Managers, and Stakeholders.

4. VistA Office Background

The Director of the VistA Office (VO) is the VistA Information System Owner (ISO). The VO has three pillars established to address the VO mission: Information Assurance, Configuration and Change Management and Business Operations Management. More information on VO and each Pillar can be found at VistA Office - Home (sharepoint.com).

VO was established to serve as a standing body for issue resolution for the many organizational stakeholders within the VistA domain. The VistA ISO is responsible for all VistA Risk Management Framework (RMF) lifecycle activities and ensuring compliance with information security requirements.

The VistA Reference Guide (VRG) was created as a tool to support the VO mission and is based on obstacles identified by the VO with existing and new products.

5. VistA Background

VistA is a comprehensive, full-featured Health Information System and Electronic Health Record (EHR) owned by the Veterans Affairs Office of Information and Technology (OIT). VistA supports a large variety of clinical settings. Facilities range from small clinics solely providing outpatient care to large medical centers with significant inpatient populations and their associated specialties.

VistA modules focus on clinically relevant record keeping which improves patient care by enhancing clinical and administrative decision making. VistA is utilized across VHA at more than 1,500 sites of care supporting Veterans Affairs Medical Centers (VAMC), Community Based Outpatient Clinics (CBOC) and Community Living Centers (CLC), as well as at nearly 300 VA Vet Centers. Enterprise VistA serves America's veterans by supporting exceptional quality healthcare. The VistA modules support a multitude of areas including medical and mental health treatment, medical imaging, supply management, decision support, medical research, and education. The purpose of the system is to collect, create, and maintain data about our VA employees, volunteers, business partners, and veterans.

VistA is comprised of the following:

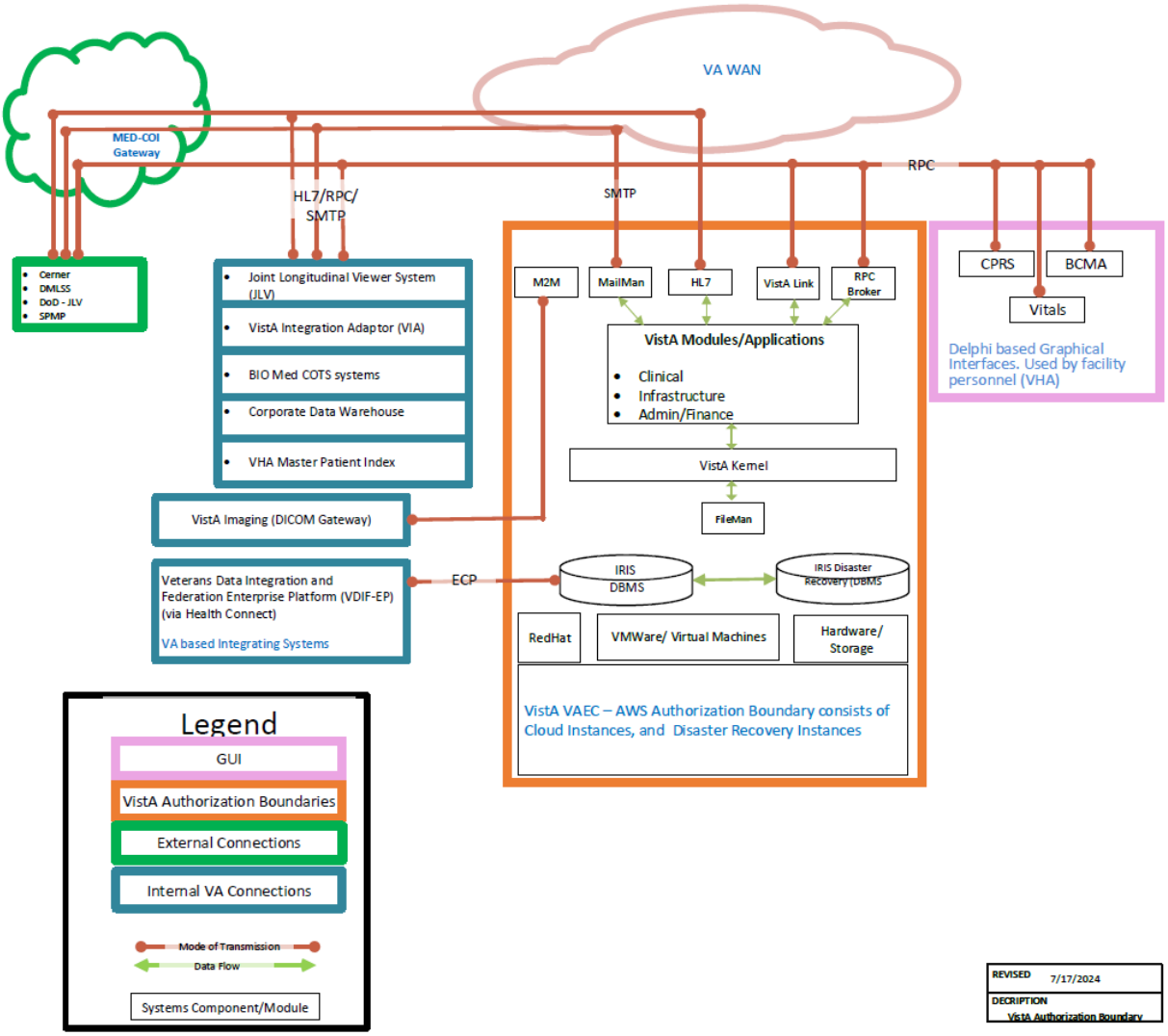
- Virtual servers
- The RedHat Linux Enterprise Operating System
- Ask VA (AVA) (Ask VA has replaced the Inquiry Routing and Information System.)
- Database Monitoring Systems (DBMS)
- The VistA database application
- Over 100 M-based application modules

Each package is comprised of multiple software programs which includes administrative and clinical data. 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 Kernel, provides data access control. Access to the system is controlled by assigned 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.

6. VistA Authorization Boundary Data Flow

Refer to Figure 6-1. The VistA Authorization Boundary Data Flow illustration depicts everything falling within VistA authorization boundaries and the flow of data entering and leaving VistA. Under the direction of the VistA ISO, the Information Assurance Staff applies the Risk Management Framework (RMF) and National Institute of Standards and Technology (NIST) standards on a continuous basis to secure the boundaries through the topics introduced in this reference guide.

Figure 6-1: VistA Authorization Boundary Data Flow



The VistA ISO is responsible for maintaining the Authority to Operate (ATO) on the VA network for that portion depicted in Figure 6-1 outlining VistA Authorization Boundaries.

Nationally released OIT DevSecOps Software Product Management (SPM) VistA software includes all interfaces installed on or interacting with VA computing environments. The OIT DevSecOps SPM VistA software reference documents are accessible by following the links in the Additional References Section of this document:

- VA Software Document Library (VDL)
- VA Enterprise Architecture (EA) VistA Dashboard
- VA System Inventory (VASI)

Refer to Table 6-1, which lists the acronyms used in Figure 6-1.

Table 6-1: Acronyms

Acronym	Expansion
AITC	Austin Information Technology Center
AVA	Ask VA
AWS	Amazon Web Services
BCMA	Bar Code Medication Administration
COI	Community of Interest
COTS	Commercial Off the Shelf (software)
CPRS	Computerized Patient Record System
DBMS	Database Management System
DMLSS	Defense Medical Logistics Standards Support
DoD-JLV	Department of Defense - Joint Longitudinal Viewer
GUI	Graphic User Interface
HL7	Health Level Seven
IRIS	InterSystems IRIS for Health (where 'IRIS' denotes Interoperable, Reliable, Intuitive, Scalable)
JLV	Joint Longitudinal Viewer System
M2M	MUMPS to MUMPS
MED-COI	Medical Communities of Interest
PITC	Philadelphia Information Technology Center
RPC	Remote Procedure Call
RPC Broker	Remote Procedure Call Broker
SMTP	Simple Mail Transfer Protocol
VDIF-EP	Veterans Data Integration and Federation Enterprise Platform
VIA	VistA Integration Adaptor
VistA VAEC	VA Enterprise Cloud
VMWare	Virtual Machine
WAN	Wide Area Network

7. VistA Reference Guide Sections

This section provides detailed guidance on the VistA Monograph, VistA Office Review Board (VORB), Standards and Conventions (SAC), VistA Package/Namespace Setup, Integration Control Registration, Interface Requirements, Kernel Security, Health Level Seven (HL7), Veterans Data Integration Federation – Enterprise Platform (VDIF-EP), VistA National Patch Release Requirements, and VistA System Security Assessments.

7.1. VistA Monograph

This section describes the VistA Monograph, its function, and processes.

7.1.1. Introduction

The VistA Monograph provides an overview of VistA and VistA-related applications used by the VHA in serving America's veterans. This collection serves as an introduction and resource to VHA software. The Monograph also provides a brief historical and technical overview of VistA.

Each application listed in the Monograph contains valuable information, such as VA Systems Inventory (VASI) Name, VA Package Name, Version, Namespace, Software Product Management (SPM) Product Line, VASI System Status, and VHA Business information. Legacy and supplemental application information is also listed as Technical References in the Monograph. Additionally, mapping and linkage to VASI and the VA Software Document Library (VDL) is provided.

7.1.2. Processes

The VistA Monograph document is the result of supporting information provided by OIT, to include SPM Product Lines who oversee the applications. On a yearly basis, VistA Office facilitates the review and update process of the Monograph document with the Product Lines. The updated Monograph document is then published to both the VDL website and the OIT SPM VistA Office SharePoint site. For more information regarding this process and to discuss any changes, including additions to Monograph, please use the VistA Office contact information below.

7.1.3. References

Monograph references are available at:

- VA Software Document Library
- VistA Office Monograph
- VA Systems Inventory (VASI)

7.1.4. Contact

For more information on the Monograph, please contact OIT SPM Monograph at OITPDProductSupportMonograph@va.gov.

7.2. VistA Software Document Library (VDL)

This section describes the VA Software Document Library (VDL), its function, and processes.

7.2.1. Introduction

The VA Software Document Library (VDL) is a public-facing repository which stores and makes available redacted reference materials regarding released VistA Class I software applications in VA.

The VDL Manager is an application internal to the VA and is used by authorized users to update and maintain the redacted, Section 508-compliant documents found on the VDL.

7.2.2. Processes

Access to the VDL Manager Application is requested via the VDL Service Request Form and can also be found on the VDL Service Management SharePoint site. The VDL Service Request Form is also used to request that new applications to be added to the VDL or to report issues concerning the VDL.

- The publishing user (VDL Manager) ensures all documents uploaded to the VDL are properly redacted and Section 508-compliant.
- For Section 508 compliance and accessibility issues, VA recommends installing the CommonLook Commercial of the Shelf (COTS) product for Microsoft Word and Adobe Acrobat since this is the tool used by the Office of the CIO to verify compliance.
- The Section 508 Office site has instructions on obtaining the CommonLook plug-in for both Word and Adobe products at Desktop Productivity Tools - Section 508 Office (va.gov).

7.2.3. References

VDL references are available at:

- VDL Service Management
- VA Software Document Library (VDL)

7.2.4. Contact

For more information regarding the VDL, please contact the VA Software Document Library Administrators at VASoftwareDocumentLibraryAdministrators@va.gov.

7.3. VistA Office Review Board (VORB)

This section describes VORB function, roles, and processes.

7.3.1. Introduction

The VistA Office Review Board (VORB) is a review and decision-making body, the purpose of which is to process requests including, but not limited to, Service Accounts and Application Interface connectivity to VistA.

The VORB process consists of four actors:

- Requestor, the person submitting the request for a VORB determination.
- Members of the VistA Office (VO) Team tasked to perform VORB Request Intake and Assessment functions.
- VistA Working Groups composed of Subject Matter Experts (SMEs) tasked to analyze requests and make recommendations to the VORB based on those analyses.
- The VORB, composed of the VO Information System Owner (ISO) and Director, the VistA Office Information Assurance (VOIA) Team Lead, the VO Management Analyst, the VistA Office Change and Configuration Management (VOCCM) Team Lead, the Sub-Product Line Manager, Operations First Response (OFR), Applications Division representative(s), Health Systems Engineering representative(s), a designated VistA Technical Lead, the VistA Information System Security Officer (ISSO), Commercial-off-the-Shelf (COTS) Interface representative(s), and any other members selected for this role by the Director.

7.3.2. Processes

The VORB process is comprised of four component subprocesses, beginning with the initial submission by the Requestor and culminating with a final VORB decision:

- **SharePoint VORB Intake Form Access and Entry:** The Requestor accesses, completes and submits the VORB Intake Form, which initiates a SharePoint display notifying the Requestor that their request has been successfully submitted.
- **Initial Intake and Assessment:** Once submitted, the completed form is assessed by members of the VO Team, which reviews the submission and checks for its validity, correctness, and completeness. Determination of invalid, incorrect, or incomplete requests serve as a SharePoint notification trigger, causing an email to be sent to the requestor and informing them of the request status and providing guidance appropriate to that status.
- **VistA SME Working Group Analysis and Recommendation:** Once the VO Team determines the request is valid, correct, and complete, the VORB Intake form is either prepared by the VO Team for further processing or, if a SME is deemed necessary, forwarded to the appropriate VistA SME Working Group, which then conducts its analysis and makes its recommendation.

- **VORB Review and Decision:** Once the Request Form is ready for VORB review and determination, the request is assigned to the VORB meeting agenda. The VO Team then presents the VORB with the analysis of and recommendation for that Request. Note there are five possible outcomes to any given request:
  - Approval
  - Approval with Constraints
  - Closed, No Action
  - Denial
  - Escalation

7.3.3. References

The following references are available on SharePoint in the VistA Office Review Board (VORB) folder:

- VistA Office Review Board (VORB) Standard Operating Procedure (SOP)
- VistA Office Review Board (VORB) Review Request Process Guide

7.3.4. Contact

For more information, please contact the VORB at OIT_DSO_SPM_HEALTH_VISTA_OFFICE_VORB@va.gov

7.4. Standards and Conventions (SAC)

This section provides information regarding VistA Standards and Conventions (SAC).

7.4.1. Introduction

Standards and Conventions (SAC) specify coding practices that *must* be adhered to (standards), and which *should* be adhered to (conventions) in VistA code. It is a set of requirements that supplements the language standard: ISO/IEC 11756:1999 *Information Technology – Programming Languages – M* by specifying constraints that must be adhered to by M based applications in the VistA environment for VistA to operate properly. Adherence to the SAC is crucial to maintaining security and privacy of data and maintaining system integrity. As an example, modern programming languages such as Java or Python typically provide namespaces as a language feature, but in VistA, segregation of code and data into individual packages (Order Entry, Lab, Pharmacy, etc.) is accomplished by imposing standards which must be followed by VistA code over and above the ISO standard.

- **System Boundaries:** For the purposes of the SAC, VistA may be defined as the set of M based applications based on Kernel and VA FileMan that run in a medical center environment. Other environments based on Kernel and FileMan such as FORUM, Master Patient Index (MPI)/Master Veteran Index (MVI), and VA Central Office (VACO) are generally considered not to fall within the system boundaries of VistA. Applications running in the medical center environment may be divided into nationally released and supported Class 1 applications and Field Enhancement and Sustainment (FES) approved

Class 2 applications, which *must* adhere to the provisions of the SAC, and locally developed and supported Class 3 applications which *should* adhere to the SAC.

- **Conformance and Exemptions:** The SAC also provides for uniformity of interfaces and a consistent user experience. Modern computer architectures and the needs of interoperability sometime require that applications vary from the SAC, so a process exists for granting exemptions (e.g., to use InterSystems ObjectScript language elements to implement web services). Exemptions are granted by a majority vote of the SAC Working Group (SAC WG) and are normally for one version only, although there are some standing exemptions, as well.
- **Compliance:** As a mechanism for ensuring compliance, Kernel Toolkit provides a tool known as XINDEX, a static analysis tool that, among other things, attempts to identify standards violations. Since M is a dynamic language, static analysis tools are limited (e.g., they cannot evaluate code built at runtime) so manual review of code to ensure compliance is also essential.

7.4.2. Processes

VistA code is modified through the release of patches, although in some rare circumstances new packages (or modules) may be introduced as VistA components. Patches are maintained through an application known as the National Patch Module (NPM). It serves both as a code repository and version management system. It also automates several aspects of the patch lifecycle.

7.4.3. References

The SAC Work Group maintains four documents describing the processes that must be followed when developing patches. These documents are the definitive references for the processes that must be followed when entering, developing, and reviewing patches, and are available on the Standards and Conventions - Home SharePoint Site and in the OIT Process Asset Library (PAL).

- Primary Developer Checklist
- Secondary Developer Checklist
- Software Quality Assurance (SQA) Checklist
- National Patch Module Guide (NMPG) (Note: The National Patch Module Guide (NPMG) provides details on how to use the National Patch Module.)

Additional SAC references include the following:

- ISO/IEC 11756:1999 Information Technology – Programming Languages – M (Note: This document was originally published as ANSI X11.1-1995)
- M Standards and Conventions (Available in the VA Technical Reference Model (TRM))
- Standards and Conventions - Home (sharepoint.com)

7.4.4. Contact

For more information on SAC, please contact the VA OIT EPMO M SAC Working Group at VAOITEPMOMSACWG@va.gov.

7.5. VistA Package Namespace Setup Guide

This section provides guidance on the VistA Package Namespace Setup for product development teams who have identified the need for a new unique package name, namespace and file range which will be used to define the application boundaries for a new product. Detailed information is available in the VistA Package Namespace Setup Guide, linked in the References section below.

7.5.1. Introduction

The VA requires all product development using M code to work within assigned package application boundaries. The package is defined in the PACKAGE file (#9.4) in FORUM by the Database Administration (DBA) Team. The PACKAGE definition entry will include package class, prefix (namespace), file range low and high numbers, and other identifying information which define the application boundary. The package namespace is used to prevent conflicts within VistA applications.

7.5.2. Processes

To request a new Package Namespace please contact the VA OIT VISTA DBA GROUP at OEDVistADBA@va.gov. Packages distributed as a VistA Class 1 product will also require a second process to set up the National Patch Module in FORUM for the new package. This process is required to release VistA package software.

When a patch is approved and ready for the first patch release from the National Patch Module, the Project manager needs to add the Product information and/or documentation to the following repositories for public access to Monograph, VA System Inventory (VASI), and VDL Service Management. To enter a request on the VDL Service Management site, use the VistA Office - VDL Service Request Form.

7.5.3. References

The VistA Package Namespace Setup folder has the following reference information:

- VistA Package Namespace Setup Guide
- VDL – Request New Application

The following are additional links that are discussed in the VistA Package Namespace Setup Guide:

- Monograph
- VistA Monograph – New Item Form Entry
- VA Software Document Library (VDL)
- VistA Office - VDL Service Request Form
- VA System Inventory (VASI)
- VA Directive 6402 Modifications to Nationally Released VistA Software is available in 'Useful Links' on the VistA Reference Guide SharePoint page.

- National Patch Module Guide is available in the National Patch Release Requirements folder.

7.5.4. Contact

For more information on VistA Package/Namespace Setup, please contact the DBA group at OEDVistADBA@va.gov.

7.6. Integration Control Registration (ICR)

This section provides information on Integration Control Registrations (ICRs) to product teams who develop a product containing a reference to a software component outside the product's application boundary (namespace). Software components include file, routine, remote procedure, option, protocol, application proxy and other access external to the product's package domain.

7.6.1. Introduction

VistA software has over 150 unique Class 1 products with Released Patches containing the software components owned by the Packages. The authoritative source for each integration agreement between two packages is defined in an Integration Control Registration (ICR).

ICRs, or integration agreements, are needed between the custodial package owning the software component and the subscribing package using the software component.

7.6.2. Processes

The following processes will be involved with establishing ICRs for the package:

- ICRs and Product Developer's Role
- ICR Definitions in FORUM
- ICR Request Process

7.6.3. References

- The VistA Office has created an ICR Process and Standards SharePoint site to provide guidance to all ICR-related content.
- Standards and Conventions Work Group SharePoint site
  - M Programming Standards and Conventions SAC (Available in the Documents section of the SAC SharePoint site)
- M Programming Standards and Conventions SAC Document (Available in the VA Technical Reference Model (TRM))
- VistA ICR Lookup

7.6.4. Contact

For more information on ICRs, please contact the OIT DSO SPM Health VistA Office Integration Control Registrations group at ICRS@va.gov.

7.7. Interface Requirements

This section provides information on Interface Requirements to both Product owners and developers on the implementation of common VistA interfaces communicating and transmitting data between two or more applications or systems. For more information regarding implementing, enhancing, maintaining, and supporting infrastructure-related products and projects, refer to the site maintained by VistA Infrastructure Shared Services (sharepoint.com).

7.7.1. Introduction

The tenets of the Identity Management process are followed to ensure user account creation (proper permissions are applied, changed, or disabled according to standard practices). A keen focus on User Identity Provisioning, User Authentication, and User Authorization must be woven within interface development practices.

7.7.2. Processes

This section encompasses Fundamental and Non-Fundamental Interfaces used to connect remote applications or systems to VistA. The term fundamental interface is used to identify the most common remotely connected interfaces which are well documented, developed, and follow the recommended development standards for VistA. To reduce scheduling delays in the release of an interface, VistA Link, Remote Procedure Calls, and Terminal Session are the three primary remote connections used to connect an application or system within VistA.

Non-fundamental interfaces connecting to VistA include—but are not limited to—the following:

- VistA Integration Adapter
- Server Options
- MUMPS-to-MUMPS Server
- Veterans Data Integration and Federation

These non-fundamental interfaces are unique remote connections that all follow a documented, developed implementation process and may require additional time and resources to securely interconnect with VistA. Non-fundamental interface requirements are documented in detail in the Interface Requirements reference document linked in the References section below.

The development of a non-fundamental interface must begin by contacting the VistA Office Review Board (VORB). Any design, architectural or coding standards and conventions applied to the development of non-fundamental interfaces must be reviewed by VistA security and integration experts before development begins. An ongoing dialog between non-fundamental interface developers, VistA security, and integration experts can be expected. To meet this need and formalize this ongoing collaborative process, the VORB has been created. For more information regarding VORB roles and processes, refer to section 7.2.

7.7.3. References

The following references are available on SharePoint in the Interface Requirements folder:

- Interface Requirements
- VistALink System Management Guide v1.6
- VistALink Developer Guide v1.6
- Kernel Authentication and Authorization for J2EE (KAAJEE) v1.2.0 Deployment Guide
- RPC Broker 1.1 Developers Guide.
- FileMan Delphi Components 1.0 (FMDC) Getting Started Guide,
- FileMan Delphi Components (FMDC) Technical Manual and Security Guide
- Kernel 8.0 & Kernel Toolkit 7.3 Technical Manual
- VistA Health Level Seven (HL7) Site Manager and Developer Manual
- VistA Messaging Services_HL7 Optimized (HLO) Developer Manual
- HealtheVet Web Services Client (HWSC) 1.0 Developer's Guide

7.7.4. Contact

For more information on Interface Requirements, please contact the VistA Process Governance Workgroup at VISTAProcessGovernanceWorkgroup@va.gov.

7.8. VistA Health Level Seven (HL7)

This section describes the VistA Health Level Seven (HL7) Package.

7.8.1. Introduction

HL7 is an American National Standards Institute (ANSI) standard messaging protocol that specifies the set of transactions and encoding rules for electronic data exchange between healthcare computer systems. In HL7, information is exchanged using HL7 messages when an event occurs in an application. Each HL7 message consists of one or more HL7 segments. To better grasp its function, think of an HL7 segment as a record in a file.

- Consisting of a set of utility routines and files that provide a generic interface to the HL7 protocol, the VistA HL7 package assists VistA applications in the exchange of healthcare information with other applications using the HL7 protocol.
- The VistA HL7 package can be divided into two parts: Lower-level protocol support and VistA interface to the HL7 protocol. Note the VistA HL7 package does not provide tools supporting either HL7 International standard version 3 or Fast Healthcare Interoperability Resources (FHIR).
- VistA HL7 is an implementation of the International Standard HL7 v2.x. VistA HL7 is an 'infrastructure package' within VistA, similar to MailMan, FileMan, VistALink, and Kernel. The current version of the VistA HL7 Package is v1.6. (v1.5 is also supported.)
- VistA HL7 is one of the fundamental means by which VistA communicates with other systems (including other VistA systems).

For more comprehensive information regarding VistA HL7 package functionality, refer to the documents listed and linked in section 7.7.3. References.

7.8.2. Processes

» **Lower-level Protocol Support**

The VistA HL7 package supports the following lower-level interfaces, which provide protocol support between sending and receiving applications:

- HL7 Hybrid Lower Layer Protocol over an RS-232 connection
- VistA MailMan messages
- X3.28
- Minimal Lower Layer Protocol (MLLP) over Transmission Control Protocol (TCP) both Original and HL7 Optimized (HLO)

Using these lower-level interfaces, the VistA HL7 package can support Layers 1–4 of the Open Systems Interconnection (OSI) model and eliminate the need for VistA applications to write lower-level interfaces each time these VistA applications seek to exchange data with another application.

These lower-level interfaces perform the following functions:

- Receive and send HL7 messages.
- Validate the HL7 Message Header (MSH/BHS/FHS) information.
- Invoke the appropriate VistA application routine to process the data in the message.
- Send HL7 accept acknowledgment (ACK) messages back to the sending application.

» **VistA Interface to the HL7 Protocol**

- **Modules**

  VistA HL7 supports several methods/Modules for interfacing to the HL7 protocol. The method established by v1.5 is still supported, but there are three other 'modules' available: MailMan, TCP, and HLO.

  - **V1.5 Module:** This is still supported for backwards compatibility; however, sites are encouraged to migrate to one of the other three Modules. Some sites still use the v1.5 module for legacy lab interfaces.
  - **MailMan Module:** Email messages containing HL7 Messages are created/received via MailMan.
  - **Original TCP (aka Standard) TCP Module:** Messages are transmitted via MLLP over TCP. This is by far the most used Module, with the greatest amount of understanding by the support and development community.
  - **HLO Module**: This was initially developed to replace the original TCP Module, but despite certain functional and efficiency enhancements, the HLO Module is often the second choice for new development projects.

- **Relationship to Application Packages**

  The transmission and processing of HL7 messages requires both the VistA HL7 package and application logic.

  - The functions of event analysis, data extraction, and data filing must be performed by each application package.
  - The VistA HL7 package provides the following utilities to assist the application package with data formatting:

    - Creation of HL7 Message Header (MSH) segments
    - Utility calls to convert HL7 data to VA FileMan formats and vice versa
    - Validation of Message Header information for all HL7 messages received
    - A set of pre-defined variables for use in building HL7 messages/segments

  - The VistA HL7 package provides the following functions to assist the application package with message administration:

    - Support for tracking transmissions and providing a status for each
    - Generation of reports on pending transmissions and transmissions with errors
    - A queue for incoming and outgoing transmissions
    - Real-time monitors to monitor active transmission links and their statuses

7.8.3. References

The following references are available in the VA Software Document Library:

- HL7 HL*1.6 HLO VMS Developer Manual
- HL7 V. 1.6*161 Site Manager Developer Manual

The following training is available via the VA Talent Management System (TMS):

- Introduction to VistA HL7
- VistA HL7 Intermediate

The following reference is available in the VistA Office SharePoint HL7 folder:

- Regional Infrastructure Team Daily System Checks Regions 1 to 4

In a sub-folder labeled Examples - HL7 Interface Documents and Resource Emails, application-specific documents and email-threads have been posted to be emulated by software developers for different applications, which provide direction for the particular purposes for which they were written:

- Create a client interface for MAG; or
- Create a client interface for HT.

These could be used by a developer to develop a checklist of things to include in their own application.

7.8.4. Contact

The HL7 Messaging Repository (previously named the Messaging Administration Repository Maintenance (MARM)) is located on SharePoint at HL7 Messaging Repository - Home (sharepoint.com). If any form of messaging is affected, an email message must be sent to the HL7 Message Administrator at OIT DSO SPM Health Services - Messaging Administration VAOITPDADCTA_MSGADM@va.gov mail group, which is responsible for reviewing and approving HL7 Messaging profiles using the Messaging Workbench (MWB) application.

7.9. Veterans Data Integration and Federation – Enterprise Platform (VDIF-EP)

This section describes the Veterans Data Integration and Federation – Enterprise Platform (VDIF-EP), with emphasis on its interrelationships with VistA applications such as Virtual Patient Record (VPR).

7.9.1. Introduction

Veterans Data Integration and Federation – Enterprise Platform (VDIF-EP) is a framework that enables a unified patient-centric view of veterans' data across the enterprise and does so in a manner that is horizontally scalable. It consists of several components, as follows:

- **InterSystems HealthShare:** A commercial product that supports sharing patient data across enterprises.
- **InterSystems HealthConnect:** The component of HealthShare that interacts directly with VistA.
- **Virtual Patient Record (VPR):** VPR is a VistA application that detects updates to the patient record and formats the relevant patient data in an InterSystems proprietary Extensible Markup Language (XML)-based format known as Summary Data Architecture (SDA) and makes it available to be "picked up" by HealthConnect through a mechanism known as Enterprise Cache Protocol (ECP) and integrated into the federated record.
- **Initial Patient Load (IPL) and Call to Populate (CTP) applications:** These are HealthShare applications that provide the initial load to HealthShare and updates to existing records when new mapped fields are added, respectively.
- **Simple Object Access Protocol (SOAP):** SOAP is a protocol based on XML to implement web services that follow an object oriented model. It is used by VDIF Web Service Layer (VWSL) to implement web services that query VistA directly. **FileMan to Class (FM2Class) utility:** Several reference tables are populated using this utility in order to maintain the stable non-patient-centric data needed for the proper functioning of VDIF.

7.9.2. Processes

Of these components, VPR is most thoroughly integrated into VistA, and requires project teams to play an active role by identifying data elements that need to be shared with VDIF and requesting that they be mapped to SDA. The process is essentially as follows:

1. New data elements (files and fields) are identified as needing to be integrated into VDIF.
2. The project team requests through the (currently evolving) intake process that these elements be mapped to the corresponding fields in either one of the thirty (30) SDA Containers or their corresponding extension elements (needed for VA-specific data elements, such as period of service).
3. The VPR team creates mappings (mappings which may not be one-to-one, and which may require transformations) using the FileMan ENTITY (#1.5) file. The VistA data elements then need to be associated with protocols that fire when those elements are updated, or with custom cross-references, which invoke VPR APIs to stage the data.
4. Updates to protocols or additional cross-references are released using patches to the relevant VistA applications. New mappings added to the ENTITY file (as well as any other changes to VPR code) are released via a VPR patch. VDIF needs to be modified to expect and handle these new data elements, which is accomplished through a new release of VDIF. New releases of VDIF and VPR patches normally occur in tandem.

7.9.3. References

The following VPR-related references are available in the Virtual Patient Record (VPR):

- Virtual Patient Record (VPR) Developer's Guide
- Virtual Patient Record (VPR) Technical Manual

Additional references include the following:

- Health Middleware Data Management (HMDM) Sub -Product Line
- InterSystems HealthShare

7.9.4. Contact:

For more information on VDIF, please contact the VDIF VPR Team at VISTA-VPRTeam@va.gov.

7.10. Kernel Security

This section provides information on Kernel Security.

7.10.1. Introduction

VistA Kernel is the intermediary layer between the host operating system and other VistA software applications to ensure VistA software can coexist in a standard operating-system-independent computing environment. Kernel provides a standard and consistent user and developer interface between software applications and the underlying M implementation. Kernel adds user identity and permissions information to this layer after the user is provisioned and authenticated.

7.10.2. Processes

VistA Kernel Security is focused on processes complying with Executive Order 14028: Improving the Nation's Cybersecurity when accessing VistA; as well as ensuring the VistA security boundary is upheld by all entities by utilizing established processes.

VistA Kernel Security has evolved over the years, and it has several components with various names and documented in different products. To better understand and describe the latest evolution in Security implementations in VistA, the Kernel Security Section contains a short description of the existing components, products, and their corresponding names and documents. The security aspects of this documentation will be mainly those in the category of User Identity Provisioning, User Authentication and User Authorization.

- **User Provisioning:** Creating user access accounts and assigning privileges or entitlements within the scope of a defined process or interaction; provide users with access rights to applications and other resources which may be available in an environment, may include the creation, modification, deletion, suspension, or restoration of a defined set of privileges. Source: FICAM Roadmap
- **User Authentication:** The process of establishing confidence in the identity of users or information systems. Source: NIST SP800-63-2
- **User Authorization:** Access privileges granted to a user, program, or process or the act of granting those privileges. Source: CNSS Instruction No. 4009

7.10.3. References

The following references are available on SharePoint in the VistA Kernel Security folder:

- VistA Kernel Security
- RPC Broker Technical Manual
- RPC Broker User Guide
- OIT-ITOPS-SOP Service Account SOP
- VistALink System Management Guide v1.6
- Kernel Authentication and Authorization for J2EE (KAAJEE) v1.2.0 Deployment Guide
- Kernel 8.0 & Kernel Toolkit 7.3 Technical Manual

Additional references related to this section include the following:

- Remote Procedure Call (RPC) Broker
- VistALink (XOBV)
- VistA Kernel
- Standards and Conventions Work Group SharePoint site
  - M Programming Standards and Conventions SAC (Available in the Documents section of the SAC SharePoint site)
- M Programming Standards and Conventions SAC Document (Available in the VA Technical Reference Model (TRM))
- IAM PIV Compliance
- Executive Order 14028: Improving the Nation's Cybersecurity

- Federal ICAM Architecture Introduction (idmanagement.gov)
- NIST SP800-63-3 Digital Identity Guidelines
- CNSS Instruction No 4009 Committee on National Security Systems (CNSS) Glossary

7.10.4. Contact

For more information on Kernel Security, please contact the VistA Process Governance Workgroup at VISTAProcessGovernanceWorkgroup@va.gov.

7.11. VistA National Patch Release Requirements

This section provides information on VistA National Patch Release Requirements.

7.11.1. Introduction

The purpose of the VistA National Patch Release Requirements information in this guide is to call attention to the importance of following and completing all the steps in the VistA patch release process. The VistA National Patch Module Guide (NPMG) is the authoritative source and provides the necessary information to initiate, develop, create, and release patches to VistA products. VistA patch products consists of both MUMPS and non-MUMPS software code affecting systems inside and outside of the VistA authorization boundary; therefore, collaboration is essential to provide support to all consumers of VistA software.

Product staff who contribute to the release of a VistA patch are comprised of both VA and contractor personnel assigned to various organizational elements. VistA patch releases are managed as national releases; a standard change management process is currently under development in coordination with Enterprise Change Management. To ensure security requirements are met, product staff is responsible for the proper execution of key tasks and responsibilities within the VistA patch release process.

7.11.2. Processes

The VistA patch release process is assessed by the Office of Inspector General (OIG) on an annual basis under the lens of the NIST Special Publication 800-53, revision 4. The primary security control evaluated is Configuration Management with a specific focus on Baseline Configurations and Change Control, Access Restrictions for Change, Security Impact Analysis, and Information System Component inventory. The OIG team reviews the practices by Product Staff to confirm the enforcement of physical and logical changes within VistA patches are approved, while inspecting an inventory of documentation associated with the release of VistA patches. The aim of this document is to eliminate the findings levied by security assessment teams when inspecting the VistA Change and Configuration Management process.

7.11.3. VistA Office Change Control Board (VOCCB)

The VOCCB reviews all VistA patches to determine whether a patch might have an impact on the VistA/Cerner Millennium environment at Transition Sites undergoing Electronic Health Record Modernization (EHRM) transition, and at Converted Sites that have completed EHRM transition. The VOCCB decides whether a patch should be installed and tested by Independent Verification & Validation (IV&V) and whether the patch is approved to be installed in the

Production environment at Transition and Converted Sites. The VOCCB VistA patch review process is in addition to, in parallel with, and synchronized with existing VIP VistA patch development, testing, and release life cycle and schedule. The VOCCB does not review VistA patches for general release, but only for installation at EHRM sites.

- **VistA Office (VO) Change Control Board (VOCCB) Submission:** The VOCCB recommends that the VistA Patch Development Project Manager (PM) submit the patch to the VOCCB for review at the beginning of IOC Production Testing (including Informational VistA patches). This is the link to the PowerApps dashboard containing the VOCCB Patch Decision (VPD) Form.

7.11.4. References

The following references are available on SharePoint in the National Patch Release Requirements folder:

- Deployment Installation Backout Rollback Template
- HISM SPM Agreement Memorandum
- IOC Site Memorandum of Understanding Template
- PLM Testing Waiver Request
- Technical Manual Template
- User Guide Template
- VistA Verifier Account Table
- VistA Network File Share (NFS) Guide
- VistA Patch Process RACI
- VistA Primary Developer Checklist Guide
- VistA Secondary Developer Review Checklist Guide
- VistA Verifier Account Maintenance Guide
- VistA Verifier Checklist
- VistA National Patch Installation Checklist Guide
- VistA National Patch Module Guide
- VistA Patch Template with Instructions Host File
- VistA Patch Template with Instructions Packman

7.11.5. Contact

For more information on VistA National Patch Release Requirements, please contact the VistA Process Governance Workgroup at VISTAProcessGovernanceWorkgroup@va.gov.

7.12. VistA System Security Assessments

This section provides information on VistA System Security Assessments.

7.12.1. Introduction

The purpose of the 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 NIST Security Standards, Risk Management Framework, and security controls are the practical steps used to secure and defend the authorization boundaries of the VistA systems.

Each year, VistA undergoes 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, and Authority-to-Connect, along with independent security and privacy control assessments and validations. One of the tenets of the Risk Management Framework is applying continuous monitoring practices to a system. Strong continuous monitoring practices create an assurance that information security practices such as administrative, technical, and non-technical security controls are in balance. The elimination of threats and vulnerabilities protects the confidentiality, integrity, and availability of an information system. This section reminds all members who read this guide of their responsibility in securing and protecting VistA.

7.12.2. Processes

VistA is maintained in the VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) environment. VistA is comprised of virtual servers, RedHat Linux Operating System, InterSystems IRIS, the VistA database application, and over 100 M code-based application modules. Each package is comprised of multiple software programs that include administrative and clinical data. Access to the system is controlled by set of menus and security keys, which are determined prior to the initial issuance of access codes to users within the organization.

Managing and securing the components comprising of VistA is a daunting task. Utilizing the Continuance Monitoring step from the Risk Management Framework, the Information System Owner can direct the Information Assurance Team to execute organizational security policies to secure the VistA system.

The VistA Information Assurance Team prepares the VistA team to undergo the following assessments at any time:

- Authority to Operate
- Office of the Inspector General
- Authority to Connect
- Security and Privacy Control Assessment

7.12.3. References

For details regarding Continuous Monitoring Procedures, refer to the VistA System Security Assessments document available on SharePoint in the System Security Assessment folder.

7.12.4. Contact

For more information on VistA System Security Assessments, please contact the VistA Process Governance Workgroup at VISTAProcessGovernanceWorkgroup@va.gov.

8. Glossary

Refer to Table 8-1.

Table 8-1: Glossary

Term	Definition
Class 1 or Class I Software	In accordance with VA Directive 6402: Nationally released OIT DevSecOps SPM VistA software includes all interfaces installed on or interacting with VA computing environments. National Software has been created by or evaluated and certified by DevSecOps to comply with VA established criteria listed below. (1) Architecture and technology (2) Capacity and performance (3) Coding standards (4) Documentation (5) Interagency agreements (6) Name spacing and interface control agreements (7) Network capacity impacts (8) OIT Technical Reference Model (TRM) (9) Privacy and confidentiality (10) Section 508 accessibility (11) Security (12) Testing
Class 2 or Class II Software	In accordance with VA Directive 6402: Represents a Class III product that has been verified as compliant with established standards. These are products coming out of field development (FD) and are certified and approved for Class II deployment and follow-on support by FD.
Class 3 or Class III Software	In accordance with VA Directive 6402: Products originating from any unrelated OIT DevSecOps SPM source including field developers, non-Information Technology (IT) VA staff (e.g., physicians), vendors, open source, research, or educational organizations located on a VAMC specific VistA instance. These software products generally have a limited and non-standardized distribution across VA systems and are not covered by OIT DevSecOps SPM support commitments.
VistA Authorization Boundary	The VistA Authorization Boundary reflects the portion of VistA that the VistA Information System Owner is responsible for maintaining Authority to Operate (ATO) on the VA network.

9. Additional References

Additional references include the following:

- VistA Reference Guide SharePoint Site
- VistA Cloud Migration
- VistA Cerner Migration Schedule | ServiceNow (va.gov)
- OIT PAL Master Glossary
- Process Asset Library (PAL)
- VA Acronym Lookup
- VistA Monograph
- VA Software Document Library (VDL)
- VDL Service Management
- VA System Inventory (VASI)
- VistA Dashboard - Power BI (powerbigov.us)
- Software Product Management (SPM) Health Intake Training
- VistA Monograph – New Item Form Entry
- VASI Registration Form – VA | Enterprise Architecture
- VistA Office - VDL Service Request Form

10. VistA Process Governance Workgroup

To contact members of the VistA Process Governance Workgroup (VPGW), please use the email address VISTAProcessGovernanceWorkgroup@va.gov.