Department of Veterans Affairs Technical Reference Model and Standards Profile

January 2007

Version 4.2

Table of Content

1 Introduction 5

1.1 Background 5

1.2 Purpose 5

1.3 Audience 5

1.4 Discussion of the TRMSP Graphic 5

1.4.1 Distributed Applications and Data 6
1.4.2 Corporate and Regional Data Processing with COOP 7
1.4.3 Cyber Security 7
1.4.4 Telecommunications 7

1.5 Scope 7

1.6 Overview of the TRMSP Process 7

1.7 Definitions 8

1.7.1 Service Description 8
1.7.2 Goals 8
1.7.3 Rules 8
1.7.4 Guidelines 9
1.7.5 Standards 9

2 Distributed Applications and Data (DA&D) 10

2.1 Client Tier 10

2.1.1 Common Presentation Services 11
2.1.2 GUI Client Services 12
2.1.3 Mobile Client Services 13
2.1.4 Web Client-Side Services 13

2.2 Middle Tier 14

2.2.1 Web Server-Side Services 15
2.2.2 Component Services 18
2.2.3 Access Services 19

2.3 Data Tier 27

2.3.1 Enterprise & Local Data Services 27
2.3.2 Warehouse Services 28
2.3.3 Legacy Application Services 28
2.3.4 Meta Data Services 30
2.3.5 Common Reference Services 34

3 Corporate and Regional Data Processing with COOP 39

3.1 Operating System Services 40

3.1.1 Desktop Operating Systems 40
3.1.2 Server Operating Systems 41

3.2 Middleware 41

3.2.1 J2EE Application Services 42
3.2.2 Message-Oriented Middleware 44
3.2.3 eCommerce 44
3.2.4 Internet Services 45
3.2.5 Multimedia Services 49

3.2.6 Search Engines 50
3.2.7 Portal 50
3.2.8 Discovery Services 51

3.3 Storage 52
3.3.1 Database Server 53
3.3.2 Enterprise Storage 54

4 Cyber Security 56

4.1 Availability 57
4.1.1 Backup 57
4.1.2 Uninterruptible Power Supply 58

4.2 Confidentiality 58
4.2.1 Credentialing & Privileging (Cyber Access) 59
4.2.2 Access Control 60
4.2.3 Encryption 61
4.2.4 VPN 63
4.2.5 Data Integrity 63
4.2.6 Checksum, Hash Value 64
4.2.7 Digital Signature 65
4.2.8 Identification & Authentication 65
4.2.9 Public Key Infrastructure 67
4.2.10 Biometrics 69
4.2.11 Passwords 70
4.2.12 Single Sign On (SSO) 71
4.2.13 Security Token 71

4.3 Security Controls 72
4.3.1 Secure Code Design 72
4.3.2 Boundary Protection 72
4.3.3 Firewalling 73
4.3.4 Unsolicited E-mail 75
4.3.5 Audit 76

4.4 Certification & Accreditation (C&A) 77

4.5 Privacy 78
4.5.1 Privacy Policy & Procedures 79
4.5.2 Privacy Enhancing Technologies 81

5 Telecommunications 83

5.1 Multimedia Transport 83

5.2 Network Management Services 85
5.2.1 Fault Management 86
5.2.2 Performance Management 87
5.2.3 Configuration Management 88
5.2.4 Accounting Management 90
5.2.5 Radio Frequency Management 91

5.3 Network and Connectivity Services 92
5.3.1 Wide Area Network (WAN) Services 92
5.3.2 Metropolitan Area Network (MAN) Services 93
5.3.3 Campus Area Network (CAN) Services 94
5.3.4 Local Area Network (LAN) Services 96
5.3.5 Cable Plant 98
5.3.6 IP Routing Services 99

5.3.7 Network Protocols 101
5.3.8 Domain Name Service (DNS) 102
5.3.9 Remote Access (VPN, PPP) 103
5.3.10 IPv6 Stack Design 104

6 Appendix - Patterns 110

6.1 Wide Area Network 110

6.2 Local Area Network 111
6.2.1 Access Layer 112
6.2.2 Distribution Layer 112
6.2.3 Core Layer 112

6.3 Campus Area Network 112
6.3.1 Access Layer 113
6.3.2 Distribution Layer 113
6.3.3 Core Layer 113

6.4 Wireless LAN Architecture Pattern 113

6.5 Internet/Intranet Gateway (firewall, DMZ, VPN) 114

6.6 Java Application Architectures 115
6.6.1 Client Tier 116
6.6.2 Middle Tier 119
6.6.3 Data Tier 121

6.7 Messaging Consolidation 124

6.8 Enterprise Telephony Agenda 126

6.9 Wideband to Narrowband Radio Frequency Transition 128

7 Appendix - Management & Planning Processes 130

7.1 System Development Life Cycle 131
7.1.1 Introduction 131
7.1.2 Infrastructure Augmentation 132
7.1.3 COTS/GOTS Implementation 139
7.1.4 Small Custom Software Development – Waterfall 149
7.1.5 Medium and Large Custom Software Development – Rational Unified Process 151

7.2 Configuration Management 155
7.2.1 Source Code Management 158
7.2.2 Hardware Management 159
7.2.3 License Management and Electronic Software Distribution 160
7.2.4 Requirements Management 161
7.2.5 Content Management 162

7.3 Capacity Management and Capacity Planning 163

7.4 Deployment Planning 165

7.5 Workflow/Event Management (EAI) 166

List of Figures

Figure 1 - TRMSP 6
Figure 2 - DA&D Overview 10
Figure 3 - J2EE Standard Enterprise Services 43
Figure 4 - Storage 52
Figure 5 - IPv6 address example 104
Figure 6 - IPv6 Header Structure 105
Figure 7 - IPv4 to IPv6 Header Comparison 106
Figure 8 - “To Be” Physical Architecture 111
Figure 9 - LAN – Pattern 111
Figure 10 – CAN - Pattern 112
Figure 11 - Wireless LAN Pattern 113
Figure 12 - Tier 1 Gateways and Security Zones Target Architecture 115
Figure 13 - Java Application Architecture 115
Figure 14 - VA Messaging Consolidation Conceptual Design (Phase One) 125
Figure 15 - Consolidation of Messaging Services to Six RDPCs (Phase Two) 126
Figure 16 - PBX To-Be 127
Figure 17 - Wideband Channel 128
Figure 18 - Narrowband Channels 129

List of Tables

Table 1 - Infrastructure Augmentation SDLC 137
Table 2 - Infrastructure Augmentation Milestone Deliverable Summary 139
Table 3 - COTS/GOTS Implementation SDLC 146
Table 4 - COTS/GOTS Implementation Milestone Deliverable Summary 149
Table 5 - Waterfall Milestone Deliverable Summary 151
Table 6 - RUP Milestone Deliverable Summary 155

1 Introduction

The Department of Veterans Affairs (VA) Technical Reference Model and Standards Profile (TRMSP) provides a framework description and design guidance for approved and proposed technology within the VA Enterprise Architecture (EA). The TRMSP uses a common vocabulary to describe selected technical services to be used by developers and implementers of technology to support business functions of the VA enterprise. Moreover, the TRMSP serves as a roadmap and tool for technology support of the VA EA. The VA TRMSP is a collaborative product of the VA information technology (IT) and business communities, developed within the VA EA process. Information contained in the Appendixes at the end of this document should be considered "work in progress" and subject to review, modification, and/or approval by the respective subject mater community. Upon final approval, the information will be moved from the appendix into the main body of the TRMSP.

1.1 Background

The Clinger-Cohen Act of 1996 (Public Law 104-106) assigns the Chief Information Officer (CIO) the responsibility to develop, maintain, and facilitate the implementation of an IT (or enterprise) architecture. The TRMSP is recognized as an integral component of the enterprise. The Office of Management and Budget (OMB), as part of the Federal Information Technology Architecture (OMB M-97-16) and OMB Circular A-130, also requires the TRMSP.

1.2 Purpose

The TRMSP supports the priorities, goals, and strategies documented in the One-VA EA. The primary purpose of the TRMSP is to define the necessary and approved IT rules, guidelines, standards, and design patterns for use in the Department of Veterans Affairs that will contribute toward the achievement of One-VA architectural goals. A secondary purpose of the TRMSP is to encourage understanding and communication of the means to accomplish EA goals, such as cross-functional integration and consistency of implementation.

1.3 Audience

The VA TRMSP is intended to form a knowledge base from which key TRMSP clients, such as architects, project managers, procurement officials, reviewers, and contractors, can obtain useful information about the services, rules, guidelines, standards, and patterns that are approved for use at VA.

1.4 Discussion of the TRMSP Graphic

The TRMSP is based on the VA EA Logical Model and is one component of the EA. The Technical Reference Model (TRM) provides the framework for integrating an organization's technical infrastructure in support of the EA. The TRM describes:

- The major components of the technical infrastructure
- A taxonomy of technical services used by the components in the infrastructure
- A common vocabulary to describe the technical services

An organization may rely on certain technical services more than others and may not use some services at all.

The Standards Profile (SP) defines the set of IT standards that support the services listed in the TRM.

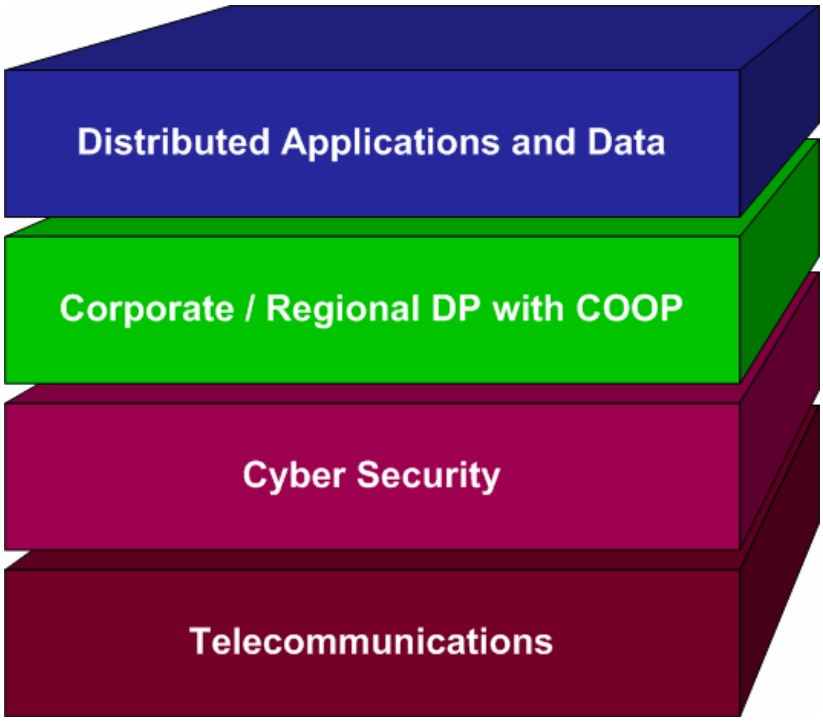

Figure 1 - TRMSP

The TRMSP identifies and describes the technical services to be used throughout the Department. Secondly, it defines the set of IT rules, guidelines, and standards that support the technical services.

The diagram shown in *Figure 1 - TRMSP* is comprised of four horizontal layers that encompass the full range of technologies, services, and functions contained within the EA. These layers serve as a convenient mechanism to form taxonomy for describing the technologies and services within the TRM. Each of the layers is described in greater detail below.

The top layer horizontal, the DA&D layer, provide the application and data services that support most VA functions, such as R&E and CM. Next, the CRDP/COOP layer is responsible for enterprise-wide data management issues, such as backups and continuity of operations. Moving downward on the cube, the Cyber Security Layer is next, whose function is to manage and enforce security constraints across the enterprise, including enforcement of privacy. The bottom layer, Telecommunications, serves to form the communications backbone for the enterprise.

The following sections provide a more detailed description of the four horizontal layers, which are the technical services of the VA TRMSP.

1.4.1 Distributed Applications and Data

The Distributed Applications and Data (DA&D) layer of the One-VA target architecture is a multi-tiered, technical architecture. These technologies support a services-based, component architecture used to expose the enterprise's functionality to both internal and external systems.

1.4.2 Corporate and Regional Data Processing with COOP

A robust corporate and regional data center infrastructure will provide the production environment for the applications layer; thus it is key to achieving the target One-VA EA and meeting strategic objectives across the Department. The CRDP/COOP layer provides close support for the DA&D Layer. Middleware, operating systems, and storage are essential components of the corporate services available to all distributed applications and data. Without the services in CRDP/COOP, DA&D would lack coherence and interoperability; and may cease to be effective as enterprise assets.

1.4.3 Cyber Security

Cyber Security consists of technologies, policies, and procedures designed to ensure the confidentiality, integrity, and availability of all electronic data assets.

VA's Cyber Security is designed to assure the veteran, their family, and VA employees that their data collected, stored, processed, and transmitted in the performance of VA business is secure.

1.4.4 Telecommunications

A robust, high performance, cost effective, and assured telecommunications infrastructure is key to achieving the target One-VA EA and meeting strategic objectives across the Department. The strategically most significant, near term element of Telecommunications Modernization Project (TMP) is an integrated, high performance, low cost, assured wide area data network as infrastructure for other integration and convergence efforts. Because it is the near term most significant effort, the target or "To Be" network architecture has focused on data communications. However, this is not to imply an exclusive focus on a data network. As this integrated network infrastructure evolves, it would be natural to expand capability to include a converged set of voice and video services. For example, toll bypass may route long distance telephone calls that both originate and terminate within the Department over the wide area network (WAN) as an alternative to commercial long distance.

1.5 Scope

The VA TRMSP applies to all VA information systems, infrastructures, and software applications at all VA organizational levels and environments. The scope of the VA TRMSP is sufficiently broad to assist in addressing a wide range of system configurations. Architects, project managers, reviewers, developers, and contractors are required to adhere to the approved rules, guidelines, and standards established in the TRMSP when proposing and developing IT initiatives within VA. No project will be approved that does not meet VA standards or for which there is no signed waiver for standards in place. The TRMSP does not attempt to prescribe a specific brand name product or application for use throughout the VA enterprise. In the few cases where a specific product is named, it was approved by the VA CTO.

1.6 Overview of the TRMSP Process

Any interested party may submit proposed changes to the EA Chief Architect, for review and for adoption. A project sponsor may request a waiver from the Director, Enterprise Architecture Service to applicable standards and rules. This waiver request must contain compelling business and technical justifications.

The Enterprise Architecture Management maintains the TRMSP. The TRMSP is formally reviewed in conjunction with a semi-annual independent industry technical assessment and a semi-annual business requirement review. These reviews are evaluated by the Enterprise Architecture Council (EAC), and are considered and adopted by the Information Technology Board (ITB). Changes are then published on the Intranet and in hardcopy versions of the TRMSP document.

1.7 Definitions

The following definitions are used in this document. If there is no rule, guideline, or standard identified as appropriate for VA use, then the term "None" will appear. If the term "TBD" (To Be Determined) appears, this indicates that research is being conducted to determine what is appropriate for VA use and will be provided in a later TRMSP release.

1.7.1 Service Description

A service description is a short, concise discussion of the service area in generic terms to help readers gain an understanding of the service. Service descriptions will be followed by applicable goals, rules, guidelines, and standards.

1.7.2 Goals

The goals will enable the Department to address cross-cutting opportunities and continue to make strides towards achieving the concept of "One VA." The seven EA goals addressed in the TRMSP are:

- IT Goal 1: Implement One-VA Enterprise Architecture.
- IT Goal 2: Implement a One-VA data network.
- IT Goal 3: Secure the One-VA enterprise against Cyber Attack.
- IT Goal 4: Establish a disciplined, non-bureaucratic project management structure.
- IT Goal 5: Establish effective metrics to measure performance.
- IT Goal 6: Implement an effective Command and Control, COOP, and COG infrastructure.
- IT Goal 7: Shape the VA IT workforce to support the target One-VA EA.
- IT Goal 8: Transform VA from line of business centric service delivery to veteran centric service delivery.

1.7.3 Rules

A rule is a statement about a mandatory characteristic of an EA component or service. Rules are developed by VA to achieve EA goals. Adherence to a rule is required with no deviation. Rules may refer to how a specific proprietary product is used if that product has become standardized in VA. The rules should address the key TRMSP clients, users, or customers, which are at a minimum: project managers, system developers, procurement officials, contractors, architects, and reviewers.

Note: Generally all VA Directives and Handbooks can be referenced at http://www.va.gov/pubs/asp/edsdirec.asp

1.7.4 Guidelines

A guideline is a "best practice" policy statement or procedure that should be followed, but it is not mandatory and does not require a waiver if it is not followed. It is an optional means to achieve an EA goal. Guidelines should usually be discussed in terms of a technology rather than a product. Guidelines may also discuss the avoidance of a particular technology.

1.7.5 Standards

Unlike rules, which are developed by VA, bodies outside of VA promulgate standards, typically by national or international standards organizations such as, ANSI, ISO, and IETF. The Standards section lists standards that have been determined as appropriate for VA and are mandatory. The Standards section contains the name, title, or number of the standard and the URL of the standard, where more detailed information can be obtained. The technologies providing the indicated services shall comply with the standards listed. The TRMSP chooses from this range of "voluntary industry standards" (as defined in the National Technology Transfer and Advancement Act) to meet VA's goals.

2 Distributed Applications and Data (DA&D)

The following section outlines the technical services provided by the distributed applications and data (DA&D) layer of the One-VA target architecture. As depicted in *Figure 2 - DA&D Overview* the services are organized into a physical multi-tiered, technical architecture that is used to expose the enterprise's functionality to both internal and external systems. Also, the services taken in isolation provide no end-user business functionality, instead they are the building blocks used to create business solutions. Finally, they are aligned with the E-Gov Enterprise Architecture Guidance (Common Reference Model) issued on July 25, 2002 by the FEAPMO.

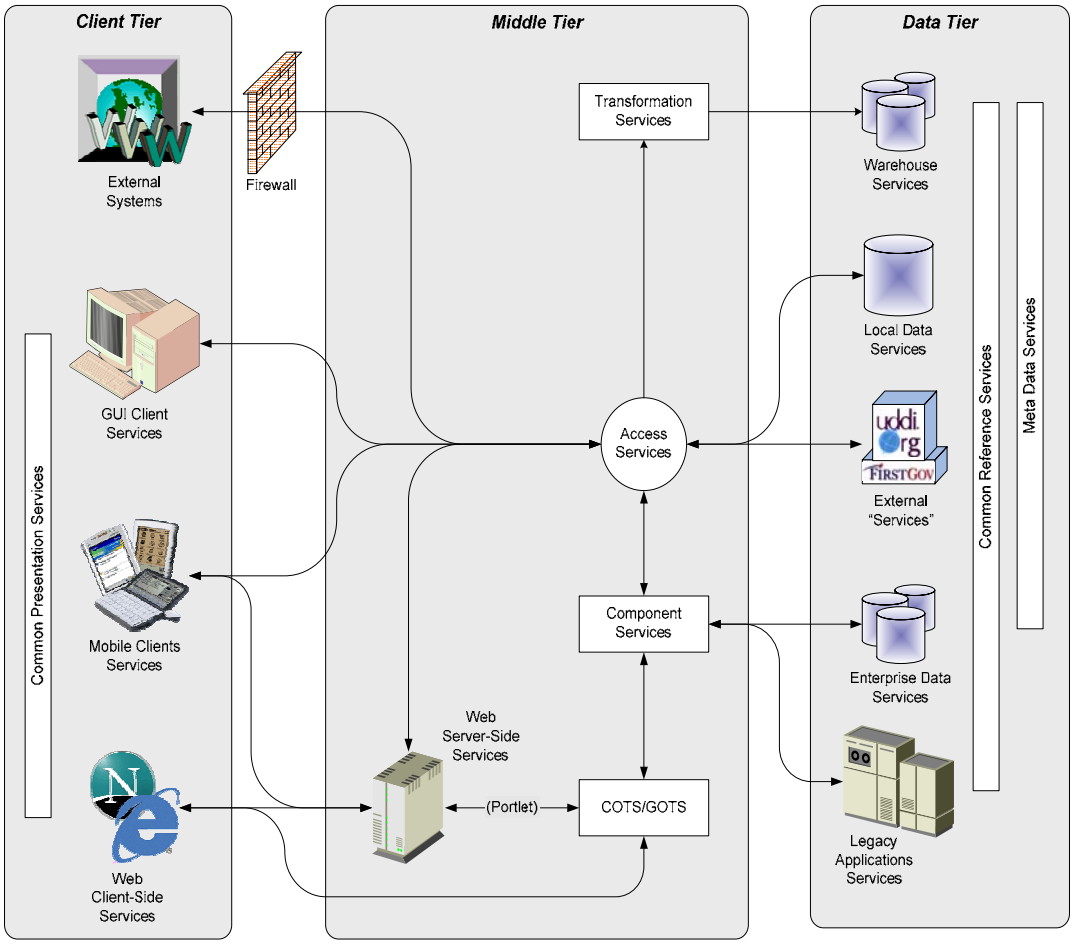

Figure 2 - DA&D Overview

2.1 Client Tier

The Client Tier is the logical layer in a distributed system that typically presents data to and captures input from the user. Usually, this tier requests data based on input using a local area network (LAN)/WAN from a server, and then formats and displays the result.

This section is structured around the three major presentation platforms: GUI applications (heavyweight clients), browser-based applications (lightweight clients), and mobile clients. Additionally, the services that are shared by all presentation modes are consolidated under the common presentation services. However, in *Figure 2 - DA&D Overview*, External Systems are

depicted in this tier as a placeholder. These are applications that are outside of the VA's domain, but require information from the enterprise; so, they act as a "client" to the enterprise. But, there are no technical services directly supporting them since their implementation is outside of the VA's domain. Regardless of their implementation, the external systems are expected to interact with the enterprise though the VA's standard access services for their information.

Goals

IT Goal 1: Implement One-VA Enterprise Architecture.

- These services are based on industry-accepted standards that are compliant with FEAPMO guidelines thereby allowing VA to participate in E-GOV initiative with a unified front.

IT Goal 2: Implement a One-VA data network.

- These technologies are based on open, industry standards communications protocols thereby eliminating the need for proprietary networking hardware or software.

IT Goal 3: Secure the One-VA enterprise against Cyber Attack.

- These technologies can support a unified authentication and authorization service thereby enabling Cyber Security's Single Sign On (SSO) and Access Control functions.

IT Goal 7: Shape the VA IT workforce to support the target One-VA EA.

- These technologies can be used to consolidate user interfaces for stovepipe applications into a consolidated view thereby reducing user training.
- These technologies are based on industry best practices and open standards thereby providing many training sources for the workforce.

2.1.1 Common Presentation Services

Common Presentation services allow end-users to interact with an application by converting and displaying application data into a human-legible form. Generically, these services are referred to as the User Interface (UI) and are commonly comprised of navigation, display, and data collection components.

Rules

- VA Directive 6300 Records & Information Management
- VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act
- VA Handbook 6300.5, Procedures for Establishing & Managing Privacy Act Systems of Records
- VA Directive 6221 Accessible Technology

Guidelines

- World Wide Web Consortium (W3C); User Agent Accessibility Guidelines 1.0; reference at http://www.w3.org/TR/xag

Standards

- Section 508 - Architectural and Transportation Barriers Compliance Board; Section 508 Standards (36 CFR Part 1194); reference at http://www.access-board.gov/sec508/508standards.pdf

2.1.2 GUI Client Services

GUI Client services are a sub-class of the Common Presentation Services and are distinguished by their need for a highly interactive user experience, dynamically generated graphics (typically graphs and charts), or locally processed data; thereby, making them a heavyweight client. Additionally, these services are tight coupled to the native desktop operating system, which is permanently connected to the enterprise network.

Note: In addition to the rules, guidelines, and standards listed below, GUI Client services inherit all of the Common Presentation Services' rules, guidelines, and standards.

Rules

- Choose the development standards, as indicated below, that most closely align with the application's targeted native desktop operating system.

Guidelines

- UI development should be platform independent; therefore, the preferred approach is to use Web Client-Side Services unless their interactive capabilities are too restrictive for a particular application.
- J2SE Swing components are preferred over AWT components because of both their expanded capabilities (more widgets) and consistent behavior across different operating systems.

Standards

When developing for Unix-based devices or cross-platform environments:

- J2SE APIs (all packages) – Sun Microsystems; Java 2 Platform Standard Edition 5.0 API Specification; reference at http://java.sun.com/j2se/1.5.0/docs/api/
- J2EE APIs (JDBC) - Sun Microsystems; Java 2 Platform, Enterprise Edition, v3.0, API Specification; reference at http://java.sun.com/products/jdbc/download.html#corespec30
- Java Language - Sun Microsystems; The Java Language Specification, Second Edition; reference at http://java.sun.com/docs/books/jls/
- JVM – Sun Microsystems; The Java Virtual Machine Specification, Second Edition; reference at http://java.sun.com/docs/books/vmspec/index.html

Note: JDBC is not part of J2SE v5.0, which causes portions of the J2EE specification to be in the client tier.

When developing for Windows-based environments:

- C# Language - European Computer Manufacturers Association (ECMA); C# Language Specification, 3rd edition (June 2005) - Standard ECMA-334; reference at http://www.ecma-international.org/publications/standards/Ecma-334.htm
- CLI - European Computer Manufacturers Association (ECMA); Common Language Infrastructure (CLI), 3rd edition (June 2005) - Standard ECMA-335; reference at http://www.ecma-international.org/publications/standards/Ecma-335.htm

2.1.3 Mobile Client Services

Mobile Client services are a sub-class of the Common Presentation Services and are distinguished by their native Personal Digital Assistant (PDA) host environment, which implies a small UI display, sporadic connectivity, and low bandwidth.

Note: In addition to rules, guidelines, and standards listed below, Mobile Client services inherit all of the Common Presentation Services' rules, guidelines, and standards.

Rules

1) VA Directive 6212 Security of External Electronic Connections

Guidelines

- Similar to GUI Client Services, UIs should be platform independent; therefore, the preferred approach to UIs on mobile devices is to use Web Client-Services via (micro) browsers.

Standards

- IEEE 1073 for medical devices; reference at http://www.ieee1073.org/standards/1073standards.html

2.1.4 Web Client-Side Services

Web Client-Side services are a sub-class of the Common Presentation Services and are distinguished by their web-browser hosted environment.

Note: In addition to rules, guidelines, and standards listed below, these services inherit all of the Common Presentation Services' rules, guidelines, and standards.

Rules

- OMB Memorandum 99-18 "Privacy Policies on Federal Web Sites" dated June 2, 1999; reference at http://www.whitehouse.gov/omb/memoranda/m99-18.html
- VA Directive 6102 Internet/Intranet Services
- VA Hand Book 6102 Internet/Intranet Services
- Any technologies that enable a Network Delivered Application (NDA) to access or modify resources of the local machine that are outside of the browser's "stand box" are strictly prohibited. Specifically, this prohibition includes signed-applets or untrusted ActiveX controls delivered through a browser's session.

Guidelines

- Look-n-Feel; Web Author Reference and Resource Center's Facelift Resources; reference at http://vaww.va.gov/facelift/Resources/facelift.htm
- The preferred language standards for developing these services are to use JavaScript for relatively simple interactions (i.e., forms validation, interactive menus, etc.) and Applets (J2SE APIs and Java Language) for complex network delivered applications.

Standards

- JavaScript - European Computer Manufacturers Association (ECMA); ECMAScript Language Specification, 3rd edition (December 1999) - Standard ECMA-262; reference at http://www.ecma-international.org/publications/standards/Ecma-262.htm
- J2SE APIs (Applet) – Sun Microsystems; Java 2 Platform Standard Edition 5.0 API Specification; reference at http://java.sun.com/j2se/1.5.0/docs/api/
- Java Language - Sun Microsystems; The Java Language Specification, Second Edition; reference at http://java.sun.com/docs/books/jls/

2.2 Middle Tier

The Middle Tier is the logical layer in a distributed system between the client and data tiers where business application logic is executed, typically running on a server over a LAN/WAN. This tier is a collection of business rules and functions that generate and operate on information. They accomplish this through business rules, which can change frequently, and are thus isolated from both the presentation and the data.

The section is structured around three major items: web standards, components standards, and transformation standards. Additionally, the items that facilitate inter- and intra-service communications are consolidated under the common access services.

Goals

IT Goal 1: Implement One-VA Enterprise Architecture.

- These technologies support a services based, component architecture thereby allowing common business functionality to be consolidated into a single technical implementation.
- These technologies are based on open interface standards that are compliant with FEAPMO guidelines thereby allowing VA to participate in E-GOV initiatives with a unified front.

IT Goal 2: Implement a One-VA data network.

- These technologies are based on open, industry standards communications protocols thereby eliminating the need for proprietary networking hardware or software.

IT Goal 6: Implement an effective Command and Control, COOP, and COG infrastructure.

- These technologies support a distributed, fault-tolerance application, thereby reducing the risk associated with a data center failure or a denial-of-service attack.

- These technologies support a strong transaction-processing model thereby eliminating the risk associated with non-isolated events.
- These technologies support an open interface standard recommended by the FEAPMO, thereby promoting interoperability with internal and external systems.

IT Goal 7: Shape the VA IT workforce to support the target One-VA EA.

- These technologies are based on industry best practices and open standards, thereby providing many training sources for the workforce.

2.2.1 Web Server-Side Services

Web Server-Side services bridge the gap between the web clients and the various levels of application logic running on a web server in either a secure or unsecured manner. They are classified into three categories ranging from low to high levels of complexity. Although categorized separately, these services all build on one another by extending its lower level services (i.e., data-oriented sites extend static-oriented sites and application-oriented sites extend data-oriented sites).

Static-Oriented

The simplest form of Web Server-Side services provides static content in response to a client's HTTP(S) GET request for a specific Uniform Resource Identifiers (URIs; a.k.a. URLs) and the site's contents are stored in a file-service's directory structure.

Rules

- None

Guidelines

- The preferred method of organizing files numbering over a few dozen is to have the directory structure mirror the major navigation of a site with graphics in a separate (images) subdirectory.
- When possible, use an externally linked, single style sheet (CSS) for an entire site to help enforce a consistent look-n-feel.

Standards

- URI/URL - Internet Engineering Task Force (IETF); Uniform Resource Identifiers (URI): Generic Syntax - RFC2396; reference at http://www.ietf.org/rfc/rfc2396.txt
- CSS - World Wide Web Consortium (W3C); Cascading Style Sheets, level 2; CSS2 Specification; W3C Recommendation 12-May-1998; reference at http://www.w3.org/TR/REC-CSS2/
- CSS Mobile - World Wide Web Consortium (W3C); CSS Mobile Profile 1.0; W3C Candidate Recommendation 25 July 2002; reference at http://www.w3.org/TR/css-mobile

Data-Oriented

These services build on the Static-Oriented services by providing the ability to interact with a data repository based on a client's HTTP(S) GET or POST request. Typically, these services are used to dynamically generate a site's content or to enter a user's non-transactional input into a database. However, the logic associated with this service should be limited to data validation, database retrieval SQL, or "gluing" component logic together.

Note: In addition to the rules, guidelines, and standards listed below, Data-Oriented services inherit all of the Static-Oriented rules, guidelines, and standards.

Rules

- Use the Java series of standards for developing these services due to its portability, scalability, and reliability. However, a script-based standard may be used for small-scale sites.

Guidelines

- Avoid putting processing logic directly in JSPs encapsulate it in either servlets or JavaBeans.

Standards

- Perl – The Perl Institute; Practical Extraction and Report Language.
- Java2 Servlets & JSPs – Sun Microsystems; Java Servlet API Specification ("Specification"), Version 2.3; reference at http://jcp.org/en/jsr/detail?id=53
- JavaBean - Sun Microsystems; JavaBeans™ API specification version 1.0; reference at http://java.sun.com/products/javabeans/glasgow/index.html
- Java Language - Sun Microsystems; The Java Language Specification, Second Edition; reference at http://java.sun.com/docs/books/jls/

Application-Oriented

These services build on the Data-Oriented services by providing the ability to process complex logic (including transactions) based on a client's HTTP(S) GET or POST request. Preferably, horizontal COTS products can be leveraged to supply the majority of the application logic. However, custom application can be written using the Component Services described later.

Note: In addition to rules, guidelines, and standards listed below, Application-Oriented services inherit all of the Data-Oriented rules, guidelines, and standards.

Rules

- Avoid using JavaBeans or servlets for transactional logic; alternatively migrate it into EJBs under Component Services.

Guidelines

- The preferred implementation of these services should follow the Model 2, Model-View-Controller (MVC) design pattern where the controller follows the servlet specification, the view follows the JSP or XSLT specification, and the model conforms to the JavaBean specification or a Component Services.

Standards

- XSLT - World Wide Web Consortium (W3C); XSL Transformations (XSLT) Version 2.0; W3C Candidate Recommendation 3 November 2005; reference at http://www.w3.org/TR/xslt20/
- XPath - World Wide Web Consortium (W3C); XML Path Language (XPath) 2.0, W3C Candidate Recommendation 3 November 2005; reference at http://www.w3.org/TR/xpath20/
- Portlet - Java Community Process; JSR 168 - Portlet Specification. Also see Portals Servers; reference at http://www.jcp.org/en/jsr/detail?id=168

Web Documents

Web documents are the basic units of transmission between the Web Client-Side Services and the Web Server-Side Services. They encapsulate the data to be rendered in a user's browser.

2.2.1.1 HyperText Markup Language (HTML)

HTML is a derivation of the Standard Generalized Markup Language (SGML) that includes a set of markup tags inserted in a file intended for display on a World Wide Web browser page. The markup tells the Web browser how to display a Web page's words and images for the user.

Rules

- None

Guidelines

- External Style sheets (CSS) are the preferred method for formatting HTML, followed by embedded CSSs, and lastly by embedded HTML formatting commands.

Standards

- HTML - World Wide Web Consortium (W3C); HTML 4.01 Specification; W3C Recommendation 24 December 1999; reference at http://www.w3.org/TR/html401/

Note: The W3C standard is cited because it's accessible without charge. However, the identical corresponding ISO standard is ISO/IEC 15445:2000/COR 1:2002.

2.2.1.2 Extensible Hypertext Markup Language (XHTML)

XHTML is a hybrid between HTML and XML specifically designed for WWW device displays. XHTML is a markup language written in XML; therefore, it is an XML application. XHTML uses three XML namespaces, which correspond to three HTML 4.0 DTDs: Strict, Transitional, and Frameset. When applied to WWW devices, XHTML must go through a modularization process. This enables XHTML pages to be read by many different platforms. A device designer, using standard building blocks, will specify which elements are supported. Content creators will then target these building blocks--or modules. Because these modules conform to certain standards, XHTML's extensibility ensures that layout and presentation stay true-to-form over any platform.

Rules

- None

Guidelines

- XHTML 1.0 Strict is the preferred namespace, which is used to achieve a clean structural mark-up, free of any tags associated with layout.

Standards

- XHTML - World Wide Web Consortium (W3C); XHTML 1.0 The Extensible HyperText Markup Language (Second Edition) A Reformulation of HTML 4 in XML 1.0; W3C Recommendation 26 January 2000, revised 1 August 2002; reference at http://www.w3.org/TR/html/

2.2.2 Component Services

Component services are the enablers of the component based architecture that encapsulates the business logic and expose a set of well-defined interfaces. The main purpose of creating components is reusability where the same component can be used in applications needing similar functionality. But even when a component is used only in a single application, the high degree of modularization given by the component architecture makes the following significantly easier: security, transaction processing, and scalability.

Enterprise JavaBean (EJB)

An enterprise bean is a server-side component that encapsulates the business logic of an application. The business logic is the code that fulfills the purpose of the application. You can think of an enterprise bean as a building block that can be used alone or with other enterprise beans to execute business logic on the J2EE server.

Rules

- None

Guidelines

- For EJBs needing 24/7-availability under COOP, the EJBs should be redundantly deployed across multiple data centers.
- Container Managed Persistence (CMP) is the preferred method for binding a component to a database service.

Standards

- EJB - Sun Microsystems; Enterprise JavaBeans™ Specification, Version 2.1; reference at http://java.sun.com/products/ejb/docs.html
- J2SE APIs (all packages) – Sun Microsystems; Java 2 Platform Standard Edition 5.0 API Specification; reference at http://java.sun.com/j2se/1.5.0/docs/api/
- J2EE APIs (All packages) - Sun Microsystems; Java 2 Platform Enterprise Edition, v 1.4; API Specification; reference at http://java.sun.com/j2ee/1.4/docs/api/index.html
- Java Language - Sun Microsystems; The Java Language Specification, Second Edition; reference at http://java.sun.com/docs/books/jls/

- JVM – Sun Microsystems; The Java Virtual Machine Specification, Second Edition; reference at http://java.sun.com/docs/books/vmspec/index.html

Naming/Location Services

These services support location transparency, where applications can lookup and dynamic binding to a component using directory services, which means that it does not care where the component is located. Therefore, an organization has the flexibility to move components to different machines and create redundancy (fault tolerance) without changing any source code.

Rules

- None

Guidelines

- None

Standards

- JNDI API – Sun Microsystems; Java Naming and Directory Interface Application Programming Interface (JNDI API), JNDI 1.2/JavaTM 2 Platform, Standard Edition, v 1.3, July 14, 1999; reference at http://java.sun.com/j2se/1.5/pdf/jndi.pdf

2.2.3 Access Services

These services facilitate programmatic communications between the various services or external entities. This service is divided into three types of access:

- **Transaction-oriented** – that itemizes inter-process communications ranging from low-level procedure calls to high-level business transactions.
- **Data-oriented** – that focuses exclusively on connectivity and querying the data services.
- **Administration-oriented** – that itemizes the vertical services required by specific administration (as parenthetically noted), but have little relevance outside of that administration.

Transaction Oriented

These services support inter-process communications ranging from low-level procedure calls to high-level business transactions.

2.2.3.1 RMI-IIOP

The Remote Method Invocation over Internet Inter-ORB Protocol (RMI-IIOP) is a Java specific mechanism that allows objects to be created and used in a distributed environment.

Rules

- None

Guidelines

- Use RMI-IIOP invocation only when both sender & receiver are internally controlled components.

Standards

- J2SE APIs (java.rmi package) – Sun Microsystems; Java 2 Platform Standard Edition 5.0 API Specification; reference at http://java.sun.com/j2se/1.5.0/docs/api/java/rmi/package-summary.html
- RMI IDL - Object Management Group; Java Language Mapping to OMG IDL, September 2003, Version 1.3, formal/03-09-04; reference at http://www.omg.org/cgi-bin/apps/doc?formal/03-09-04.pdf

2.2.3.2 Web Services API

The Web Services API mechanism enables a remote procedure call from a client to be communicated to a remote server. A server defines a service as a collection of procedures that are callable by remote clients. A client calls procedures to access service defined by the server. In Web Services, a remote procedure call is represented using an XML based protocol defined by the SOAP specification for exchanging information in a decentralized, distributed environment. SOAP defines a convention for representation of remote procedure calls and responses in addition to the definition of the SOAP envelope and encoding rules.

Rules

- None

Guidelines

- HTTP is the preferred SOAP transport protocol since it can be more easily secured using SSL.
- If possible, the following data types should always be avoided because they are not completely defined in the JAX-RPC and/or XML Schema specification and can lead to unpredictable results: Char Type, Unsigned Numerical Types, and Enumerations. Alternatively, arrays can be used instead of enumerated collections.
- If possible, Complex Data types & Binary Data (via SOAP attachments) should be avoided when JAX-RPC is used to communicate with web services implemented in other languages. Alternatively, binary data can be mapped to xsd:base64Binary and xsd:hexBinary, but this mapping can be inefficient with large amounts of data.
- SOAP Fault Codes are the preferred method for handling problems since throwing exceptions can only be successfully caught if the “client” is also using Java.

Standards

- JAX-RPC - Sun Microsystems; Java Web Services Developer Pack (Version 1.6) Combined API Specification; reference at http://java.sun.com/webservices/docs/1.6/api/index.html

2.2.3.3 Electronic Data Interchange (EDI)

EDI is the computer-to-computer interchange of strictly formatted messages that represent documents other than monetary instruments. EDI implies a sequence of messages between two parties, either of whom may serve as originator or recipient. The formatted data representing the

documents may be transmitted from originator to recipient via telecommunications or physically transported on electronic storage media.

Rules

- Federal Information Processing Standards Publications; Electronic Data Interchange (FIPS PUB 161-2); reference at http://www.itl.nist.gov/fipspubs/fip161-2.htm

Guidelines

- None

Standards

- US EDI - National: Accredited Standards Committee (ASC) on Electronic Data Interchange (ANSI ASC X12 Standards); reference at http://disa.org/bookstore/public/index.cfm
- UN EDI - International: The United Nations Center for Trade Facilitation and Electronic Business, Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules, Documents EDIFACT Syntax Version 4 Release 1; reference at http://www.gefeg.com/jswg/v41/data/v41_docs.htm (equivalent to the official ISO 9735-1, Second edition 2002-07-01)

2.2.3.4 ebXML

ebXML specifications provide a framework in which EDI's substantial investments in Business Processes can be preserved in an architecture that exploits XML's new technical capabilities. The specification is built on three basic concepts: (1) provide an infrastructure that ensures data communication interoperability; (2) provide a semantics framework that ensures commercial interoperability; and (3) provide a mechanism that allows enterprises to find each other, agree to become trading partners and conduct business with each other.

Rules

- None

Guidelines

- A Business-Process-Specification (contract) is preferred between partners, which define the technical capabilities and documents agreements between partners, but it is not required.

Standards

- Messaging - Organization for the Advancement of Structured Information Standards (OASIS); Message Service Specification, Version 2.0; reference at http://www.ebxml.org/specs/ebMS2.pdf
- Contract - Organization for the Advancement of Structured Information Standards (OASIS); Collaboration-Protocol Profile and Agreement Specification, Version 2.0; reference at http://www.ebxml.org/specs/ebcpp-2.0.pdf

Data Oriented

Data Oriented services support the means to pass data between the processing logic in the business tier or GUI Application and the persistent storage in the data tier.

2.2.3.5 JDBC

JDBC is a Java API that enables Java programs to execute SQL statements. This allows Java programs to interact with any SQL-compliant database. Since nearly all relational database management systems (DBMSs) support SQL, and because Java itself runs on most platforms, JDBC makes it possible to write a single database application that can run on different platforms and interact with different DBMSs.

Rules

- None

Guidelines

- The preferred JDBC drives are of Type 3 or 4 (pure Java with network or native protocols, respectively) with Type 1 (JDBC-ODBC Bridge) being the least preferred.

Standards

- J2EE APIs (JDBC) - Sun Microsystems; Java 2 Platform, Enterprise Edition, v3.0, API Specification; reference at http://java.sun.com/products/jdbc/download.html#corespec30

2.2.3.6 Java Data Objects (JDO)

JDO defines interfaces and classes to be used by application programmers when using classes whose instances are to be stored in persistent storage (persistence-capable classes), and specifies the contracts between suppliers of persistence-capable classes and the runtime environment (which is part of the JDO Implementation).

Rules

- None

Guidelines

- As JDO is the preferred data access method over JDBC.

Standards

- JDO – Java Data Objects Expert Group; Java Data Objects, JSR12, Version1.0.1; reference at http://www.jcp.org/en/jsr/detail?id=012

2.2.3.7 Open Database Connectivity (ODBC)

ODBC is a standard API for accessing databases. ODBC provides plug-and-play functionality from applications to multiple databases by converting SQL requests into the appropriate database-specific calls. Developers can code with ODBC function calls rather than focusing on the complexities of proprietary database interfaces. The resulting applications are database independent: target databases can be updated, switched or added without the need to recode the application.

Rules

- None

Guidelines

- Database specific OLE DB is preferred over ODBC when it's available and applicable.
- The preferred ODBC drivers should support these minimum specifications (a) API functionality for Core and Level 1 and (b) SQL Grammar for Minimum and Core

Standards

- ODBC - Microsoft Corp.; ODBC Programmer's Reference, Part 4 – API Reference; http://msdn.microsoft.com/library/en-us/odbc/htm/odbcabout_this_manual.asp

Note: The ODBC v3.0 specification is a superset of ISO/IEC 9075-3:1995 Information technology -- Database languages -- SQL -- Part3: Call Level Interface (SQL/CLI)

2.2.3.8 OLE DB

OLE DB is a specification for a set of data access interfaces designed to provide applications with uniform access to data stored in diverse information sources and that also provide the ability to implement additional database services. These interfaces comprise an industry standard for data access and manipulation of both relational and non-relational data through a common API that can ensure consistency and interoperability in a heterogeneous world of data and data types. Additionally, OLE DB allows the manipulation of semi-structured and hierarchical data (such as XML data).

Rules

- None

Guidelines

- None

Standards

- OLE DB - Microsoft Corporation; OLE DB Programmer's Reference, Part 4 – OLE DB Reference; referenced at http://msdn.microsoft.com/library/en-us/oledb/htm/oledbabout_the_ole_db_documentation.asp

2.2.3.9 Structured Query Language (SQL)

SQL is a standard interactive and programming language for getting information from and updating a database.

Rules

- None

Guidelines

- None

Standards

- SQL-3 - International Organization for Standardization (ISO); ISO/IEC 9075-1:1999 Information technology -- Database languages -- SQL -- Part 1: Framework (SQL/Framework) with corollary ISO/IEC 9075-1:1999/Cor 1:2000; referenced at http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=26196

2.2.3.10 SQL for Java (SQLj)

SQLj, synonymously with SQL Object Language Bindings (SQL/OLB), is a Java language extension that allows a programmer to embed SQL statements inline with their code. It was developed to complement the dynamic JDBC SQL model with a static SQL model. Unlike the ODBC and JDBC dynamic models, the static model provides strong type checking at application translation time, better manageability of data access through separation of package owner from package runner, and because all SQL is compiled, a vehicle for better performance.

Rules

- None

Guidelines

- None

Standards

- SQLj - International Organization for Standardization (ISO); ISO/IEC 9075-10:2000, Information Technology – Database Languages - SQL - Part 10: Object Language Binding (SQL/ OLB); reference at http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=30613

Administration Oriented

Administration Oriented services support specific requirements within a VA administration, as parenthetically noted. They represent vertical services that do not conflict with the enterprise-wide horizontal services described throughout this document, but have little relevance outside of the noted administration.

2.2.3.11 Medical/Radiology Images Exchange (VHA Only)

Medical/Radiology Images Exchange standards facilitate interoperability of diagnostic medical imaging equipment by specifying: (a) A set of protocols to be followed by devices, (b) The syntax and semantics of Commands and associated information, and (c) Information that must be supplied with an implementation

Rules

- None

Guidelines

- Use DICOM and JPEG-2000 to exchange clinical images between imaging systems.
- Use HL7 to exchange data between imaging systems and health information systems.

Standards

- DICOM - National Electrical Manufacturers Association; Digital Imaging and Communications in Medicine (DICOM), DICOM PS 3 – 2003; reference at http://medical.nema.org/dicom/2001.html
- HL7 - Health Level Seven; The Messaging Standard, version 2.4; reference at http://www.hl7.org/about/hl7about.htm#v24

2.2.3.12 Health Information Data Exchange (VHA Only)

Health Information Data Exchange standards support batch-oriented, messaging capability (i.e., orders, results, admission, discharge, transfer, etc.) between health information systems.

Rules

- None

Guidelines

- Use HL7 when the application is hosted on a PC or Server-based platform, not a micro-controller platform.
- The FDA has not accepted HL7 for use in regulated medical devices.

Standards

- HL7 - Health Level Seven; The Messaging Standard, version 2.4; reference at http://www.hl7.org/about/hl7about.htm#v24
- OMG PIDS – Object Management Group; Person Identification Service; reference at http://www.omg.org/docs/formal/99-03-05.pdf

2.2.3.13 Medical Device Interoperability (VHA Only)

Medical Device Interoperability standards allow for health care providers to plug medical or point of care devices into information and computer systems that allows health care providers to monitor information from inpatient bedside or home healthcare environments (a.k.a. Tele-medicine).

Rules

- None

Guidelines

- Use IEEE1073 when the application is hosted on micro-controller platform, not a PC or server-based platform.

Standards

- Series - Institute of Electrical and Electronics Engineers; Point of Care Medical Device Communication Standards, reference at http://www.ieee1073.org/standards/standards-at-a-glance/standardsataglance.html
    a) Device data / semantics (ISO/IEEE 11073-1xxxx series)
    b) General communication services (ISO/IEEE 11073-2xxxx series)

c) Transports (ISO/IEEE 11073-3xxxx series)

2.2.3.14 Pharmacological Orders Exchange (VHA Only)

Pharmacological Orders Exchange standards allow pharmacies to standardize information between health care providers and the pharmacies for ordering drugs and to facilitate electronic submission of pharmacy claims at the point of service.

Rules

- None

Guidelines

- None

Standards

- NCDCP - National Council on Prescription Drug Programs; NCPDP Telecom Standard Version 5.1; reference at http://www.ncpdp.org/PDF/standards_order_form.pdf

2.2.3.15 Computer Based Training (CBT) Exchange (VHA Only)

Computer Based Training (CBT) Exchange standards support the development, deployment, and interoperability of CBT and Learning systems.

Rules

- None

Guidelines

- Aviation Industry CBT Committee; AICC Guidelines and Recommendations (AGR's); reference at http://www.aicc.org/pages/down-docs-index.htm
    a) AGR006 - Computer Managed Instruction (CMI), Version 2
    b) AGR010 - Web-based Computer Managed Instruction (CMI), Version 1
    c) CMI001 - CMI Guidelines for Interoperability, Version 4.0

Standards

- None

Transformation Services

Transformation services support the processes that capture, cleanse, integrate, and move structured and unstructured data from the application environment into warehousing services.

Rules

- TBD

Guidelines

- TBD

Standards

- TBD

2.3 Data Tier

The Data Tier is the logical layer in a distributed system that maintains persistent data. Additionally, it provides services to interact with legacy applications to integrate their functionality (logic and data) into the enterprise.

In *Figure 2 - DA&D Overview*, External "Services" are depicted in this tier as a placeholder. These applications are outside of the VA's domain, but provide information to the enterprise; so, they act as data repositories to the enterprise. However, there are no technical services directly supporting them since their implementation is outside of the VA's domain. Regardless of their implementation, they are expected to interact with the enterprise though the VA's standard Access Services for their information.

Goals

IT Goal 6: Implement an effective Command and Control, COOP, and COG infrastructure.

- These technologies support an open interface standard, recommended by the FEAPMO, thereby promoting interoperability with internal and external systems.
- These technologies support loosely coupling of heterogeneous legacy systems thereby unifying business functions.

IT Goal 7: Shape the VA IT workforce to support the target One-VA EA.

- These technologies are based on industry best practices and open standards thereby providing many training sources for the workforce.

2.3.1 Enterprise & Local Data Services

Enterprise & Local Data Services is the logical layer in a distributed system that enables the sharing of data between applications. These data services provide for the independent management of data shared by multiple applications by supporting the definition, storage, and retrieval of data elements from Database Management Systems (DBMSs).

Rules

- Enterprise-level data should be stored using a relational model to enforce referential integrity.

Guidelines

- For enterprise-level data needing 24/7-availability under COOP, it should be automatically replicated across multiple data centers.
- Component services are the preferred access method to enterprise-level data especially when dealing with updateable transactions.
- Third Normal Form (3NF) is the preferred minimal normalization standard for all data.

Standards

- Repository

- TBD

Processing (Stored Procedures & Triggers):

- SQLj - International Organization for Standardization (ISO); ISO/IEC 9075-10:2000, Information Technology – Database Languages - SQL - Part 10: Object Language Binding (SQL/ OLB); reference at http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=30613
- SQL/PSM - International Organization for Standardization (ISO); ISO/IEC 9075-4:1999, Information technology – Database languages – SQL – Part 4: Persistent Stored Modules (SQL/PSM); reference at http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=29864

2.3.2 Warehouse Services

Warehouse services are a subject-oriented, integrated, time-variant, non-volatile collection of structured and non-structured data used to support the strategic decision-making process for the enterprise. It is the central point of data integration for business intelligence delivering a common view of enterprise data.

Rules

- TBD

Guidelines

- TBD

Standards

- Model - Object Management Group (OMG); Common Warehouse Metamodel (CWM) Specification; March 2003 Version 1.1, Volume 1 (formal/03-03-02); reference to http://www.omg.org/docs/formal/03-03-02.pdf

2.3.3 Legacy Application Services

The following Legacy Application services provide methods to interact with legacy applications (“as-is”) to integrate their functionality (logic & data) into the enterprise (“to-be”).

J2EE Connector Architecture (JCA)

J2EE Connector Architecture (JCA) defines a standard architecture for connecting the J2EE platform to heterogeneous systems that include COTS products (i.e., ERP, Supply Chain, HR, etc.); other technology platforms (i.e., .NET, DCOM/MTS, MUMPS, etc.) and non-mainstreams database technologies. The connector architecture defines a set of scalable, secure, and transactional mechanisms that enable the integration of these systems with application servers and enterprise applications.

Rules

- None

Guidelines

- None

Standards

- JCA - Sun Microsystems; J2EE Connector Architecture Specification, Version 1.5; reference at http://java.sun.com/j2ee/connector/download.html

Resource Adapters

A resource adapter is a system-level software driver that is used by a Java application to connect to a specific vendor's product under the J2EE Connector Architecture. The resource adapter plugs into an application server and provides connectivity between the EIS, the application server, and the enterprise application.

Rules

- None

Guidelines

- Sun Microsystems; The Java 2, Enterprise Edition Connector Architecture's Resource Adapter; reference in http://java.sun.com/developer/technicalArticles/J2EE/connectorclient/resourceadapter.html

Standards

- JCA - Sun Microsystems; J2EE Connector Architecture Specification, Version 1.5; reference at http://java.sun.com/j2ee/connector/download.html

Common Object Request Broker Architecture (CORBA)

Common Object Request Broker Architecture (CORBA) is a specification for an open, vendor-independent architecture and infrastructure that computer applications use to work together over networks. Using the standard protocol IIOP, a CORBA-based program from any vendor, on almost any computer, operating system, programming language, and network, can interoperate with a CORBA-based program from the same or another vendor, on almost any other computer, operating system, programming language, and network.

Rules

- None

Guidelines

- None

Standards

- CORBA - Object Management Group (OMG); The Common Object Request Broker: Architecture and Specification, July 2002, Version 3.0 (formal/02-06-33); reference at http://www.omg.org/docs/formal/02-06-33.pdf

2.3.4 Meta Data Services

Generically metadata is information about other information. Generally, metadata is used by applications, not humans, to "discover" things about the structure of information it's processing.

Markup Languages Services

These tag-based meta-languages are used to describe the content and structure of documents.

2.3.4.1 Extensible Markup Language (XML)

XML is a pared-down version of the Standard Generalized Markup Language (SGML) especially well suited for the transmission of information from application to application. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.

Rules

- None

Guidelines

- U.S. Federal CIO Council XML Working Group; Draft Federal XML Developer's Guide: Version 0.2, April 2002; reference at http://xml.gov/documents/in_progress/developersguide.pdf
- XSD is preferred for describing the structure of XML documents over DTDs; however, if DTDs are used, then it's recommended to describe the data types using DT4DTD

Standards

- XML - World Wide Web Consortium (W3C); Extensible Markup Language (XML) 1.0 (Third Edition), W3C Recommendation 04 February 2004; reference at http://www.w3.org/TR/REC-xml/
- DT4DTD - World Wide Web Consortium (W3C); Datatypes for DTDs (DT4DTD) 1.0, W3C Note 13 January 2000; reference at http://www.w3.org/TR/dt4dtd
- XPoint - World Wide Web Consortium (W3C); XML Pointer Language (XPointer) Version 1.0, W3C Working Draft 16 August 2002; reference at http://www.w3.org/TR/xptr/

2.3.4.2 XML Schema (XSD)

XML Schemas function as DTDs, but are written in XML for XML documents. They extend DTDs by adding a richer set of data types, attributes, and introduces namespaces. Namespaces are used to qualify element and attributes names by associating them with a URI reference, which prevents identically custom-named tags that may be used in different XML documents from being read the same way. The full specification consists of two parts:

- **Schema** - structures specifies the XML Schema definition language, which offers facilities for describing the structure and constraining the contents of XML 1.0 documents, including those which exploit the XML Namespace facility.

- **Datatypes** - defines facilities for defining datatypes to be used in XML Schemas as well as other XML specifications. The datatype language provides a superset of the capabilities found in XML 1.0 document type definitions (DTDs) for specifying datatypes on elements and attributes.

Rules

- None

Guidelines

- Namespace (emerging) - Logistics Management Institute; Recommended XML Namespace for Government Organizations; GS301L1/August 2003; reference at http://xml.gov/documents/completed/lmi/GS301L1_namespace.pdf

Standards

- Schema - World Wide Web Consortium (W3C); XML Schema Part 1: Structures Second Edition, W3C Recommendation 28 October 2004; reference at http://www.w3.org/TR/xmlschema-1/
- Data Type - World Wide Web Consortium (W3C); XML Schema Part 2: Datatypes Second Edition, W3C Recommendation 28 October 2004; reference at http://www.w3.org/TR/xmlschema-2/
- Namespace - World Wide Web Consortium (W3C); Namespaces in XML (REC-xml-names-19990114); reference at http://www.w3.org/TR/REC-xml-names/

2.3.4.3 Web Services Definition Language (WSDL)

Web Services Definition Language (WSDL) is an XML-based language used to describe the services a business offers and to provide a way for individuals and other businesses to access those services electronically. WSDL is the cornerstone of the Universal, Discovery, and Integration (UDDI) initiative spearheaded by Microsoft, IBM, and Ariba.

Rules

- Use proprietary extensions only for privately (internal) published interfaces.

Guidelines

- The Rules & Guidelines listed under section: *Extensible Markup Language (XML)*.

Standards

- WSDL - World Wide Web Consortium (W3C); Web Services Language (WSDL) 1.1; W3C Note 15 March 2001; reference at http://www.w3.org/TR/wsdl

2.3.4.4 Meta-Meta-Data "Language"

The Meta-Meta-Data specification defines a "language" for describing structure and semantics of both general and domain specific meta-models (i.e., schemas for meta-data) based on a four-layer metadata architecture, where the layers are:

- The user object layer that is comprised of the information that we wish to describe ("Data").
- The model layer is comprised of the meta-data that describes information usually as models.
- The meta-model layer is comprised of the descriptions that define the structure and semantics of meta-data.
- The meta-meta-model layer is comprised of the description of the structure and semantics of meta-meta-data.

Rules

- None

Guidelines

- To exchange meta-model information, both have to conform to the MOF specification.

Standards

- Model - Object Management Group (OMG); Meta Object Facility (MOF) 2.0 Core Specification; reference at http://www.omg.org/cgi-bin/apps/doc?ptc/04-10-15.pdf
- Exchange - Object Management Group (OMG); MOF 2.0 / XMI Mapping Specification, v2.1; reference at http://www.omg.org/cgi-bin/doc?formal/2005-09-01

2.3.4.5 Universal Description, Discovery, and Integration (UDDI)

Universal Description, Discovery, and Integration (UDDI) is an XML-based registry for businesses worldwide to list their services on the Internet. Its ultimate goal is to streamline online transactions by enabling companies to find one another on the Web and make their systems interoperable for e-commerce. UDDI is often compared to a telephone book's white, yellow, and green pages. The project allows businesses to list themselves by name, product, location, or the XML Web services they offer.

Rules

- None

Guidelines

- None

Standards

- UDDI - Organization for the Advancement of Structured Information Standards (OASIS); UDDI Version 3.0; Published Specification, 19 July 2002; reference at http://uddi.org/pubs/uddi-v3.00-published-20020719.pdf

2.3.4.6 ebXML Registry/Repository

The ebXML Registry provides a set of services that enable sharing of information between interested parties for the purpose of enabling business process integration between such parties

based on the ebXML specifications. The shared information is maintained as objects in a repository and managed by the ebXML Registry Services specified below.

Rules

- None

Guidelines

- None

Standards

- **Registry** - Organization for the Advancement of Structured Information Standards (OASIS); OASIS/ebXML Registry Services Specification, v2.1, June 2002; reference at http://www.oasis-open.org/committees/regrep/documents/2.1/specs/ebrs.pdf
- **Model** - Organization for the Advancement of Structured Information Standards (OASIS); ebXML Registry and Repository, Repository Information Model Specification 2, Working Draft 10-August-2000; reference at http://lists.ebxml.org/archives/ebxml-regrep/200009/pdf00003.pdf

2.3.4.7 Metadata Registry/Repository

The Metadata Registry/Repository specifications support the standardization of the structure and contents of metadata registries for accessibility and greater interoperability.

Rules

- None

Guidelines

- None

Standards

- **Design** - International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC); ISO/IEC 11179, Information Technology – Metadata Registries (MDR); reference at http://www.iso.ch/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeStandardsListPage.TechnicalCommitteeStandardsList?COMMID=160
    a) Part 1: Framework
    b) Part 2: Classification
    c) Part 3: Registry Metamodel and Basic Attributes
    d) Part 4: Formulation of Data Definitions
    e) Part 5: Naming and Identification Principles
    f) Part 6: Registration

- **Implementation** – Organization for the Advancement of Structured Information Systems (OASIS); OASIS Registry/Repository Technical Specification, Working Draft 1.1 December 20, 2000; reference at ftp://xsun.sdct.itl.nist.gov/regrep/OasisRegrepSpec.pdf

2.3.5 Common Reference Services

Common Reference services describe the basic building blocks of information that can be stored across the data services.

Data Reference, Health-Oriented (VHA Only)

Data Reference, Health-Oriented represents data content standards within the health care industry that have been accepted by the VHA.

Rules

- VA Handbook 6300.5, Procedures for Establishing & Managing Privacy Act Systems of Records
- VA Directive 6300 Records & Information Management
- Veterans Health Administration (VHA); VistA Lexicon Utility

Guidelines

- None

Standards

- CPT - American Medical Association; Current Procedural Terminology (CPT 4); reference at https://webstore.ama-assn.org/index.jhtml
- DSM - American Psychiatric Association (APA); Diagnostic and Statistical Manual of Mental Disorders, Fourth Edition
- HCPCS - Health Care Financing Administration; Health Care Financing Administration Common Procedure Coding System
- HL7-CDA - Health Level Seven; Clinical Document Architecture; reference at http://www.hl7.org/library/standards_non1.htm#CDA
- ICD - The International Classification of Diseases;
    a) Version 9 - Mortality (ICD-9, Volume 1); reference at ftp://ftp.cdc.gov/pub/Health_Statistics/NCHS/Publications/ICD-9/
    b) Morbidity (ICD-9-CM); reference at ftp://ftp.cdc.gov/pub/Health_Statistics/NCHS/Publications/ICD9-CM/
    c) ICD-9-PCS
- LOINC - Regenstrief Institute for Health Care; Logical Observation Identifiers Names and Codes version 2.08; reference at http://www.loinc.org/download
- NDC - Drug Listing Act of 1972; National Drug Code System; reference at http://www.fda.gov/cder/ndc/

- SNOMED CT - Systematized Nomenclature of Medicine International (SNOMED); SNOMED - Clinical Terms; reference at http://www.snomed.org/main.html
- UHID - ASTM International; Standard Guide for Properties of a Universal Healthcare Identifier (E1714-00); reference at http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/PAGES/E1714.htm?E+mystore

Native Document Formats

Native Document formats are the standard internal organization schemes for human-readable documents meant for public distribution.

Rules

- None

Guidelines

- PDF is the preferred format for document distributed to the general public over the web.

Standards

- PDF - Adobe; PDF Reference, Fifth Edition, Version 1.6; reference at http://partners.adobe.com/public/developer/pdf/index_reference.html#5
- RTF - Microsoft; Rich Text Format (RTF) Specification, Version 1.6; reference at http://msdn.microsoft.com/library/?url=/library/en-us/dnrtfspec/html/rtfspec.asp?frame=true
- Word - Microsoft; Microsoft's Office Word 2000 (doc)

Native Graphics Formats

Native Graphics formats are the standard internal organization schemes for static and interactive two- and three-dimensional images.

Rules

- None

Guidelines

- SVG is the preferred format if the client application can support it because the vector-based image is scalable without losing detail.
- JPEG or GIF are the preferred formats for web-based applications, where JPEG is best used for full color, "natural" scenes and GIF is best for black & white images or man-made graphics.
- JPEG-2000 is the preferred format for medical image exchange using DICOM.

Standards

- GIF - CompuServe Incorporated; Graphics Interchange Format Specification (GIF); reference at http://www.w3.org/Graphics/GIF/spec-gif89a.txt

- JPEG - Independent JPEG Group (IJG); JPEG File Interchange Format, Version 1.02; reference at http://www.w3.org/Graphics/JPEG/jfif3.pdf
- JPEG-2000 (emerging) – The International Organization for Standardization (ISO); Information technology – Information technology -- JPEG 2000 image coding system -- Part 1: Core coding system; reference at http://www.iso.ch/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=15444:1
    a) Part 1 (ISO/IEC 15444-1:2000) with Corollaries (ISO/IEC 15444-1:2000/Cor 1:2002 through ISO/IEC 15444-1:2000/Cor 3:2002) and Amendment (ISO/IEC 15444-1:2000/Amd 1:2002)
- OpenGL - OpenGL Architecture Review Board (ARB); The OpenGL Graphics System: A Specification (Version 2.0 - October 22, 2004); reference at http://www.opengl.org/documentation/specs/version2.0/glspec20.pdf
- PNG - World Wide Web Consortium (W3C); PNG (Portable Network Graphics) Specification, Version 1.0; reference at http://www.w3.org/TR/REC-png.pdf
- SVG - World Wide Web Consortium (W3C); Scalable Vector Graphics (SVG) 1.0 Specification; reference at http://www.w3.org/TR/2001/REC-SVG-20010904/REC-SVG-20010904.pdf

Native Audio Formats

The Native Audio formats service deals with the compression, decompression, processing, and encoding representation of audio.

Rules

- None

Guidelines

- Use MPEG-1 audio Layer 3 (MP3) for audio being burned onto a CD-ROM.

Standards

- MP3 - MPEG-1 - The International Organization for Standardization (ISO); Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s, reference at http://public.ansi.org/ansionline/:
    a) Part 3: Audio (ISO/IEC 11172-3:1993) with Corollary (ISO/IEC 11172-3:1993/Cor 1:1996)

Native Video Formats

The Native Video formats service deals with the compression, decompression, processing, and coded representation of combined moving pictures and audio.

Rules

- None

Guidelines

- Use MPEG-1 for video being burned onto a CD-ROM.
- Use MPEG-2 for video being broadcasted (streaming) over very high bandwidth devices.
- Use MPEG-4 for video being broadcasted (streaming) over low bandwidth devices.

Standards

The following specifications can be referenced at http://public.ansi.org/ansionline/

- MPEG-1 - The International Organization for Standardization (ISO); Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s:
    a) Part 1: Systems (ISO/IEC 11172-1:1993) with Corollaries (ISO/IEC 11172-1:1993/Cor 1:1996 & ISO/IEC 11172-1:1993/Cor 2:1996)
    b) Part 2: Video (ISO/IEC 11172-2:1993) with Corollaries (ISO/IEC 11172-2:1993/Cor 1:1996 & ISO/IEC 11172-2:1993/Cor 2:1996)
    c) Part 3: Audio (ISO/IEC 11172-3:1993) with Corollary (ISO/IEC 11172-3:1993/Cor 1:1996)
- MPEG-2 - The International Organization for Standardization (ISO); Information technology -- Generic coding of moving pictures and associated audio information:
    a) Part 1: Systems (ISO/IEC 13818-1:2000) with Corollaries (ISO/IEC 13818-1:2000/Cor 1:2002 & ISO/IEC 13818-1:2000/Cor 2:2002)
    b) Part 2: Video (ISO/IEC 13818-2:2000) with Corollaries/Amendments (ISO/IEC 13818-2:2000/Cor 1:2002 & ISO/IEC 13818-2:2000/Amd 1:2001)
    c) Part 3: Audio (ISO/IEC 13818-3:1998)
    d) Part 6: Extensions for DSM-CC (ISO/IEC 13818-6:1998) with Corollaries/Amendments (ISO/IEC 13818-6:1998/Cor 1:1999, ISO/IEC 13818-6:1998/Amd 1:2000/Cor 1:2002, ISO/IEC 13818-6:1998/Cor 2:2002, ISO/IEC 13818-6:1998/Amd 1:2000, ISO/IEC 13818-6:1998/Amd 2:2000, & ISO/IEC 13818-6:1998/Amd 3:2001)
    e) Part 7: Advanced Audio Coding (ISO/IEC 13818-7:1997) with Corollary (ISO/IEC 13818-7:1997/Cor 1:1998)
    f) Part 9: Extension for real time interface for systems decoders ISO/IEC 13818-9:1996)
- MPEG-4 - The International Organization for Standardization (ISO); Information technology -- Coding of audio-visual objects:
    a) Part 1: Systems (ISO/IEC 14496-1:2001) with Amendment (ISO/IEC 14496-1:2001/Amd 1:2001)
    b) Part 2: Visual (ISO/IEC 14496-2:2001) with Amendments (ISO/IEC 14496-2:2001/Amd 1:2002 & ISO/IEC 14496-2:2001/Amd 2:2002)
    c) Part 3: Audio (ISO/IEC 14496-3:2001) with Corollary (ISO/IEC 14496-3:2001/Cor 1:2002)

d) Part 6: Delivery Multimedia Integration Framework (ISO/IEC 14496-6:2000)

3 Corporate and Regional Data Processing with COOP

The Corporate and Regional Data Processing (CRDP)/Continuity of Operations (COOP) layer provides close support for the Distributed Applications and Data Layer. In fact many of the services in DA&D have counterparts in the CRDP/COOP layer. The core of the CRDP/COOP layer is middleware. However, operating systems and storage are essential components of the corporate services available to all distributed applications and data. Without the services in CRDP/COOP, DA&D would lack coherence and interoperability; they would cease to be effective as enterprise assets.

Goals

IT Goal 1: Implement One-VA Enterprise Architecture.

- These technologies support a services based, component architecture thereby allowing common functionality to be consolidated into a single source.
- These technologies support loosely coupling of heterogeneous legacy systems thereby unifying business functions.
- These technologies are based on open interface standards that are compliant with FEAPMO guidelines thereby allowing VA to participate in E-GOV initiative with a unified front.

IT Goal 2: Implement a One-VA data network.

- These technologies are based on open, industry standards communications protocols thereby eliminating the need for proprietary networking hardware or software.

IT Goal 3: Secure the One-VA enterprise against Cyber Attack.

- These technologies can support a unified authentication and authorization service thereby enabling Cyber Security's Single Sign On (SSO) and Access Control functions.

IT Goal 5: Establish effective metrics to measure performance.

- These technologies establish a common technical baseline for measuring the impact of development efforts on productivity and mission effectiveness.

IT Goal 6: Implement an effective Command and Control, COOP and COG infrastructure.

- These technologies support a distributed, fault-tolerance application thereby reducing the risk associated with a data center failure or a denial-of-service attack.
- These technologies ensure a common set of organizing principles so that prompt relocation and recovery is feasible.
- These technologies support a strong transaction-processing model thereby eliminating the risk associated with non-Isolated events.
- These technologies support an open interface standard, recommended by the FEAPMO, thereby promoting interoperability with internal and external systems.

IT Goal 7: Shape the VA IT workforce to support the target One-VA EA.

- These technologies can be used to consolidate user interfaces into a common view thereby reducing user training.
- These technologies employ a common technical approach that maximizes the flexibility of the VA IT workforce to address a wide variety of applications and leverages technical training.
- These technologies are based on industry best practices and open standards thereby providing many training sources for the workforce.

3.1 Operating System Services

Operating systems (OS) are complex software systems that provide services for controlling, managing and using programs, platforms, and networks. These services are often referred to as core system services that support the application software in terms of portability and interoperability. Typically, operating systems shield applications from the implementation details of the machine; and efficiently distribute hardware and operating system services among various contending application tasks. The operating system handles the interface to peripheral hardware, schedules tasks, allocates storage, and presents a default interface to the user when no application program is running. The OS may be split into a kernel which is always present and various system programs which use facilities provided by the kernel to perform higher-level house-keeping tasks, often acting as servers in a client-server relationship.[1]

Goals

IT Goal 3: Secure the One-VA enterprise against Cyber Attack.

- A corporate configuration minimizes the variety of threats and economizes on deterrents.
- A common OS facilitates efforts to keep current with patches and releases.

IT Goal 4: Establish a disciplined, non-bureaucratic project management structure.

- A common suite of tools encourages interoperability and sharing between projects.

IT Goal 6: Implement an effective Command and Control, COOP and COG infrastructure.

- A corporate configuration minimizes recovery and reaction time.

IT Goal 7: Shape the VA IT workforce to support the target One-VA EA.

- A corporate configuration facilitates training, employee mobility, and program flexibility.

3.1.1 Desktop Operating Systems

The desktop OS is a multitasking operating system running in the client tier that can execute multiple user applications concurrently. The desktop OS manages the internal resources (i.e., memory and processors); generally the desktop system is configured with one processor. The desktop OS handles the I/O for all attached hardware I/O devices (i.e., hard disks, network interface card, and direct attached printers). The desktop OS communicates the status of the operations run and any errors that occur back to the applications and user.

[1] http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?operating+system

Rule:

- Microsoft XP Professional Edition with latest recommended service pack.

Guidelines

- None

Standards

- None

3.1.2 Server Operating Systems

The server OS is a multitasking operating system running in the middle tier that can execute multiple business or enterprise applications concurrently. The server OS manages the internal resources (i.e., memory and processors); generally a server is configured with multiple processors and the server OS can provide parallel process ring for applications/programs that can run on more than one processor at a time. The server OS handles the input and output (I/O) for all configured hardware I/O devices. The server OS communicates the status of the operations run and any errors that occur back to the applications and users.

Rules

- Microsoft Windows 2003 Server (including Basic, Advanced, and Data Center) with the latest recommended service pack is recommended.
- UNIX and LINUX are preferred for the middle tier and data tier of three tiered applications.

Guidelines

- Existing WinNT implementations shall be replaced, as funds are available.

Standards

- The Single UNIX Specification, Version 3; references at http://www.unix.org/version3/

3.2 Middleware

Middleware is a class of software technologies designed to help manage the complexity and heterogeneity inherent in distributed systems. It is defined as a layer of software above the operating system but below the application program that provides a common programming abstraction across a distributed system. In doing so, it provides a higher-level building block for programmers than Application Programming Interfaces (APIs) such as sockets that are provided by the operating system. This significantly reduces the burden on application programmers by relieving them of this kind of tedious and error-prone programming. Middleware is sometimes informally called “plumbing” because it connects parts of a distributed application with data pipes and then passes data between them.

Goals

IT Goal 3: Secure the One-VA enterprise against Cyber Attack.

- Many of the services, rules, guidelines and standards in this layer are needed to support the Cyber Security Layer. The security needed to support these services is to appear in the Cyber Security Layer, not this layer.

IT Goal 4: Establish a disciplined, non-bureaucratic project management structure.

- Middleware tools link the project participants across the network.

IT Goal 5: Establish effective metrics to measure performance.

- Configuration management assures consistent units of measure, which is a prerequisite to establishing meaningful metrics.
- Capacity Planning and Performance Measurement assures consistent units of measure, which is a prerequisite to establishing meaningful metrics.

IT Goal 6: Implement an effective Command and Control, COOP, and COG infrastructure.

- Middleware tools provide the interoperability essential to efficient and effective recovery.
- Effective recovery requires identification and management of components, data, and code libraries.
- Offer, and continuously evolve, a vast portfolio of value-added, tailorable, enhanced services
- Promote resource sharing
- Improve ability to share information
- Coordinate technology investments within the infrastructure

3.2.1 J2EE Application Services

The J2EE (Java 2 Enterprise Edition) architecture from SUN provides portability across multiple operating systems and hardware. The J2EE platform uses a multi-tiered distributed application model. Application logic is divided into components according to function, and the various application components that make up a J2EE application are installed on different machines depending on the tier in the multi-tiered J2EE environment to which the application component belongs. The J2EE application parts are represented by J2EE Components in the following list.

- Client-tier components run on the client machine.
- Web-tier components run on the J2EE server or a separate web server.
- Business-tier components run on the J2EE server.
- Enterprise information system (EIS)-tier software runs on the EIS server.

Although a J2EE application can consist of the three or four tiers, J2EE multi-tiered applications are generally considered to be three tiered applications because they are distributed over three different locations: client machines, the J2EE server machine, and the database or legacy machines at the back end. Three-tiered applications that run in this way extend the standard two-tiered client and server model by placing a multithreaded application server between the client application and back-end storage.

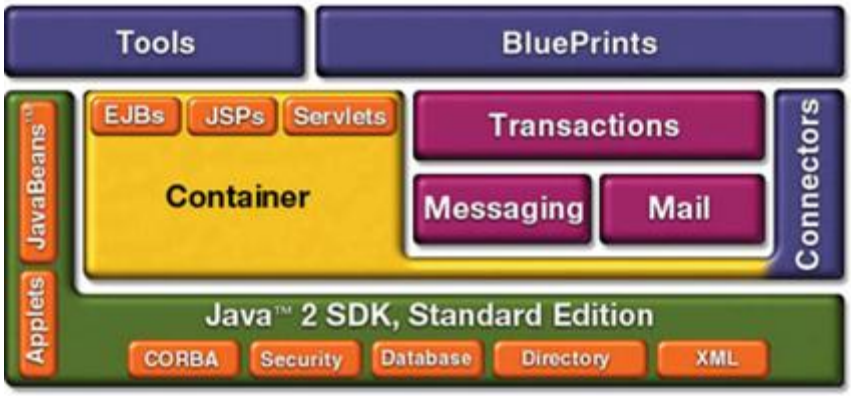

Figure 3 - J2EE Standard Enterprise Services

Rules

- J2EE application servers are the directed and preferred architecture for the business logic tier. This does not mean that no other approach for the business logic tier can be proposed, but justification is required for a different approach. The decision as to whether an existing/ongoing application development must convert or migrate to J2EE will be made at the appropriate Milestone review. Such a decision will depend upon where the project is in the development cycle, the cost associated with migration/conversion, the benefit gained by compliance with One-VA EA, how pervasive the project is in the enterprise, and business factors.

Guidelines

- Java Authentication and Authorization Service Specification, Version 1.0 (JAAS specification) via the Java version of the standard Pluggable Authentication Module (PAM) framework at http://java.sun.com/security/jaas/doc/pam.html
- Java Online Analytical Processing (JOLAP) is a Java API for the J2EE environment that supports the creation and maintenance of OLAP data and metadata, in a vendor independent manner. http://www.jcp.org/jsr/detail/69.jsp

Standards

- J2SE APIs http://java.sun.com/j2se/1.3/docs/api/index.html - Sun Microsystems; Java 2 Platform, Standard Edition, v 1.3.1, API Specification
- J2EE APIs http://java.sun.com/j2ee/sdk_1.3/techdocs/api/index.html - Sun Microsystems; Java 2 Platform, Enterprise Edition, v 1.3, API Specification
- The Internet Inter-ORB Protocol (IIOP) forms the common basis for broad-scope mediated bridging. The inter-ORB bridge support can be used to implement both immediate bridges and to build "half-bridges" to mediated bridge domains. http://www.omg.org/technology/documents/formal/corba_iiop.htm. See CORBA.

References

- http://java.sun.com/j2ee/download.html#platformspec
- ftp://ftp.java.sun.com/pub/j2ee/aklmn44/j2ee-1_3-doc-tutorial-draft5.pdf

3.2.2 Message-Oriented Middleware

Message-Oriented Middleware (MOM) supports communication between objects and applications by storing messages for asynchronous delivery to target applications. There are two prominent messaging models—message queuing and message passing. Message queuing is used to support point-to-point communication through a message queue. Message queuing enables applications running at different times to communicate across heterogeneous networks and systems that may be temporarily offline. Applications send messages to queues and read messages from queues. Message queuing provides guaranteed message delivery, efficient routing, security, and priority-based messaging. It can be used to implement solutions for both asynchronous and synchronous scenarios requiring high performance. Message passing uses a model known as publish/subscribe whereby a message is pushed to the interested parties that have subscribed to the message. Both models provide guaranteed secured delivery of a single message.[2]

Rules

- TBD

Guidelines

- TBD

Standards

- TBD

3.2.3 eCommerce

Electronic commerce is the buying and selling of goods and services, and the transfer of funds, through digital communications. However EC also includes all inter-company and intra-company functions (such as marketing, finance, manufacturing, selling, and negotiation) that enable commerce and use electronic mail, EDI, file transfer, fax, video conferencing, workflow, or interaction with a remote computer. Electronic commerce also includes buying and selling over the World-Wide Web and the Internet, electronic funds transfer, smart cards, digital cash (e.g., Mondex), and all other ways of doing business over digital networks.[3]

B2BI (Business-to-Business integration) connects customer, supplier, and partner applications, as well as business processes across the Internet. A B2BI approach can be used to achieve collaborative planning among supply chain partners as well as coordinated manufacturing and distribution management. The main function of B2BI is to automate the delivery of messages and business documents. To coordinate processes across company boundaries, B2BI uses

[2] e-Business Infrastructure Integration: Practical Approaches, An Executive White Paper, November 2001, Aberdeen Group, Inc. One Boston Place Boston, Massachusetts 02108 USA http://www-3.ibm.com/e-business/doc/content/feature/offers/infraintegration.pdf Also, see page 31, Appendix A-1,

[3] http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?query=electronic+commerce

technologies such as distributed transaction processing, workflow, publish/subscribe message brokers, and distributed object brokering.[4]

Rules

- TBD

Guidelines

- IETF RFC 1865 "EDI Meets the Internet" http://www.ietf.org/rfc/rfc1865.txt

Standards

- TBD

3.2.4 Internet Services

Internet services are provided via client/server applications that use TCP/IP to communicate across computer networks external to an organization. Intranet services adopt Internet technologies and apply them for use within an organization's internal information systems. The Intranet provides a means of communication between VA developer communities and their customers.

References

- See Network Protocols.

Mail Services

Mail services pass messages between "Message Transfer Agent" (MTA) - a program that is responsible for either delivering the message locally or passing it to another MTA, often on another host. MTAs on different hosts on a network often communicate using SMTP. The message is eventually delivered to the recipient's mailbox - normally a file on his computer - from where he can read it using a mail-reading program (which may or may not be the same Mail User Agent (MUA) as used by the sender).[5]

Rules

- VA Handbook 6102 Internet/Intranet Services

Guidelines

- RFC 1957 Some Observations on Implementations of the Post Office Protocol (POP3). R. Nelson. June 1996.
- VA supports a corporate mail list management service. http://vaww.listserv.med.va.gov/default.htm

Standards

[4] e-Business Infrastructure Integration: Practical Approaches, An Executive White Paper, November 2001, Aberdeen Group, Inc. One Boston Place Boston, Massachusetts 02108 USA http://www-3.ibm.com/e-business/doc/content/feature/offers/infraintegration.pdf

[5] [5] http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?electronic+mail

- Post Office Protocol (POP) version 3 allows a client to access and manipulate electronic mail messages on a server
    a) RFC 1939; reference at http://www.ietf.org/rfc/rfc1939.txt
    b) RFC 2449 POP3 Extension Mechanism updated RFC 1939; reference at http://www.ietf.org/rfc/rfc2449.txt.
- Internet Message Access Protocol (IMAP) V 4.1 replaces POP and permits manipulation of remote message folders, called "mailboxes", in a way that is functionally equivalent to local mailboxes. IMAP4rev1 also provides the capability for an offline client to resynchronize with the server.
    a) RFC 1734; reference at http://www.ietf.org/rfc/rfc1734.txt
    b) RFC2060; reference at http://www.ietf.org/rfc/rfc2060.txt
    c) RFC 2061; reference at http://www.ietf.org/rfc/rfc2061.txt
- Multipurpose Internet Mail Extensions (MIME) extends the format of Internet mail to allow non-US- American Standard Code for Information Interchange (ASCII) textual messages, non-textual messages, multi-part message bodies, and non-US-ASCII information in message headers. MIME support allows compliant e-mail clients and servers to accurately communicate embedded information to internal and external users.
    a) RFC 2045; reference at http://www.ietf.org/rfc/rfc2045.txt
- RFC 821 – Simple Mail Transfer Protocol (SMTP) facilitates transfer of electronic-mail messages. It specifies how two systems are to interact, and the messages format used to control the transfer of electronic mail services.
    a) RFC 821; reference at http://www.ietf.org/rfc/rfc0821.txt
- Extended Simple Mail Transfer Protocol (ESMTP) allows new service extensions to SMTP to be defined and registered with Internet Assigned Numbers Authority (IANA).
    a) RFC 1869; reference at http://www.ietf.org/rfc/rfc1869.txt
    b) RFC 1870; reference at http://www.ietf.org/rfc/rfc1870.txt

Simple Object Access Protocol (SOAP) Services

Simple Object Access Protocol (SOAP) is a protocol for exchanging XML-formatted messages between network peers. The SOAP protocol specification does not mandate a particular underlying transport protocol; implementations currently exist for HTTP and SMTP; more transport bindings may be available in the future. Nor does SOAP specify a particular programming model; both RPC and message-oriented systems can be designed around the SOAP protocol.

SOAP Services are the portion of the web server that listens on a port for SOAP requests. SOAP enables web applications to talk to one another and complete transactions without humans interacting. These services enable documents on different computer platforms to appear to be linked to each other. Based on established and emerging Internet standards, a Web service is a self-describing application component that can be created, published, located, and invoked over a network. A Web service can discover and engage other XML web services to complete complex

tasks over the Internet. XML web services are considered to be the "building blocks" for constructing the next generation of loosely coupled, dynamic e-Business applications that support "just-in-time" solutions.

Rules

- None

Guidelines

- Using XML web services to assemble applications delivers greater levels of business benefits than earlier e-Business approaches. Reuse of existing XML web services improves the efficiencies of business software development. They allow deeper connectivity and integration among applications that exist across companies. Exposing both data and business processes to partners enables more powerful e-Business transactions. Getting immediate access to newly published services enables companies to syndicate applications across multiple Web sites.

Standards

- World Wide Web Consortium (W3C); Simple Object Access Protocol (SOAP) 1.1; W3C Note 08 May 2000; reference at:
    a) http://www.w3.org/TR/2002/WD-soap12-part1-20020626/
    b) http://www.w3.org/TR/2002/WD-soap12-part2-20020626/

Hypertext Transfer Protocol (HTTP) services

Web servers are World Wide Web platforms for creating, managing, and intelligibly distributing information and on-line applications. The web server should address Internet message handling, advanced authoring, and a range of security issues. Most web servers enable users to navigate, create, edit, and publish HTML documents in a user-friendly environment. Web servers and application servers allow developers to create arbitrarily complex and highly scalable n-tier applications that can support rapidly growing e-Business needs. They provide Web connectivity, e-Business functionality, runtime services—e.g., load balancing, failover, hot swapping, transaction management, object management, session management, connection pooling — component integration, and application and data integration services.

Rules

- None

Guidelines

- None

Standards

- HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol that can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers. A feature of

HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred. http://www.apps.ietf.org/rfc/rfc2616.txt

- Transport Layer Security (TLS) is a popular mechanism for enhancing TCP communications with privacy and authentication. TLS is in wide use with the HTTP protocol, and is also being used for adding security to many other common protocols that run over TCP. RFC 2818 describes how to use TLS to secure HTTP connections over the Internet. Current practice is to layer HTTP over SSL (the predecessor to TLS), distinguishing secured traffic from insecure traffic by the use of a different server port. This document documents that practice using TLS. A companion document describes a method for using HTTP/TLS over the same port as normal HTTP [RFC2817]. HTTP [RFC2616] was originally used in the clear on the Internet. However, increased use of HTTP for sensitive applications has required security measures. SSL, and its successor TLS [RFC2246] were designed to provide channel-oriented security.
- ftp://ftp.rfc-editor.org/in-notes/rfc2818.txt
- http://www.apps.ietf.org/rfc/rfc2817.html

File Transfer Protocol (FTP) Services

File Transfer Protocol (FTP) Services are the portion of a server that listens on a port for FTP requests. The default port is 21.

Rules

- None

Guidelines

- None

Standards

- IETF RFC 959; reference at http://www.ietf.org/rfc/rfc0959.txt
- IETF RFC 2228; reference at http://www.ietf.org/rfc/rfc2228.txt
- IETF RFC 2640; reference at http://www.ietf.org/rfc/rfc2640.txt

Terminal Services

Terminal services provide a general, bi-directional, communications capability. Its primary goal is to be a standard method of interfacing terminal devices and terminal-oriented processes to each other.

Rules

- None

Guidelines

- None

Standards

- IETF RFC 854; reference at http://www.ietf.org/rfc/rfc0854.txt

- IETF RFC 855; reference at http://www.ietf.org/rfc/rfc0855.txt
- IETF RFC 856; reference at http://www.ietf.org/rfc/rfc0856.txt

Servlet Services

Servlets are the Java platform technology of choice for extending and enhancing Web servers. Servlets provide a component-based, platform-independent method for building Web-based applications, without the performance limitations of CGI programs. Servlets are independent of server- and platform. A servlet can be thought of as an applet that runs on the server side. Servlets have access to the entire family of Java APIs, including the JDBCTM API to access enterprise databases. Servlets can also access a library of HTTP-specific calls and receive all the benefits of the mature Java language, including portability, performance, reusability, and crash protection.

Rules

- None

Guidelines

- None

Standards

- Java Server Pages (JSP) is part of Sun's J2EE architecture and provides template capabilities for presenting dynamically generated web content. JSPs are text files written in a combination of standard HTML tags, JSP tags, and Java code. http://java.sun.com/products/jsp/

3.2.5 Multimedia Services

Multimedia services provide capabilities for processing various multimedia applications, including presentation services, and make available a broad spectrum of collaboration services. They support the simultaneous sharing of multimedia information across multiple, geographically dispersed work sites. Presentation software support temporal specification and real-time synchronization of multiple media in arbitrary conditions and the importing, transporting, creating, editing, retrieving, and exporting of multimedia information. Collaboration capabilities enable individuals and groups to communicate and work together in either asynchronous or synchronous settings through techniques of shared whiteboards, audio conferencing, video conferencing, text chatter, and shared applications.

Rules

- TBD

Guidelines

- TBD

Standards

- TBD

3.2.6 Search Engines

A remotely accessible program that lets users do keyword searches for information on the Internet. There are several types of search engine; the search may cover titles of documents, URLs, headers, or the full text.[6]

Rules

- TBD

Guidelines

- TBD

Standards

- TBD

3.2.7 Portal

Enterprise Information Portals (EIPs) provide management, aggregation, organization, indexing, and searching of structured and unstructured information. EIPs provide a platform for integrating applications, document systems, databases, real-time information feeds, reports, events, news sources, and calendars for delivery to any community of users—employees, partners, or customers. The targeted user is able to obtain a highly personalized view of pertinent information.[7] Portals bring different web enabled applications into an integrated view. "Portals represent the leading concept for integrating many different information sources into a single mechanism for interacting with the user. They also facilitate providing services in a secured manner that can comply with Section 508 requirements. Multiple projects can share a portal, and multiple portals can be linked to integrate even more information sources and applications. Vertical portals focus on a particular subject, say education at (http://www.students.gov/) or medicine (http://www.health.gov/). The First Gov portal (http://www.firstgov.gov/) has been established as the root portal for the Federal Government."[8]

Rules

- TBD

Guidelines

- TBD

Standards

- Access Board Standards for Section 508 http://www.access-board.gov/sec508/508standards.htm

---

[6] http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?query=search+engines

[7] e-Business Infrastructure Integration: Practical Approaches, An Executive White Paper, November 2001, Aberdeen Group, Inc. One Boston PlaceBoston, Massachusetts 02108 USA http://www-3.ibm.com/e-business/doc/content/feature/offers/infraintegration.pdf

[8] Draft – E-Gov Architecture Guidance, Common Reference Model (CRM), Interagency FEA Working Group at http://www.feapmo.gov/resources/E-Gov_Guidance_Final_Draft_v2.0.pdf

3.2.8 Discovery Services

Directory services help people and applications find the names and addresses of objects and services available to an application. Directory services implemented across an enterprise enable people to find destination recipients in other organizations. Directory services can be connected to the entire VA and can store information such as names of users; organizations; network resources; mailbox addresses; and message distribution lists. Interoperability among external computer systems is supported through compliance with international directory services and standards protocols.

Goals

IT Goal 3: Secure the One-VA enterprise against Cyber Attack.

- The roles and responsibilities of VA employees may be found via these services.

IT Goal 7: Shape the VA IT workforce to support the target One-VA EA.

- The assignments and capabilities of VA employees may be found via these services.

IT Goal 6: Implement an effective Command and Control, COOP and COG infrastructure.

- Systems that are well organized in support of discovery services may also be easier to catalog, monitor, and recover.
- Users can more readily find relocated applications.

Rules

- Directory Services shall run a native Lightweight Directory Services Protocol (LDAP) Directory Server running directly over TCP to a database acting as a backend to another server.

Guidelines

- "The Directory can be used as a repository for many kinds of information. The full power of DAP is unnecessary for applications that require simple read access to a few attribute values. Applications addressing is a good example of this type of use where an application entity needs to determine the Presentation Address (PA) of a peer entity given that peer's Application Entity Title (AET). If the AET is a Directory Name (DN), then the required result can be obtained from the PA attribute of the Directory entry as identified by the AET. This is very similar to DNS."[9]
- LDAP is preferred to full X.500 services.

Standards

- LDAP[10]

[9] ftp://ftp.isi.edu/in-notes/rfc1798.txt

[10] ftp://ftp.isi.edu/in-notes/rfc1798.txt and ftp://ftp.isi.edu/in-notes/rfc2251.txt

3.3 Storage

Enterprise Information Integration (EII) products represent an enterprise-wide solution for data integration that can reduce development time by as much as 50%. An EII platform provides integrated views of different databases across the enterprise or extended enterprise. EII provides a standardized data integration solution, rather than a stovepipe approach, that is usable by each application. An EII system collects information about existing databases and stores the information for rapid reuse in a metadata repository. The metadata includes physical data definitions of source systems such as source data type and location, as well as local schema definitions. Catalog information for a local schema includes table definitions, table names, keys, fields, and data types. EII also captures the meaning of the data in different databases so that an enterprise-integrated view can be generated. [11]

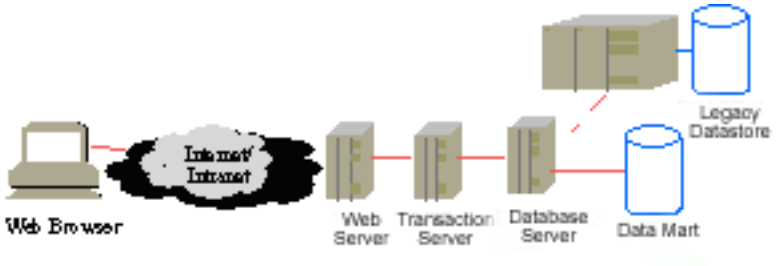

Figure 4 - Storage

Goals

IT Goal 1: Implement One-VA Enterprise Architecture.

- These technologies support a services-based, component architecture thereby allowing common and consolidated data architecture.
- These technologies support loosely coupling of heterogeneous legacy systems thereby unifying disparate data models.
- These technologies are based on open data standards that are compliant with FEAPMO guidelines thereby allowing VA to participate in E-GOV initiative with a unified front.

IT Goal 2: Implement a One-VA data network.

- These technologies support requirements for a robust and survivable network so that data sharing is reliable and prompt.

IT Goal 3: Secure the One-VA enterprise against Cyber Attack.

- These technologies shall support a unified authentication and authorization service thereby enabling Cyber Security's Single Sign On (SSO) and Access Control functions.

IT Goal 5: Establish effective metrics to measure performance.

- These technologies establish a common data repository for collecting and disseminating authoritative measurement data.

[11] e-Business Infrastructure Integration: Practical Approaches, An Executive White Paper, November 2001, Aberdeen Group, Inc. One Boston Place Boston, Massachusetts 02108 USA http://www-3.ibm.com/e-business/doc/content/feature/offers/infraintegration.pdf

IT Goal 6: Implement an effective Command and Control, COOP and COG infrastructure.

- These technologies support a distributed, fault-tolerance data architecture thereby reducing the risk associated with a data center failure or a denial-of-service attack.
- These technologies ensure a common set of organizing principles so that prompt relocation and recovery is feasible.
- These technologies support a strong transaction-processing model thereby eliminating the risk associated with non-Isolated events.
- These technologies support an open interface standard, recommended by the FEAPMO, thereby promoting interoperability with internal and external systems.

IT Goal 7: Shape the VA IT workforce to support the target One-VA EA.

- These technologies can be used to consolidate data models into a common view thereby reducing user training and encouraging data reuse.
- These technologies employ a common technical approach that maximizes the flexibility of the VA IT workforce to improve data hygiene and leverage technical training.
- These technologies are based on industry best practices and open standards thereby providing many training sources for the workforce.

Rules

- Effective enterprise storage solutions must be capable of accommodating a variety of interfaces and have the software support/agents capable of interfacing with major database management systems to be able to maintain data integrity and capture data for backups.
- The key to an effective enterprise storage technology choice is the storage-operating environment (software) that interfaces with the infrastructure. This software must effectively provide the automated means to control and execute data replication in support of business continuity of operations.

Guidelines

- TBD

Standards

- TBD

3.3.1 Database Server

The corporate and regional database server provides an interface to access data stored in diverse legacy databases and interface with non-SQL data repositories.

Rules

- These technologies shall support a unified authentication and authorization service thereby enabling Cyber Security's Single Sign On (SSO) and Access Control functions

Guidelines

- TBD

Standards

- TBD

3.3.2 Enterprise Storage

Enterprise Storage consists of physical and virtual places to host data on the network with varying degrees of persistence (e.g., disk farms, archiving, COOP, content staging). These services include RAID, hierarchical store, data replication, disaster recovery, and site-to-site fail over.

Rules

- Enterprise data storage architecture must be host independent, have a robust disaster recovery capability and be capable of adhering to the following criteria:
- **Information Management**—The enterprise storage solution must include a common information management environment in order to simplify oversight from a centrally managed control center, and implement standardized critical IT processes across the service. For example, it should enable a seamless backup and restore capability and delivery of user performance data for every platform from one primary location, even when the information is distributed to multiple locations. Furthermore, storage management framework software must be provided to perform such tasks as monitoring, configuring (dynamically and statically), problem isolation, problem rectification, and infrastructure planning.
- **Information Sharing**—The enterprise storage solution must employ advanced software intelligence to make data formats and location transparent to users and provide faster, user-friendly access. Through information sharing, the enterprise storage solution must bridge mainframe and open systems environments. This feature requires the ability to share data across the heterogeneous environment including the capability to copy files at channel speeds from one environment to another within the storage device, thus having no impact on the communication LAN.
- **Information Protection**—The enterprise storage solution should provide robust replication functionality to address the requirement for assured and highly reliable continuity of operations (COOP) as protection against planned and unplanned outages. The solution must ensure maximum protection and 99.99 percent data availability for operational readiness and mission continuance. The solution must offer enhancements to improve disk subsystem availability with minimal performance degradation and enhance capabilities to restore operations quickly. The replication solution must be near real-time, work over extended distances, be bi-directional and have the ability to fail over to remote location(s) and fail back to the primary location as a means of recovery from unplanned outages.
- **Enterprise Connectivity**—A host independent enterprise storage solution that connects, stores and retrieves data from all major computing platforms, to include concurrent mainframe and open systems environments is required. This includes connectivity to networks, file servers, web servers, and management interfaces throughout the

organization to enable interoperability for operational support and mission success in a joint environment.

- **Scalability**—The enterprise storage solution must be scalable in terms of usable storage, cache memory and supported users.
- **Cascadability**—The enterprise storage solution must be cascadable or capable of being re-used or re-deployed, even as legacy applications and (or) servers are discarded and replaced. This characteristic demands that the architecture of the enterprise storage solution be fully capable of seamlessly assimilating breakthroughs in storage technology such as the migration from SCSI to Fiber Channel to Gigabit Ethernet; or the rapid insertion of a faster bus, a higher capacity disk drive, or higher capacity cache, etc.

Guidelines

- TBD

Standards

- TBD

4 Cyber Security

Cyber Security consists of technologies, policies, and procedures designed to ensure the confidentiality, integrity, and availability of all electronic data assets.

VA's Cyber Security is designed to assure the Veteran, his family, and VA employees that their data collected, stored, processed, and transmitted in the performance of VA business is secure.

Note: Any rule, guideline, or standard listed in this introductory section of Cyber Security applies to all services defined below.

Rule

All elements of OneVA's Information Technology Infrastructure will comply with all laws, regulations, and directives dealing with Cyber Security; including but not limited to:

- PL 85-857, 38 USC Title 38 Veterans' Benefits, 2 Sep 1958 Sections 5701, 5705, 7332 (Confidentiality of certain information)
- 5USC552a (PL093-579 Privacy Act), 1973
- United States Code of Federal Regulations Title 18 USC Sec.1030 Fraud and Related Activity in Connection with Computers (Public Law 99-474 Computer Fraud and Abuse Act), 1986
- United States Code of Federal Regulations Title 18 USC Sec.1030 Fraud and Related Activity in Connection with Computers (Public Law 99-474 Computer Fraud and Abuse Act), 1986
- Public Law 100-235 Computer Security Act of 1987 codified at 40USC Sec.759, 8 January 1988
- United States Code of Federal Regulations Title 18 USC Sec.2701 Unlawful Access to Stored Communications, 1/16/96
- OMB Circular A-130, "Management of Federal Information Resources" (http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)
- Public Law 104-191, Health Insurance Portability And Accountability Act Of 1996, Aug. 21, 1996
- Department of Health and Human Services, 45 CFR Parts 160, 162, and 164 - Health Insurance Reform: Security Standards Final Rule, February 20, 2003
- FIPS
- VA Directive 6500 – Cyber Security (DRAFT Updated: February 11, 2003. Rescindes VA Directive 6210) http://vaww.va.gov/publ/direc/pubind.asp
- VA Handbook 6500 – Cyber Security (DRAFT Updated: February 11, 2003. Rescindes VA Handbook 6210) http://vaww.va.gov/publ/direc/pubind.asp
- All VA Publications are listed at http://vaww.va.gov/pubs/direc/

Guideline

- "Current and Future Requirements for Federal Wireless Services in the United States," Revision December 2001 (http://is2.antd.nist.gov/fwuf/index.html)
- "Federal User's Wireless Telephone Security Risks" (http://is2.antd.nist.gov/fwuf/index.html)
- FCC Rule 22.919, "Cellular Fraud" (http://wireless.fcc.gov/services/cellular/operations/fraud.html)
- Federal Information Processing Standards (FIPS) http://csrc.nist.gov/publications/fips/index.html
- Draft NIST Special Publications "800 Series" http://csrc.nist.gov/publications/nistpubs/index.html
- Federal Communications CFR, Title 47, Part 15 (http://www.access.gpo.gov/nara/cfr/waisidx_00/47cfr90_00.html)
- NTIA Manual of Regulations & Procedures for Federal Radio Frequency Management, January 2000 Edition with 2001 Revisions (http://www.army.mil/spectrum/library/regulations.htm)

Standard

- TBD

4.1 Availability

The Cyber Security services provided within the One-VA IT infrastructure are designed to ensure information, assets, and critical services are available to meet business requirements. Availability services ensure that timely and regular system and communications services are available. These services are intended to minimize delay or non delivery of data across communications networks. These services include protecting systems and communications networks from accidental or intentional damage and ensuring graceful degradation in services.

4.1.1 Backup

Backup services ensure that data integrity is maintained and recoverable.

Rules

- Each application or data store shall have an established system backup schedule designed for the criticality of the data contained within the system. See VA Handbook 6500 http://vaww.va.gov/pubs/direc/.

Guidelines

- Exercise the backup-recovery routine at least once per year.

Standards

- TBD

4.1.2 Uninterruptible Power Supply

Uninterruptible Power Supply (UPS) services ensure clean, reliable power is available for all systems, networks and communications. The primary purpose for UPS is to provide for a graceful degradation for non-critical system and to provide power in a transition period to alternate power sources and then transition back once primary power is restored for mission critical systems, networks, and communications. See COOP.

Rules

- UPS systems protecting physical access controls, intrusion detection, alarms, or safety devices shall supply electrical energy to support operation disconnected from any other source of power for at least 24 hours.

Guidelines

- All mission critical systems shall be protected with UPS systems.
- All UPS systems shall provide as a minimum enough time for the operator to save work in progress, exit application, and perform a controlled shutdown.
- Alternate power sources should be tested quarterly.
- Transfer to alternate power sources should be practiced annually.

Standards

- TBD

4.2 Confidentiality

Confidentiality refers to keeping electronic data private; i.e., preventing unauthorized individuals or processes from gaining access to documents, transactions, data, or messages. Confidentiality services ensure that data is not made available or disclosed to unauthorized individuals or computer processes. This is accomplished through the use of data encryption, security association, and key management. In addition, these services ensure that observation of usage patterns of communications resources is not possible.

Rules

- Confidentiality services shall be applied to devices that permit human interaction with the information system.
- Servers that use SSL should be configured to enable SSL v3 only.
- All software and hardware providing encryption services shall be certified according to the FIPS 140 standards.
- Data at rest encryption should employ products that use the symmetric data encryption algorithm AES.

Guidelines

- E-mail encryption should be deployed as S/MIME v2-based solutions (S/MIME v3 in the future). PKI supports trusted digital signatures in S/MIME messages and should be utilized to implement e-mail encryption.

- ISO/IEC 10181-4: 1997 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework; reference at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=24330

Standards

- IETF RFC 2246 - The TLS Protocol version 1.0; reference at http://www.ietf.org/rfc/rfc2246.txt
- IETF RFC 2406 - IP Encapsulating Security Payload (ESP); reference at http://www.ietf.org/rfc/rfc2406.txt
- IETF RFC 2409 - The Internet Key Exchange (IKE); reference at http://www.ietf.org/rfc/rfc2409.txt
- IETF RFC 2633 - S/MIME Version 3 Message Specification; reference at http://www.ietf.org/rfc/rfc2633.txt
- IETF RFC 2660 - The Secure Hypertext Transfer Protocol; reference at http://www.ietf.org/rfc/rfc2660.txt
- ISO/IEC 10181-5: 1996 - Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Confidentiality framework; reference at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=24330
- NIST FIPS 171 - Key Management Using ANSI X9.17, April 1992; reference at http://csrc.nist.gov/publications/fips/index.html
- NIST FIPS 180-2 - Secure Hash Standard, August 2002; reference at http://csrc.nist.gov/publications/fips/index.html
- NIST FIPS 185 - Escrowed Encryption Standard, February 1994; reference at http://csrc.nist.gov/publications/fips/index.html
- NIST FIPS 186-2 - Digital Signature Standard (DSS), January 2000; reference at http://csrc.nist.gov/publications/fips/index.html
- NIST FIPS 197 – Advanced Encryption Standard (AES); specifies the use of AES, May 2002; reference at http://csrc.nist.gov/publications/fips/index.html

4.2.1 Credentialing & Privileging (Cyber Access)

Credentialing and privileging is the key elements used to establish the initial positive identity of an individual. Once the individual has been identified they are assigned to an access group, which sets their privileges to access or use different equipment, data, applications, or functions within the enterprise.

For example, in the Medical community it is the process of establishing a physician's authority and rights to perform medical services within an organization. Information about a physician's university degrees and hospitals where they completed their internship and residency programs is collected and validated. Validation information is provided to the medical director who then determines what privileges the provider should be granted (i.e., what they can do at the hospital or medical institution including admitting, consulting, treating, or operating) and for what disciplines they have those privileges.

Rules

- VA VHA Policy Handbook 1100.19; reference at http://vaww.va.gov/publ/direc/health/publications.asp?publ=handbook&order=Issue&dir=desc

Guidelines

- Credentialing includes, at a minimum, the following:
  a) Training, experience and privileges within the institution to manage the services they are providing;
  b) Completion of a recognized training program documented by a certificate of completion;
  c) Continuing medical education of a minimum of 16 hours every 2 years after initial credentialing;
- Physician credentialing documentation must be kept in patients' medical file/record.
- Credentialing and privileging must be in accordance with federal and agency-specific requirements in the health care service provider industry.

Standards

- TBD

4.2.2 Access Control

Access control services prevent the unauthorized use of information system resources. These services may be applied to various aspects of access to a resource (e.g., access to communications with the resource; the reading, writing; or deletion of an information or data resource; or the execution of a processing resource) or to all accesses to a resource.

Rules

- Access Controls will be applied according to VA Handbook 6500 – "Cyber Security" and IETF RFC 2196 – "Site Security Handbook" for services like TELNET, CGI, and FTP, which may access VA, protected servers.

Guidelines

- Authorized system administrators should be the only ones allowed to perform access services like telnet and rlogin.

Standards

- ISO 10181-3 : 1996 Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework; reference at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=24330
- OMG RAD 10164-9 "Information Processing Systems – Open Systems Interconnection – Systems Management – Part 9: Objects and Attributes for Access Control"; reference at http://www.omg.org/

Additional Standards to apply for protecting Individual Health Information:

- ASTM E1985 E1985-98 Standard Guide for User Authentication and Authorization; reference at http://www.astm.org/
- ASTM E1986 E1986-98 Standard Guide for Information Access Privileges to Health Information; reference at http://www.astm.org/

4.2.3 Encryption

Encryption services use cryptographic algorithms to encode clear text to prevent anyone other than the intended recipient(s) from reading that data. Encryption services are utilized in numerous information protection mechanisms and in infrastructure components required to support these mechanisms, such as data at rest encryption, e-mail encryption, and World Wide Web (WWW) encryption.

Rules

- Servers that use SSL shall be configured to enable SSL v3 only.
- Data at rest encryption products should only employ products that use the symmetric data encryption algorithm AES. Other symmetric encryption algorithms require prior approval before use.
- Adherence to NIST FIPS Pub 140-2 – Security Requirements for Cryptographic Modules, June 2002 – is required when using cryptography for Privacy.

Guidelines

- E-mail encryption should be deployed as S/MIME-based solutions (currently S/MIME v2, possibly S/MIME v3 in the future). PKI supports trusted digital signatures in S/MIME messages and should be used to implement e-mail encryption.
- ISO/IEC 10181-4: 1997 - Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework; reference at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=24330
- ISO/IEC 10181-5: 1996 - Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Confidentiality framework; reference at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=24330

Standards

- NIST – reference at http://csrc.nist.gov/publications/fips/index.html
- NIST FIPS Pub 140-2 - Security Requirements for Cryptographic Modules, June 2002; reference at http://csrc.nist.gov/publications/fips/index.html
- NIST FIPS 171 - April 1992, Key Management Using ANSI X9.17; reference at http://csrc.nist.gov/publications/fips/index.html
- NIST FIPS 180-2 - November 2002, Secure Hash Standard; reference at http://csrc.nist.gov/publications/fips/index.html

- NIST FIPS 185 - February 1994, Escrowed Encryption Standard; reference at http://csrc.nist.gov/publications/fips/index.html
- NIST FIPS 186-2 - January 2000, Digital Signature Standard (DSS) ; reference at http://csrc.nist.gov/publications/fips/index.html
- RFC 2246 - The TLS Protocol version 1.0; reference at http://www.ietf.org/rfc/rfc2246.txt
- RFC 2406 - IP Encapsulating Security Payload (ESP) ; reference at http://www.ietf.org/rfc/rfc2406.txt
- RFC 2409 - The Internet Key Exchange (IKE) ; reference at http://www.ietf.org/rfc/rfc2409.txt
- RFC 2633 - S/MIME Version 3 Message Specification; reference at http://www.ietf.org/rfc/rfc2633.txt
- RFC 2660 - The Secure Hypertext Transfer Protocol; reference at http://www.ietf.org/rfc/rfc2660.txt
- NIST FIPS 197 - Advanced Encryption Standard (AES); specifies the use of AES, May 2002; reference at http://csrc.nist.gov/publications/fips/index.html

Additional Standards to apply for protecting Individual Health Information:

- ASTM E1762 E1762-95 Standard Guide for Electronic Authentication of Health Care Information
- ASTM E1986 E1986-98 Standard Guide for Information Access Privileges to Health Information

Additional Standards to apply in a wireless environment:

- EAP, Extensible Authentication Protocol (defined in IEEE 802.1x)
- TTLS, Tunneling TLS
- WTLS, Wireless Transport Layer Protocol
- LEAP, Lightweight EAP (Cisco proprietary implementation of EAP)
- PEAP, Protected EAP
- TTLS-EAP
- WEP, Wireless Equivalent Privacy protocol (the security protocol for IEEE 802.11 systems, defined in 802.11b)
- TKIP, Temporal Key integrity Protocol (the key exchange protocol defined in the draft IEEE 802.11i)
- WPA, Wireless Protected Access protocol

4.2.4 VPN

Virtual Private Network (VPN) is a service that allows authorized users to access a protected network from an untrusted network.

Rules

- Use of RAS is no longer the preferred method of accessing protected VA infrastructure or assets. VA approved VPN services are the preferred access method for authorized users of the VA network who must access protected assets from outside the One-VA Network.

Guidelines

- IETF RFC 2547 - BGP/MPLS VPNs, March 1999; reference at http://www.ietf.org/rfc/rfc2547.txt
- IETF RFC 2917 - A Core MPLS IP VPN Architecture, September 2000; reference at http://www.ietf.org/rfc/rfc2917.txt

Standards

- IETF RFC 2401 – Security Architecture for the Internet Protocol (IPSec) ; reference at http://www.ietf.org/rfc/rfc2401.txt
- IETF RFC 2402 – IP Authentication Header (AH) ; reference at http://www.ietf.org/rfc/rfc2402.txt
- IETF RFC 2406 – IP Encapsulating Security Payload (ESP) ; reference at http://www.ietf.org/rfc/rfc2406.txt
- IETF RFC 2409 – The Internet Key Exchange (IKE) ; reference at http://www.ietf.org/rfc/rfc2409.txt

4.2.5 Data Integrity

Data integrity is the condition where data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Integrity, in terms of data and network security, is the assurance that information can only be modified by those authorized to do so. Measures taken to ensure integrity include controlling the physical environment of networked terminals and servers, restricting access to data, and maintaining rigorous identification, authentication, and authorization practices. Data integrity can also be threatened by environmental hazards, such as heat, dust, water, and electrical surges.

Practices followed to protect data integrity in the physical environment include: making servers accessible only to network administrators; keeping transmission media (such as cables and connectors) covered and protected to ensure that they cannot be tapped; and protecting hardware and storage media from power surges, electrostatic discharges, and magnetism.

Network administration measures to ensure data integrity include: maintaining current authorization levels for all users, documenting system administration procedures, parameters, and maintenance activities, and creating disaster recovery plans for occurrences such as power outages, server failure, and virus attacks.

Rules

- TBD

Guidelines

- FIPS PUB 113 - Computer Data Authentication; reference at http://csrc.nist.gov/publications/fips/index.html
- SP 800-25 - Federal Agency Use of Public Key Technology for Digital Signatures and Authentication; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- The 60-Minute Network Security Guide (First Steps Towards a Secure Network Environment) – NSA Systems and Network Attack Center (July 12, 2002)

Standards

- TBD

4.2.6 Checksum, Hash Value

A checksum or hash value is used to detect errors or manipulation during transmission.

A checksum is a count of the number of bits in a transmission unit that is included with the unit so that the receiver can check to see whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received. Both TCP and UDP communication layers provide a checksum count and verification as one of their services.

Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. The hashing algorithm is called the hash function. A good hash function should not produce the same hash value from two different inputs. In this manner, comparison of hash values can be used to verify the integrity of a data file or element.

Rules

- TBD

Guidelines

- FIPS PUB 113 - Computer Data Authentication; reference at http://csrc.nist.gov/publications/fips/index.html
- SP 500-156 – Message Authentication Code (MAC) Validation System: Requirements and Procedures; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- SP 800-21 - Guideline for Implementing Cryptography in the Federal Government; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- SP 800-25 - Federal Agency Use of Public Key Technology for Digital Signatures and Authentication; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- The 60-Minute Network Security Guide (First Steps Towards a Secure Network Environment) – NSA Systems and Network Attack Center (July 12, 2002)

Standards

- FIPS PUB 180-1 - Secure Hash Standard (SHS/SHA-1); reference at http://csrc.nist.gov/publications/fips/index.html

- FIPS PUB 198 - The Keyed-Hash Message Authentication Code (HMAC); reference at http://csrc.nist.gov/publications/fips/index.html

4.2.7 Digital Signature

A Digital Signature is a Cryptographic process used to assure message originator authenticity, integrity, and non-repudiation.

Rules

- TBD

Guidelines

- SP 800-2 - Public-Key Cryptography; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- SP 800-21 - Guideline for Implementing Cryptography in the Federal Government; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- SP 800-25 - Federal Agency Use of Public Key Technology for Digital Signatures and Authentication; reference at http://csrc.nist.gov/publications/nistpubs/index.html

Standards

- FIPS Pub 140-2 - Security Requirements for Cryptographic Modules, June 2002; reference at http://csrc.nist.gov/publications/fips/index.html
- FIPS PUB 186-2 – Digital Signature Standard (DSS); reference at http://csrc.nist.gov/publications/fips/index.html
- IETF RFC 2807 - XML-Signature Requirements; reference at http://www.ietf.org/rfc/rfc2807.txt
- IETF RFC 3076 - Canonical XML Version 1.0; reference at http://www.ietf.org/rfc/rfc3076.txt
- IETF RFC 3075 - XML-Signature Syntax and Processing; reference at http://www.ietf.org/rfc/rfc3075.txt
- IETF RFC 3275 - XML-Signature Syntax and Processing; reference at http://www.ietf.org/rfc/rfc3275.txt

4.2.8 Identification & Authentication

Identification & Authentication is a set of security measures designed to establish the validity of an identity of a user, user device, or other entity.

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Currently, authentication is most commonly done through the use of logon passwords. Some business processes may require a more stringent authentication process. The use of digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure is another way to perform authentication with higher assurance. Logically, authentication precedes authorization.

Rules

- VA Information System Account and Password Management Policy (January 2000)
- VA Security Standards Profile Summary and Department of Veterans Affairs Protection Profiles for Information Systems (November 13, 2001)
- Authentication methods and technologies implemented by the VA shall offer no less than two-factor authentication.

Guidelines

- The 60-Minute Network Security Guide (First Steps Towards a Secure Network Environment) – NSA Systems and Network Attack Center (July 12, 2002)
- FIPS PUB 48 - Guidelines On Evaluation Of Techniques For Automated Personal Identification; reference at http://csrc.nist.gov/publications/fips/index.html
- FIPS PUB 190 - Guideline For The Use Of Advanced Authentication Technology Alternatives; reference at http://csrc.nist.gov/publications/fips/index.html
- SP 800-12 - An Introduction to Computer Security: The NIST Handbook; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- SP 800-25 - Federal Agency Use of Public Key Technology for Digital Signatures and Authentication; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- IETF RFC 2989 - Criteria for Evaluating AAA Protocols for Network; reference at http://www.ietf.org/rfc/rfc2989.txt
- IETF RFC 3127 - Authentication, Authorization, and Accounting: Protocol Evaluation; reference at http://www.ietf.org/rfc/rfc3127.txt
- Authentication, Authorization and Accounting (AAA) Transport Profile
- ISO 10181-2 "Open Systems Interconnection -- Security frameworks for open systems: Authentication framework"; reference at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=24330

Additional Guidelines to apply for protecting Individual Health Information:

- ASTM E1985-98 – Guide for User Authentication and Authorization, 1998
- ASTM E1714-95 - Properties of a Universal Healthcare Identifier (UHID), 08/15/1995

Standards

- IEFT RFC 2865 - Remote Authentication Dial In User Service (RADIUS). June 2000; reference at http://www.ietf.org/rfc/rfc2865.txt
- OASIS_SAML – Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML), 31 May 2002

Additional Standards to apply in a wireless environment:

- EAP, Extensible Authentication Protocol (defined in IEEE 802.1x)
- TTLS, Tunneling TLS
- WTLS, Wireless Transport Layer Protocol
- LEAP, Lightweight EAP (Cisco proprietary implementation of EAP)
- PEAP, Protected EAP
- TTLS-EAP

4.2.9 Public Key Infrastructure

The Public key Infrastructure is a framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies.

PKI provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. PKI facilitates the use of public key cryptography, which is a common method for authenticating an individual or encrypting a file. PKI consists of:

- A certificate authority (CA) issues and verifies digital certificate. A certificate includes the public key or information about the public key,
- A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor,
- One or more directories where the certificates (with their public keys) are held, and
- A certificate management system.

Rules

- VA Directive 6213 – VA Public Key Infrastructure
- Federal Bridge Certificate Authority (FBCA) Certificate Policy, 12/27/2000; reference at http://cs-www.ncsl.nist.gov/pki/fbca/
- Department of Veterans Affairs, VA PKI: Certificate Policy, DRAFT v2.0, June 14, 1999

Guidelines

- FIPS PUB 48 - Guidelines On Evaluation Of Techniques For Automated Personal Identification; reference at http://csrc.nist.gov/publications/fips/index.html
- FIPS PUB 190 - Guideline For The Use Of Advanced Authentication Technology Alternatives; reference at http://csrc.nist.gov/publications/fips/index.html
- FIPS PUB 196 - Entity Authentication Using Public Key Cryptography; reference at http://csrc.nist.gov/publications/fips/index.html
- SP 800-2 - Public-Key Cryptography; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- SP 800-15 - Minimum Interoperability Specification for PKI Components (MISPC), Version 1; reference at http://csrc.nist.gov/publications/nistpubs/index.html

- SP 800-21 - Guideline for Implementing Cryptography in the Federal Government; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- SP 800-25 - Federal Agency Use of Public Key Technology for Digital Signatures and Authentication; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- SP 800-32 - Introduction to Public Key Technology and the Federal PKI Infrastructure; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- IETF RFC 3447 - PKCS #1: RSA Cryptography Standard: RSA Cryptography Specifications V2.1, February 2003; reference at http://www.ietf.org/rfc/rfc3447.txt
- IETF RFC 2315 - PKCS #7: Cryptographic Message Syntax V1.5, March 1998; reference at http://www.ietf.org/rfc/rfc2315.txt
- IETF RFC 2527 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework; reference at http://www.ietf.org/rfc/rfc2527.txt
- IETF RFC 2631 - PKCS #3: Diffie-Hellman Key Agreement Method, June 1999; reference at http://www.ietf.org/rfc/rfc2631.txt
- IETF RFC 2985 - PKCS #9: Selected Object Classes and Attribute Types V2.0, November 2000; reference at http://www.ietf.org/rfc/rfc2985.txt
- IETF RFC 2986 - PKCS #10: Certification Request Syntax Specification, November 2000; reference at http://www.ietf.org/rfc/rfc2986.txt
- PKCS #6: Extended-Certificate Syntax Standard
- PKCS #8: Private-Key Information Syntax Standard
- PKCS #11: Cryptographic Token Interface Standard
- PKCS #12: Personal Information Exchange Syntax Standard
- PKCS #13: Elliptic Curve Cryptography Standard
- PKCS #15: Cryptographic Token Information Format Standard

Additional Guidelines to apply for protecting Individual Health Information:

- ASTM E2212-02 – Standard Practice for a Healthcare Certificate Policy, 2002

Standards

- FIPS Pub 140-2 - Security Requirements for Cryptographic Modules, June 2002; reference at http://csrc.nist.gov/publications/fips/index.html
- IETF RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile; reference at http://www.ietf.org/rfc/rfc2459.txt
- IETF RFC 2510 - Internet X.509 Public Key Infrastructure Certificate Management Protocols; reference at http://www.ietf.org/rfc/rfc2510.txt
- IETF RFC 2511 - Internet X.509 Certificate Request Message Format; reference at http://www.ietf.org/rfc/rfc2511.txt

- IETF RFC 2528 - Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates; reference at http://www.ietf.org/rfc/rfc2528.txt
- IETF RFC 2559 - Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2; reference at http://www.ietf.org/rfc/rfc2559.txt
- IETF RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP; reference at http://www.ietf.org/rfc/rfc2560.txt
- IETF RFC 2587 - Internet X.509 Public Key Infrastructure LDAPv2 Schema; reference at http://www.ietf.org/rfc/rfc2587.txt
- IETF RFC 2585 - Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP; reference at http://www.ietf.org/rfc/rfc2585.txt
- IETF RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile; reference at http://www.ietf.org/rfc/rfc3280.txt

4.2.10 Biometrics

Biometrics deals with the automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristic.

Biometrics is the science and technology of measuring and statistically analyzing biological data. Biometrics usually refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes.

Fingerprint and other biometric devices consist of a reader or scanning device, software that converts the scanned information into digital form, and wherever the data is to be analyzed, a database that stores the biometric data for comparison with previous records. When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data scanned when a user tries to gain access.

Rules

- TBD

Guidelines

- FIPS PUB 48 - Guidelines On Evaluation Of Techniques For Automated Personal Identification; reference at http://csrc.nist.gov/publications/fips/index.html
- FIPS PUB 190 - Guideline For The Use Of Advanced Authentication Technology Alternatives; reference at http://csrc.nist.gov/publications/fips/index.html
- Common Data Security Architecture (CDSA) - Human Recognition Services (HRS) Module
- ISO/IEC SC17 7816-11 - Personal Verification Through Biometric Methods

Standards

- ANSI/INCITS 358 - BioAPI V1.1
- ANSI X9.84 - Biometric Information Management and Security
- CBEFF – NISTIR 6529 - Common Biometric Exchange File Format
- ANSI/NIST-ITL-1-2000 - Data Format for Finger/Facial/SMT

4.2.11 Passwords

A password is a protected and private string of numbers, text, and other characters used to authenticate an identity.

A password is an un-spaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user. Typically, users of a multi-user or securely protected single-user system claim a unique name (often called a user ID) that can be generally known. In order to authenticate that someone entering that user ID really is that person, a second identification, the password, known only to that person and to the system itself, is entered by the user.

Rules

- VA Information System Account and Password Management Policy (January 2000)

Guidelines

- The 60-Minute Network Security Guide (First Steps Towards a Secure Network Environment) – NSA Systems and Network Attack Center (July 12, 2002)
- FIPS PUB 48 - Guidelines On Evaluation Of Techniques For Automated Personal Identification; reference at http://csrc.nist.gov/publications/fips/index.html
- FIPS PUB 112 - Password Usage; reference at http://csrc.nist.gov/publications/fips/index.html
- FIPS PUB 181 - Automated Password Generator (APG) ; reference at http://csrc.nist.gov/publications/fips/index.html
- FIPS PUB 190 - Guideline For The Use Of Advanced Authentication Technology Alternatives; reference at http://csrc.nist.gov/publications/fips/index.html
- SP 800-12 - An Introduction to Computer Security: The NIST Handbook; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- SP 800-23 - Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products; reference at http://csrc.nist.gov/publications/nistpubs/index.html

Standards

- TBD

4.2.12 Single Sign On (SSO)

Single Sign On (SSO) is a session or user authentication process that permits a user to enter one name and password in order to access multiple applications. The SSO, which is requested at the initiation of the session, authenticates the user to access all the applications and data to which they have rights on the system, and eliminates future authentication prompts when the user switches applications during that particular session.

Rules

- TBD

Guidelines

- FIPS PUB 48 - Guidelines On Evaluation Of Techniques For Automated Personal Identification; reference at http://csrc.nist.gov/publications/fips/index.html
- SP 800-23 - Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products; reference at http://csrc.nist.gov/publications/nistpubs/index.html

Standards

- OASIS_SAML - Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML), 31 May 2002; reference at http://www.oasis-open.org/committees/security/

4.2.13 Security Token

A Security Token is a physical device, such as a special smart card, that together with something that a user knows, such as a PIN, enables authorized access to a computer system or network.

Rules

- TBD

Guidelines

- FIPS PUB 190 - Guideline For The Use Of Advanced Authentication Technology Alternatives; reference at http://csrc.nist.gov/publications/fips/index.html
- FIPS PUB 196 - Entity Authentication Using Public Key Cryptography; reference at http://csrc.nist.gov/publications/fips/index.html
- SP 500-167 – Smart Card Technology: New Methods for Computer Access Control; reference at http://csrc.nist.gov/publications/nistpubs/index.html
- GSC-IS – Government Smart Card Interoperability Specification (V2.0 NIST)
- PKCS #11: Cryptographic Token Interface Standard
- PKCS #15: Cryptographic Token Information Format Standard
- ISO/IEC 7816 - Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Inter-industry commands for interchange

Standards

- FIPS Pub 140-2 - Security Requirements for Cryptographic Modules, June 2002; reference at http://csrc.nist.gov/publications/fips/index.html

4.3 Security Controls

Security Controls are a collection of services used to maintain the security posture of an enterprise.

4.3.1 Secure Code Design

Secure code design is a set of engineering principles for designing system security. These principles provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities can be constructed.

While the primary focus of these principles is the implementation of technical controls, these principles highlight the fact that, to be effective, a system security design should also consider non-technical issues, such as policy, operational procedures, and user education.

Rules

- Use NIST SP 800-27 for guidance on establishing secure code design practices; reference at http://csrc.nist.gov/publications/nistpubs/index.html

Guidelines

- NIST SP 800-27 - NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001; reference at http://csrc.nist.gov/publications/nistpubs/index.html

Standards

- TBD

4.3.2 Boundary Protection

Boundary protection encompasses tools, technologies, and policies designed to prevent penetration or compromise of VA systems from the outside. This concept can also be extended to protecting specific internal network sections or enclaves (high trust levels) from the rest of the VA network.

Rules

- VA Assistant Secretary for Information and Technology Memorandum of October 19, 2001 “Implementing Defense-in-Depth for VA Networks”.

Guidelines

- TBD

Standards

- TBD

4.3.3 Firewalling

A firewall is a system designed to prevent unauthorized access to or from a different parts of a network architecture. In addition to providing network access control, a properly configured and managed firewall can provide network intrusion prevention and limit damage caused by any single intrusion or security event.

Rules

- VA Firewall Policy. (Attachment to the VA Assistant Secretary for Information Technology Memorandum of August 29, 2001 "Securing the Department's Information Technology Infrastructure")
- VA Memorandum Aug 29, 2001 – "Securing the Department's Information Technology Infrastructure"

Guidelines

- All information systems should use application layer gateway network firewalls to secure connections to public networks. Network firewalls can be centrally located, centrally managed, and shared between multiple sites only if a secure intranet is used to connect the sites.
- Network firewalls should be configured with the most restrictive security policy possible, "that which is not expressly allowed is denied."
- Information systems must ensure that any protocols used across public inter-networks are compatible with application layer gateway network firewalls.
- Use host-based firewalls:
    a) With large web portals or web farms
    b) With servers that provide critical services, i.e., database servers, e-mail servers, etc.
    c) With services that process and store critical or proprietary information, i.e., payroll, accounting, human resources, etc.
- Use personal firewalls on:
    a) All client workstations
- Personal firewalls on client workstations shall be centrally managed.
- SP 800-41 - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-41 Guidelines on Firewalls and Firewall Policy; reference at http://csrc.nist.gov/publications/nistpubs/index.html

Standards

- TBD

Intrusion Detection Devices

Intrusion detection services monitor the events occurring in a computer system or network and analyze them for signs of intrusion. An Intrusion Detection System (IDS) is a software or

hardware system that automates the process of monitoring the events occurring in a computer system or network, and then analyzing these events for signs of security problems.

Host-Based Intrusion Detection Systems (HIDS) services monitor specific files, logs and registry settings on a single machine (workstation or server) and can alert on any access, modification, deletion, and copying of the monitored object. The role of a HIDS is to flag any tampering with a specific machine and automatically replace altered files when changed to ensure data integrity.

Network-based Intrusion Detection Systems, (NIDS) provide the ability to monitor different segments of the network in order to discover, define and warn about attacks to the network infrastructure.

Rules

- TBD

Guidelines

- The IDS are not the first line of defense. If firewalls and filtering routers are already in place, then IDS sensors should be placed inside the network to test the effectiveness of firewall and router policies. Placing sensors inside and outside the firewall provides a pre-emptive capability in identifying the threat in the early stages of reconnaissance (i.e., scanning and probing).
- Whenever possible, IDS deployments should combine products from more than one vendor and more than one type. This gives added assurance that attacks can be detected, since not all the sensors types may be able to detect all the known attacks in any given environment or operating condition.

Standards

- NIST SP 800-31 - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-31 Intrusion Detection Systems (IDS), November 2001; reference at http://csrc.nist.gov/publications/nistpubs/index.html

Malicious Code Detection

Malicious Code Detection (anti-virus or virus checking programs) services monitor for viruses and may take action to remove or isolate the virus, preventing it from executing and spreading.

Rules

- All PC-based workstations and servers (including those using the Windows 2000, Windows NT, Windows 95, Windows 98, Linux, Unix (all variants), and Macintosh operating systems) shall employ anti-virus software.
- Updated virus detection signatures shall be downloaded and installed at least monthly.
- Anti-virus software shall be configured to run in a background mode.
- Procedures shall be implemented to:
    a) Scan all files upon access

b) Scan all files before they are attached to outgoing e-mail or transmitted to another machine. A record of the time and date of the scan as well as the tool used should be included in the body of the e-mail.

c) Scan all files and executables.

d) Scan all files incoming to the computer system (e-mail, floppy, CD, FTP, etc.)

- Procedures should be implemented requiring files to be virus scanned before they are attached to outgoing e-mail. A record of the time and date of the scan as well as the tool used should be included in the body of the e-mail.
- Executable files from questionable sources, such as electronic greeting cards and shareware downloads, should be blocked at the external gateways because they may contain malicious software.

Guidelines

- Anti-virus software to detect viruses in resources such as e-mail messages and hard drives and eliminates any that are found must be updated regularly in order to defend against new viruses.
- NIST Virus Information at http://csrc.nist.gov/virus/

Standards

- TBD

4.3.4 Unsolicited E-mail

Unsolicited e-mails congest and restrict the availability of the network to work at acceptable performance levels. SPAM is defined as: to post irrelevant or inappropriate messages to one or more Usenet newsgroups, mailing lists, or other messaging system in a deliberate or accidental manner.

Rules

- All E-mail servers (including those using the Windows 2000, Windows NT, Linux, Unix (all variants), and Macintosh operating systems) shall employ anti-SPAM software.
- Updated SPAM detection signatures shall be downloaded and installed at least monthly.
- Anti-SPAM software shall be configured to run in a background mode.
- Procedures shall be implemented to:

  a) Scan all emails upon access

  b) Scan all emails before they are or transmitted to another machine.

  c) Scan all emails incoming to the domain

- Procedures should be implemented requiring email to be SPAM scanned before they are delivered to outgoing e-mail. A record of the time and date of the scan as well as the tool used should be included in the body of the e-mail.

Guidelines

- Controlling the Assault of Non-Solicited Pornography and Marketing ACT of 2003, January 1, 2004

Standards

- TBD

4.3.5 Audit

A system's audit trail is a collection of audit records containing data about security relevant events, i.e., attempted violations of the security policy and changes to the security state of the system. Audit services provide the means to record the chronological set of related records that provide evidence of system activity.

Rules

- There must be a separation of duties between security personnel who administer the access control function and those who administer the audit trail.
- Reviewers should know what to look for to be effective in spotting unusual activity. They need to understand what normal activity looks like.
- Develop guidelines that describe how frequently audit trails are reviewed and whether there are review guidelines.
- Application owners, data owners, system administrators, data processing function managers, and computer security managers should determine how much review of audit trail records is necessary, based on the importance of identifying unauthorized activities.
- Design the system to allow audit trail function queries by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information. This makes the Audit trail reviews easier and more efficient.
- The appropriate system-level or application-level administrator should review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.

Guidelines

- The audit logs should be maintained for a retention period specified in the applicable security policy.
- At a minimum, each audit record should include the following, if applicable:
  a) The type of event
  b) The date and time the event occurred
  c) A success or failure indicator
  d) The identity of the entity and/or operator that caused the event.
- Actions taken as a result of these reviews should be documented.

- ISO 10181-7 "Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework"; reference at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=24330
- ISO 10164-8 "Information Processing Systems - Open Systems Interconnection - Systems Management - Part 8: Security Audit Trail Function"; reference at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=24330

Standards

- TBD

4.4 Certification & Accreditation (C&A)

Certification & Accreditation (C&A) is the comprehensive evaluation of the technical and non-technical security features and other safeguards of an IT system (system includes: software, hardware, interface, and communication components) to establish the extent that a particular design and implementation meets a set of specified security requirements. The evaluation is made in support of an accreditation process. Certification of the system is based on the documented results of design reviews, system tests, and the recommendations of the testing teams.

Rules

- New Automated Information System (AIS) resources, or those not fully operational, must complete all certification requirements and be accredited (approved for processing) prior to full implementation. Prior to accreditation, each AIS resource must undergo appropriate technical certification evaluations to ensure that:
    a) It meets all Federal and agency-specific policies, regulations, and standards.
    b) All installed security safeguards are adequate and appropriate for the protection requirements of the system.
    c) Systems shall be re-certified when substantial changes are made or at least every 3 years.
- Accreditation is required for all systems. New AIS, or those not fully operational, must complete all requirements and be accredited prior to full implementation.
    a) The designated management official reviews the accreditation support documentation (i.e., security plan, risk analysis, certification results, contingency plan, rules of behavior) and either concurs, thereby declaring that a satisfactory level of operational security is present; or does not concur, indicating that the level of risk either has not been adequately defined or reduced to an acceptable level for operational requirements.
    b) The approving official signs a formal accreditation statement declaring that the system appears to be operating at an acceptable level of risk, or specifies any conditions or constraints that are required for appropriate system protection. Systems shall be re-accredited when major changes occur to the system or every 3 years, whichever occurs first.

- VA Directive 6214 - VA IT Security Certification and Accreditation Program (ITSCAP)
- VA Handbook 6214 - VA IT Security Certification and Accreditation Program (ITSCAP)

Guidelines

- SP 800-23 - Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- ISO IS 15408-1 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model; reference at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=23615&ICS1=35&ICS2=100&ICS3=1
- ISO IS 15408-2 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements; reference at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=23615&ICS1=35&ICS2=100&ICS3=1
- ISO IS 15408-3 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements; reference at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=23615&ICS1=35&ICS2=100&ICS3=1
- NIST SP 800-37 - Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, October 2002; reference at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=23615&ICS1=35&ICS2=100&ICS3=1

Standards

- TBD

4.5 Privacy

Privacy services ensure that an individual's privacy is maintained.

Note: Any Rule, Guideline, or Standard listed in this introductory section of Privacy applies to all services defined below.

Rules

All elements of OneVA's Information Technology Infrastructure will comply with all laws, regulations, and directives dealing with Privacy; including but not limited to:

- PL 85-857, 38 USC Title 38 Veterans' Benefits, 2 Sep 1958 Sections 5701, 5705, 7332 (Confidentiality of certain information)
- 5USC552a (PL093-579 Privacy Act), 1973
- United States Code of Federal Regulations Title 18 USC Sec.1030 Fraud and Related Activity in Connection with Computers (Public Law 99-474 Computer Fraud and Abuse Act), 1986

- United States Code of Federal Regulations Title 18 USC Sec.1030 Fraud and Related Activity in Connection with Computers (Public Law 99-474 Computer Fraud and Abuse Act), 1986
- Public Law 100-235 Computer Security Act of 1987 codified at 40USC Sec.759, 8 January 1988
- United States Code of Federal Regulations Title 18 USC Sec.2701 Unlawful Access to Stored Communications, 1/16/96
- OMB, Circular No. A-130, Revised February 8, 1996
- Public Law 104-191, Health Insurance Portability And Accountability Act Of 1996, Aug. 21, 1996
- Department of Health and Human Services, 45 CFR Parts 160, 162, and 164 - Health Insurance Reform: Security Standards Final Rule, 13 February 2003
- VA Directive 6502 – Privacy Program (DRAFT)

Guidelines

- None

Standards

- NIST FIPS Pub 140-2 – Security Requirements for Cryptographic Modules, June 2002.

4.5.1 Privacy Policy & Procedures

Privacy policy is a plan or course of action intended to influence and determine decisions, actions, and other matters concerning the maintenance of an individual or organization's privacy.

Procedures are platform or role-specific and detail how to implement policy and/or standards. Procedures are generally more detailed and proprietary in nature and, therefore, distributed only to those responsible for implementing them.

Rules

- Adherence to NIST FIPS Pub 140-2 – Security Requirements for Cryptographic Modules, June 2002 – is required when using cryptography for Privacy.

Guidelines

- Elements of a Policy:
  a) Scope. Outlines the purpose of the policy.
  b) High-level Policy statement(s) lists the goal(s) of the policy and the basic rules to follow.
  c) Accountability. Identifies the personnel involved in enforcing the policy, standard, or guidelines.
  d) Non-compliance. Identifies the potential loss that could occur if the policy is not fulfilled.

e) Monitoring. Addresses how the policy will be maintained.

f) Exceptions. Identifies the mechanism for granting temporary variances for parts of the organization that cannot be compliant with the policy.

- Key steps for Policy Development:
- Identify participants, i.e., who develops, who implements, and who authorizes.
- Determine drivers, i.e., government requirements
- Review existing policy documentation
- Establish categories for policy:
  a) Based on ISC2 domains
  b) Based on RFC 2527 (or other standards)
  c) Based on Common Criteria
  d) Based on ISO 17799
- Establish policy components:
  a) Policy number
  b) Date of issuance
  c) Status
  d) Revision history
  e) References and related documents
  f) Purpose
  g) Applicability and scope
  h) Policy
  i) Responsibilities
  j) Policy change procedure
- Key steps for Procedures Development:
- Identify participants, i.e., who develops, who implements, and who authorizes.
- Identify affected system(s)
- Determine drivers, i.e., government requirements, applicable standards, etc.
- Review existing documentation
- Establish procedural components:
  a) ID number
  b) Date
  c) Status

d) Revision history

e) References and related documents

f) Purpose

g) Detailed procedures

h) Responsibilities

i) Change (configuration management) procedure

- Evaluate the Privacy impact each time two or more systems are integrated or data is combined from multiple sources and analytical components. Privacy protection means

  a) Being sensitivity to the privacy concerns of aggregating data from previously separate systems and organizations with potentially different privacy policies and safeguards.

  b) For application components it means controlling the access to Privacy Sensitive data and maintaining the integrity of that data.

Standards

- RFC 2196 - Developing a Security Policy; reference at http://www.ietf.org/rfc/rfc2196.txt
- NIST FIPS Pub 140-2 – Security Requirements for Cryptographic Modules, June 2002.

4.5.2 Privacy Enhancing Technologies

Privacy Enhancing technologies specifically provide privacy services for creating and processing consents and notices, and maintaining confidentiality of data, data integrity, and data availability.

XML – Tagging of Privacy Data

Rules

- TBD

Guidelines

- The XML Registry should identify Privacy Sensitive data, and E-Gov solutions using Privacy Sensitive XML Schemas should form communities of interest to develop and implement consistent, effective safeguards in accordance with the Privacy Act of 1974.

Reference

- http://xmlregistry.nist.gov/xml-gov/
- http://xml.gov/registries.htm

Safe Harbor

Under the safe harbor method, covered entities must remove all of a list of 18 enumerated identifiers and have no actual knowledge that the information remaining could be used, alone or in combination, to identify a subject of the information. The identifiers that must be removed include direct identifiers, such as name, street address, social security number, as well as other

identifiers, such as birth date, admission and discharge dates, and five-digit zip codes. The safe harbor requires removal of geographic subdivisions smaller than a State, except for the initial three digits of a zip code if the geographic unit formed by combining all zip codes with the same initial three digits contains more than 20,000 people. In addition, age, if less than 90, gender, ethnicity, and other demographic information not listed may remain in the information.

Rules

- Ensure that these personal identifiers are removed as required.
- List of Personal Identifiers (Privacy Rule Section 164.514)
    - Name
    - Medical Record Number
    - Telephone/Fax#
    - License #
    - E-mail address
    - SSN
    - Health Plan Beneficiary #
    - Geo-division < state
    - Date elements
    - Web URL
    - Health Plan ID #
    - Account #
    - Certificate/License #
    - Vehicle identifier
    - Device identifier
    - Internet Protocol Address
    - Biometric identifiers
    - Photographic Images
    - Any other unique identifying number, characteristic or code.

Guidelines

- TBD

Standards

- TBD

5 Telecommunications

Telecommunications services provide two-way communications using electrical, electromagnetic, or an optical transmission medium. Information delivered may take the form of voice, video, data, or messaging and can be transported via telephone lines, cables, microwaves, satellites, or light beams.

5.1 Multimedia Transport

Multimedia transport services provide a convergence of the existing voice, video, and data infrastructures. Toll bypass applications use routers (gateways) to route voice and fax calls from one telephone switch to another using packet networks instead of the traditional switched telephone network. Transporting voice over a common infrastructure allows the VA to route voice calls between medical centers using the WAN, reducing expenditures on costly leased lines and public network calls and minimizing the operational costs of moving telephone equipment as employees move from location to location. A converged infrastructure will become increasingly important as the VA increases its use of telemedicine and tele-radiology applications.

Goals

IT Goal 2: Implement a One-VA data network.

- Deploy an efficient and broadly defined network infrastructure
- Offer, and continuously evolve, a vast portfolio of value-added, tailorable, enhanced services
- Reduce telecommunications and network costs, including overhead associated with separate networks for voice, data, and video
- Promote resource sharing
- Improve ability to share information
- Coordinate technology investments within the infrastructure

Rules

- IP PBXs are approved for VA use. This option would allow desktop phones to be replaced by IP telephones and existing PBXs to be replaced with pure IP PBXs. IP PBXs are server-based, highly specialized call management. All include the call control server, a gateway, and analog, digital, or Ethernet phones. An IP PBX provides all the switching on the IP network and connects to the PSTN through the gateway. PBXs must have a modular architecture. PBXs must be expandable and upgradeable to support full interoperability for VoIP internetworking.
- PBXs that do not support VoIP capability are not approved for VA use. All traffic must have the capability to traverse the VA WAN and the VA intranet.

- New PBX equipment must support detection and blocking of incoming modem calls where not allowed. This should be done using Caller ID, Time restrictions, and destination phone numbers.[12]

Guidelines

- PBXs that do not have toll bypass capability should be replaced or upgraded.
- Ensure that existing PBXs support PSTN backup.
- Fine-tune or update your network to adequately support VoIP involves a series of protocols and features geared toward quality of service (QoS).
- Switches that do not support QoS should be replaced.

Standards

- FIPS PUB 178: Video Teleconferencing Services at 56 to 1,920 Kbps. This standard defines the specifications for video teleconferencing and video telephony systems. The standard is intended to ensure interoperability among federal video teleconferencing and videophone systems employing codecs at rates between 56 and 1,920 Kbps.
- ITU T.120: Data Protocols for Multimedia Conferencing: The T.120-Series (T.120-T.132) recommendations are a suite of standards that collectively define a multipoint data communication service for use in multimedia conferencing environments.
- T.120 is a suite of standards that contains a series of communication and application protocols and services that provide support for real-time, multi-point data communications.
- T.121 Generic Application Template
- T.122 Multipoint Communication Service (MCS) for Audiographic and Audiovisual Conferencing
- T.123 Protocol Stacks for Audiographics and Audiovisual Teleconference Applications
- T.124 Generic Conference Control for Audio-Visual and Audiographic Terminals
- T.125 Multipoint Communication Service Protocol Specification
- T.126 Still Image [Conferencing] Protocol Specification
- T.127 Multipoint Binary File Transfer Protocol Specification
- T.130 Real-time Architecture for Multimedia Conferencing
- T.131 Real-Time Stream Multipoint Communications Service
- T.132 Real-time Link Management
- H.221 through H.323 standards provide a foundation for audio, video, and data communications across IP-based networks, including the Internet over LANs. They

[12] This is needed to prevent hackers from war dialing and finding modem equipment and also to assist in identifying people that are trying to break into the VA.

establish standards for compression and decompression of audio and video data streams, ensuring that equipment from different vendors will have some area of common support.

- H.221 Recommendation regarding frame structure for audiovisual teleservices.
- H.223 Multiplexing Protocol for Low Bitrate Multimedia Communication
- H.230 Recommendation regarding frame-synchronous control and indication signals for audiovisual systems
- H.231 Recommendation for multipoint control units using channels up to 2 Mbps
- H.242 Recommendation regarding: System for Establishing Communication Between Audiovisual Terminals using Digital Channels up to 2 Mbps
- H.243 Procedures for Establishing Communication Between Three or More Audiovisual Terminals using Digital Channels up to 2 Mbps
- H.245 Control Protocol for Multimedia Communication
- H.261 Recommendation for simultaneous graphics transmission in the North American region
- ITU H.320: Defines narrow-band telephony systems and terminal equipment in ISDN contexts. This recommendation specifies technical requirements for narrow-band visual telephone systems and terminal equipment, typically for videoconferencing and telephone services.
- ITU H.323 (LAN): Defines packet-based multimedia communications for real-time facsimile transmission in LAN contexts.
- ITU H.310 (ATM): Defines broadband audio-visual communications in ATM networks.
- ITU Q.931 (ISDN): The protocol defined in this standard is the specification for ISDN to establish, maintain, and clear ISDN connections.
- Trunk support for ISDN PRI Q.931 signaling
- Support for QSIG. Also known as Private Signaling System No. 1 (PSS1), QSIG is an important peer-to-peer signaling standard that enables call setup between voice-enabled equipment made by different manufacturers. It is based on the ISDN Q.931 standard.

References

- IETF RFCs; reference at http://www.ietf.org/rfc.html

5.2 Network Management Services

Network management services offer the technical means to monitor and control operation of systems, platforms, networks, and environmental interfaces. Network management refers to the process of determining the amount of resources used by all fixed and mobile VA facilities, systems, and networks. Proactive network management is checking the health of the network during normal operation in order to spot potential problems, optimize performance, and plan upgrades.

5.2.1 Fault Management

Fault management describes the process of preventing, isolating, diagnosing and resolution of problems when they occur. To ensure that critical information is always available at the right place and time, fault management services provide the capability to monitor and detect fault conditions. Fault management can provide the capability for restarting failed processes, and switching over to a secondary device or site, in the event the primary device or site becomes inoperable. A goal of fault management is to ensure COOP and provide rapid network recovery within any defined and agreed upon maximum downtime.

Goals

IT Goal 2: Implement a One-VA data network.

- Provide potential for reduced infrastructure support costs
- Improve manageability of the network

IT Goal 3: Secure the One-VA enterprise against Cyber Attack

IT Goal 5: Establish effective metrics to measure performance

- Organize information faster and cost-effectively

IT Goal 6: Implement an effective Command and Control, COOP, and COG infrastructure

- Provide a network that is available 99.998 percent of the time
- Ensure COOP for network

Rules

- The VA approves for use network management systems that are based on the Simple Network Management Protocol (SNMP Version 3). The network management system shall display management data, monitor and control managed devices, and communicate with management agents. Data link and physical layer parameters shall be monitored by management systems that are based on Remote Monitoring (RMON) standards.

Guidelines

- Select a designated router, server, switch, or end system on each network to be a local management device.
- Users expect quick and reliable fault resolution. Whenever possible, users should be informed about ongoing problems, and given a timeframe for resolution.
- After a problem is resolved, the problem should be tested and then documented in a problem-tracking database.

Standards

- SNMP v3 (IETF RFC 2272): SNMP v3 is the Transmission Control Protocol/Internet Protocol (TCP/IP) suite protocol that manages and controls IP gateways and the networks to which they are attached. It provides a way to monitor and set network configuration and runtime parameters; reference at http://www.ietf.org/rfc/rfc2272.txt

- MIB: This memo defines Management Information Base (MIB) objects for managing remote network monitoring devices and MIB II where the memo defines the second version of the Management Information Base (MIB–II) for use with network management protocols in TCP/IP-based Internets.
    - IETF RFC 1155; reference at http://www.ietf.org/rfc/rfc1155.txt
    - IETF RFC 1157; reference at http://www.ietf.org/rfc/rfc1157.txt
    - IETF RFC 1213; reference at http://www.ietf.org/rfc/rfc1213.txt
    - IETF RFC 2819; reference at http://www.ietf.org/rfc/rfc2819.txt
- RMON: Remote Network Monitoring (RMON) provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed local area networks and interconnecting communication lines (e.g., T1/E1, T3/E3) from a central site.
    - IETF RFC 2021; reference at http://www.ietf.org/rfc/rfc2021.txt
    - IETF RFC 2034; reference at http://www.ietf.org/rfc/rfc2034.txt

5.2.2 Performance Management

Performance management measures available performance parameters to ensure that acceptable levels of performance are maintained. Performance management strives to achieve network conditions where users are satisfied in terms of network responsiveness. Performance management evaluates and reports on the behavior of telecommunications equipment and the effectiveness of the network or network devices. End-to-end performance management measures performance across an internetwork. Component performance measures the performance of individual links or devices. Performance management gathers statistical information, maintains and examines historical logs, determines system performance under natural and simulated conditions. To ensure that the VA is receiving a maximum return on its technical investment, service level agreements (SLAs) should be obtained to confirm that the performance is at the expected levels.

Goals

IT Goal 1: Implement a One-VA Enterprise Architecture

IT Goal 2: Implement a One-VA data network.

- Organize information faster and cost-effectively
- Promote resource sharing

IT Goal 5: Establish effective metrics to measure performance

- Provide a network that is available 99.998 percent of the time
- Provide potential for reduced infrastructure support costs
- Improve manageability of the network

Rules

- The VA approves for use network management systems that are based on the Simple Network Management Protocol (SNMP Version 3). The network management system shall display management data, monitor and control managed devices, and communicate with management agents. Data link and physical layer parameters shall be monitored by management systems that are based on Remote Monitoring (RMON) standards.

Guidelines

- Select a designated router, server, switch, or end system on each network to be a local management device.

Standards

- SNMP v3 (IETF RFC 2272): SNMP v3 is the Transmission Control Protocol/Internet Protocol (TCP/IP) suite protocol that manages and controls IP gateways and the networks to which they are attached. It provides a way to monitor and set network configuration and runtime parameters, reference at http://www.ietf.org/rfc/rfc2272.txt
- MIB: This memo defines Management Information Base (MIB) objects for managing remote network monitoring devices and MIB II where the memo defines the second version of the Management Information Base (MIB–II) for use with network management protocols in TCP/IP-based Internets.
    - IETF RFC 1155; reference at http://www.ietf.org/rfc/rfc1155.txt
    - IETF RFC 1157; reference at http://www.ietf.org/rfc/rfc1157.txt
    - IETF RFC 1213; reference at http://www.ietf.org/rfc/rfc1213.txt
    - IETF RFC 2819; reference at http://www.ietf.org/rfc/rfc2819.txt
- RMON: Remote Network Monitoring (RMON) provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed local area networks and interconnecting communication lines (e.g., T1/E1, T3/E3) from a central site.
    - IETF RFC 2021; reference at http://www.ietf.org/rfc/rfc2021.txt
    - IETF RFC 2034; reference at http://www.ietf.org/rfc/rfc2034.txt

5.2.3 Configuration Management

Configuration management is the management of system change. Configuration management includes procedures for change control, system and network building, network baselining, auditing, and version management. Configuration management establishes change control. The challenge of change is that a change to the network is likely to introduce new faults or expose other faults that had not been observed prior to the change. Change control procedures ensure that the changes to a system are made in a controlled way so that their effect on the system can be predicted. Version management refers to keeping track of the version of operating systems running on the network devices.

Goals

IT Goal 2: Implement a One-VA data network.

IT Goal 5: Establish effective metrics to measure performance

- Organize information faster and cost-effectively
- Provide potential for reduced infrastructure support costs
- Improve manageability of the network

Rules

- The VA approves for use network management systems that are based on the Simple Network Management Protocol (SNMP Version 3). The network management system shall display management data, monitor and control managed devices, and communicate with management agents.
- Data link and physical layer parameters shall be monitored by management systems that are based on Remote Monitoring (RMON) standards.
- Use the Dynamic Host Configuration Protocol (DHCP) as a tool for configuration management. DHCP frees up management time for more strategic tasks.
- Use the VLAN Trunking Protocol (VTP) as a tool for configuration management. VTP keeps track of users membership in VLANs as they move and relocate.

Guidelines

- A configuration management database should be used to house information about network configurations. When a network is operational, it is important that changes be implemented using a controlled methodology.
- Select a designated router, server, switch, or end system on each network to be a local management device.
- After a configuration is verified and validated, it should be stored for future reference.

Standards

- SNMP v3 (IETF RFC 2272): SNMP v3 is the Transmission Control Protocol/Internet Protocol (TCP/IP) suite protocol that manages and controls IP gateways and the networks to which they are attached. It provides a way to monitor and set network configuration and runtime parameters, reference at http://www.ietf.org/rfc/rfc2272.txt
- MIB: This memo defines Management Information Base (MIB) objects for managing remote network monitoring devices and MIB II where the memo defines the second version of the Management Information Base (MIB–II) for use with network management protocols in TCP/IP-based Internets.
    a) IETF RFC 1155; reference at http://www.ietf.org/rfc/rfc1155.txt
    b) IETF RFC 1157; reference at http://www.ietf.org/rfc/rfc1157.txt
    c) IETF RFC 1213; reference at http://www.ietf.org/rfc/rfc1213.txt
    d) IETF RFC 2819; reference at http://www.ietf.org/rfc/rfc2819.txt
- RMON: Remote Network Monitoring (RMON) provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of

distributed local area networks and interconnecting communication lines (e.g., T1/E1, T3/E3) from a central site.

a) IETF RFC 2021; reference at http://www.ietf.org/rfc/rfc2021.txt

b) IETF RFC 2034; reference at http://www.ietf.org/rfc/rfc2034.txt

5.2.4 Accounting Management

One goal of accounting management is to measure network utilization parameters so that individual, group, and department network resources can be fairly allocated. Individual departments or projects are monitored for network use so traffic growth can be estimated for the next capacity-planning phase. In addition to resource information, accounting management information can yield billing information for system usage. Accounting management can also track network usage to detect inefficient network use or abuse of network privileges.

Goals

IT Goal 2: Implement a One-VA data network.

IT Goal 5: Establish effective metrics to measure performance

- Provide potential for reduced infrastructure support costs
- Improve manageability of the network

Rules

- The VA approves for use network management systems that are based on the Simple Network Management Protocol (SNMP Version 3). The network management system shall display management data, monitor and control managed devices, and communicate with management agents.
- The VA shall not approve manual accounting entries to track resource usage

Guidelines

- Select a designated router, server, switch, or end system on each network to be a local management device.
- Accounting management results should be stored in a database.

Standards

- SNMP v3 (IETF RFC 2272): SNMP v3 is the Transmission Control Protocol/Internet Protocol (TCP/IP) suite protocol that manages and controls IP gateways and the networks to which they are attached. It provides a way to monitor and set network configuration and runtime parameters, reference at http://www.ietf.org/rfc/rfc2272.txt
- MIB: This memo defines Management Information Base (MIB) objects for managing remote network monitoring devices and MIB II where the memo defines the second version of the Management Information Base (MIB–II) for use with network management protocols in TCP/IP-based Internets.

  a) IETF RFC 1155; reference at http://www.ietf.org/rfc/rfc1155.txt

b) IETF RFC 1157; reference at http://www.ietf.org/rfc/rfc1157.txt

c) IETF RFC 1213; reference at http://www.ietf.org/rfc/rfc1213.txt

d) IETF RFC 2819; reference at http://www.ietf.org/rfc/rfc2819.txt

- RMON: Remote Network Monitoring (RMON) provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed local area networks and interconnecting communication lines (e.g., T1/E1, T3/E3) from a central site.

  a) IETF RFC 2021; reference at http://www.ietf.org/rfc/rfc2021.txt

  b) IETF RFC 2034; reference at http://www.ietf.org/rfc/rfc2034.txt

5.2.5 Radio Frequency Management

Radio Frequency (RF) services provide the capability for all radio communication devices to transmit and receive efficiently. Radio communication devices in a given area must cooperate if they are to avoid interference problems. If they operate on the same frequencies, at the same time and in the same area, their transmissions produce interference in each other's receivers. RF services regulate the spectrum and controls access because of the potential for interference between uncoordinated uses.

Frequency management provides guidance and support for the assignment, management, and use of radio frequencies used by all elements of the VA. The most common use for VA frequency management is mobile communications, using Ultra High Frequency (UHF) and Very High Frequency (VHF). As the demand for frequency usage has increased, technology has developed radios that can perform the same function at higher unused frequencies or with decreased bandwidth at the same frequency. The VA is converting wideband 25-kilohertz (kHz) channels to narrowband 12.5 kHz channels. The conversion doubles the number of channels and provides communications capability for more users.

Rules

- The National Telecommunications and Information Administration (NTIA) Interdepartmental Radio Advisory Committee must approve the use and acquisition of all VA telecommunications radio equipment.
- Radio frequency assignments shall be valid for five years.

Guidelines

- None

Standards

- National Telecommunications and Information Administration (NTIA) Regulations & Procedures for Federal Radio Frequency Management

Reference:

- http://www.ntia.doc.gov/osmhome/redbook/redbook.html

5.3 Network and Connectivity Services

5.3.1 Wide Area Network (WAN) Services

Wide Area Network (WAN) services are used to link computer systems that span distances beyond the local LAN or campus. WAN services refer to connections between locations over long distances and have no geographical boundary limitation. WAN services are typically rendered by a service provider and support communications between sites that might be in different cities, states, or nations. A variety of WAN service connections are available. Some factors that determine an appropriate WAN connection are cost, the amount of traffic between locations, and the quality of service needed. Technologies commonly used in WAN environments include Frame Relay, Integrated Services Digital Network (ISDN), and ATM.

Goals

IT Goal 1: Implement a One-VA Enterprise Architecture

IT Goal 2: Implement a One-VA data network.

- Deploy an efficient and broadly defined network infrastructure
- Offer, and continuously evolve, a vast portfolio of value-added, tailorable, enhanced services
- Provide a network that scales as new high-bandwidth applications are added in the future
- Provide a network that uses state-of-the-art high speed technologies from the WAN service providers
- Improve the performance of the existing WAN to support more efficient communications
- Increase the bandwidth of the WAN connection to support new applications and the expanded use of current applications

Rules

- The VA shall approve for use ATM as the transport protocol for the enterprise core and distribution layers.
- Frame Relay is viewed as a cost-effective transport service and will continue to be supported by the VA.
- The VA shall no longer approve for use X.25 as a transport to provide site-to-site connectivity.

Guidelines

- Enterprise routers must offer high throughput, high availability, and advanced features to optimize the utilization of high-speed WAN circuits
- A choice of network technologies will continue to be considered for use on a regional basis for localized WAN connectivity across the access layer, as a function of the available local telecommunications infrastructure and marketplace dynamics.

Standards

- ISDN (FIPS 182): The Integrated Services Digital Network defines the generic protocols necessary to establish transparent ISDN connections among government networks and between government and conformant common carrier networks.
- ITU Q.931: The protocol defined in this standard is the specification for ISDN to establish, maintain, and clear ISDN connections.
- Trunk support for ISDN PRI Q.931 signaling
- Support for QSIG. Also known as Private Signaling System No. 1 (PSS1), QSIG is an important peer-to-peer signaling standard that enables call setup between voice-enabled equipment made by different manufacturers. It is based on the ISDN Q.931 standard.
- Frame Relay (ANSI T1.606, ANSI T1.618): Frame relay is a switched packet technology that provides meshed data networks capable of operating at speeds up to T1 (1.544 megabits per second
- ANSI T1.606: The Integrated Services Digital Network (ISDN) Architectural Framework and Service for Frame Relaying Bearer Service establishes an architectural framework within which frame relaying service is described.
- ANSI T1.618: The protocol defined in this standard is a protocol operating in the lowest sublayer of the data link layer of the OSI reference model and is based on a subset of ANSI T1.602 (LAPD) called the "core aspects."
- ATM (ANSI T1.627, T1.629, T1.630), migrating from CCITT ITU–T X.25: ATM is an emerging, cell-based technology that is expected to unify the currently separate networks used for voice, video, and data applications. Consolidation of these networks has the potential to provide significant economic benefits. The service is available in speeds ranging from 1.544 Mbps (T1 or DS-1) to 155 Mbps (Optical Carrier Level 3 or OC-3), with rates expected to be available down to 64 Kbps and up to 622 Mbps (OC-12).

References

- FIPS PUBS: http://www.itl.nist.gov/fipspubs/0-toc.htm
- ATM: http://www.atmforum.com
- Frame Relay: http://www.mot.com/networking/frame-relay/resources.html
- ISO Standards http://www.ansi.org
- X.25: http://www.itu.int
- IETF RFCs: http://www.ietf.org/rfc.html

5.3.2 Metropolitan Area Network (MAN) Services

Metropolitan area network (MAN) services provide access between networks in a metro region. The MAN is the network that picks up traffic from the LAN and passes it to another LAN in the same metro area or to the WAN. The MAN can be described in terms of distance and function. In terms of distance, LANs typically span fewer than two kilometers while MANs can cover distances of up to 150 kilometers. In contrast, the WAN extends beyond the MAN, typically

spanning farther than 150 km. In terms of function, a goal of MAN services is to provide secure distributed broadband access to end-users.

Goals

IT Goal 2: Implement a One-VA data network.

- Deploy an efficient and broadly defined network infrastructure
- Offer, and continuously evolve, a vast portfolio of value-added, tailorable, enhanced services
- Select and implement proven technologies

Rules

- The VA shall approve fiber optic cabling for connectivity between MANs and LANs

Guidelines

- None

Standards

- Synchronous Optical Network (SONET): ANSI T1.105: SONET is made up of a series of standards that define a modular family of rates and formats available for use in interfaces generally referred to as SONET. This series of documents is identified by the T1.105 prefix. ANSI T1.105 describes a base rate and format along with a multiplexing scheme
- Switched Multimegabit Data Service (SMDS): ANSI/IEEE 802.6 Local and metropolitan area networks - Specific requirements Part 6: Distributed Queue Dual Bus (DQDB) Subnetwork of a Metropolitan Area Network (MAN). SMDS is a high-speed, packet-switched WAN networking technology used for communication over public data networks. SMDS can use fiber or copper based media. SMDS support speeds from 1.544 MB to 44 MB.
- IETF RFC 1209: The Transmission of IP Datagrams over the SMDS Service.
- This memo defines a protocol for the transmission of IP and ARP packets over a Switched Multi-megabit Data Service (SMDS) network configured as a logical IP subnetwork.

References

- ANSI Standards http://www.ansi.org
- SONET, IEEE 802.6 http://www.nssn.org
- IETF: http://rfc-1209.rfc-index.com

5.3.3 Campus Area Network (CAN) Services

A campus area network (CAN) is an interconnection of local area networks on land that is usually commonly owned and located, like a hospital campus or a military base. The interconnecting cabling between the buildings is usually commonly owned as well. CANs

require fiber optic cables for connectivity between LANs and can achieve very high throughputs. CANs use a switched infrastructure to span the local wiring closet and local data center, while providing the capacity for high bandwidth requirements. Switched architecture provides virtual local area networks (VLANs). A virtual local area network (VLAN) is a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when they may be located on physically different LAN segments.

Goals

IT Goal 2: Implement a One-VA data network.

- Deploy an efficient and broadly defined network infrastructure
- Offer, and continuously evolve, a vast portfolio of value-added, tailorable, enhanced services
- Provide a network that scales as new high-bandwidth applications are added in the future
- Improve the performance of the existing LAN to support more efficient communications
- Take advantage of standardization based on common functions and customers
- Provide efficient access to information
- Select and implement proven technologies

Rules

- All switches shall support IP multicast technologies to minimize the need for broadcast and point-to-point technologies for multimedia applications.
- All switches shall support the Simple Network Management Protocol (SNMP) Version 3 and the Remote Monitoring (RMON) standard.

Guidelines

- Select switches that contain or can be upgraded to include Layer 3 routing functionality.
- Select switches that support the Virtual LAN Trunking Protocol (VTP)
- Descriptive VLAN names should be used whenever possible to define the campus-wide VLANs. Include the department that the VLAN supports in the VLAN name.
- Ensure that every CAN Layer 2 switch participates in at least two VLANs: one for management and at least one for the users.
- Do not disable spanning-tree on a campus VLAN.

Standards

- IEEE 802.3u (100BaseT Ethernet), migrating from 10BaseT: Category 5 cabling is the recommended cable used for LAN wiring and has ANSI specifications. The name derives from the specifications for meeting the requirements of transmitting up to one hundred million bits per second (or 100 Mbps) across the cable.
- 1000-Base-T Gigabit Ethernet (IEEE 802.3z, 802.3ab), migrating from 100Base T: Category 5e cabling is the recommended cable used for LAN wiring and has ANSI

specifications. The name derives from the specifications for meeting the requirements of transmitting up to one billion bits per second (or 1 Gbps) across the cable.

- IEEE 802.11 (Wireless): The IEEE 802.11a standard is recommended for wireless LANs, while IEEE 802.11b is an alternate. The IEEE 802.11 series of standards defines three characteristics for wireless LANs - diffused infrared, direct sequence and frequency hopping spread spectrum. The 802.11a standard operates at the 5-GHz band and supports data rates between 6 and54 Mbps. The 802.11b standard operates at the 2.4-GHz band and supports data rates between 1 and11 Mbps.
- IEEE 802.1Q (VLAN)
- Fiber Distributed Data Interface (FDDI) (ISO 9314): FDDI is a standard for data transmission on fiber optic lines in a local area network that can extend in range up to 200 km (124 miles).

References

- CSMA: http://webopedia.internet.com/TERM/C/CSMA_CD.html
- 10Base-T: http://webopedia.internet.com/TERM/1/10BaseT.html
- 100Base-T: http://webopedia.internet.com/TERM/1/100BaseT.html
- ISO Standards http://www.ansi.org

5.3.4 Local Area Network (LAN) Services

Local Area Network (LAN) services provide organization by using network devices to share resources and job-specific work tasks. LAN services enable a group of devices, like workstations, servers, and printers, to communicate with each other within a limited geographic area. A typical LAN is located on the same floor or within the same department or building. Ethernet is the most common LAN technology. The first release of Ethernet supported traffic speeds up to 10 Megabytes (10 millions bytes per second). A later version of Ethernet, called Fast Ethernet, supports speeds up to 100 Megabytes (100 million bytes per second). The newest version of Ethernet represents an upgrade from Fast Ethernet and supports network speeds up to 1 Gigabyte (1 billion bytes per second). A virtual local area network (VLAN) is a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when they may be located on physically different LAN segments. Since VLANs are based on logical instead of physical connections, they are extremely flexible. Wireless services represent the newest form of LAN services. Wireless services provide the features and benefit of the LAN without wires or cables. Wireless services use infrared light or radio frequencies. Workstations can communicate with strategically located access points and users are allowed to roam cable free within the limits of the access point coverage.

Goals

IT Goal 2: Implement a One-VA data network.

- Deploy an efficient and broadly defined network infrastructure
- Offer, and continuously evolve, a vast portfolio of value-added, tailorable, enhanced services

- Provide a network that scales as new high-bandwidth applications are added in the future
- Improve the performance of the existing LAN to support more efficient communications
- Take advantage of standardization based on common functions and customers
- Provide efficient access to information
- Select and implement proven technologies

Rules

- The VA network shall approve for use switched Ethernet as the standard for LAN data link layer technology in all LAN installations. Switched Ethernet meets scalability requirements for applications and bandwidth.
- All switches shall support IP multicast technologies to minimize the need for broadcast and point-to-point technologies for multimedia applications.
- All switches shall support the Simple Network Management Protocol (SNMP) Version 3 and the Remote Monitoring (RMON) standard.
- All networks shall support the Dynamic Host Configuration Protocol (DHCP) standard. Designated network devices such as routers, switches, and servers may use static IP addresses for configuration and security purposes.
- The VA network shall not use shared Ethernet. Hubs and bridges do not satisfy the design requirements for scalability

Guidelines

- The VA is currently implementing 100 Mbps Ethernet technologies. New LAN installations should target this technology instead of 10 Mbps networks. Gigabit Ethernet is being used in the Austin Automation Center and should be evaluated for new projects that require such bandwidth.
- Select switches that contain or can be upgraded to include Layer 3 routing functionality.
- Select switches that support the Virtual LAN Trunking Protocol (VTP)

Standards

- IEEE 802.3: Local and Metropolitan Area Networks – Specific Requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.
- The 802.3 standards define the CSMA/CD protocol used in the Ethernet LANs. The standards define network operation over twisted-pair and optical fiber cables at rates of 10 Mbps, 100 Mbps, 1,000 Mbps (1GB), and 10,000 Mbps (10GB).
- IEEE 802.11 (Wireless): The IEEE 802.11a standard is recommended for wireless LANs, while IEEE 802.11b is an alternate. The IEEE 802.11 series of standards defines three characteristics for wireless LANs - diffused infrared, direct sequence and frequency hopping spread spectrum. The 802.11a standard operates at the 5-GHz band and supports

data rates between 6 and54 Mbps. The 802.11b standard operates at the 2.4-GHz band and supports data rates between 1 and11 Mbps.

- IEEE 802.1Q (VLAN): Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.
- Fiber Distributed Data Interface (FDDI) (ISO 9314): FDDI is a standard for data transmission on fiber optic lines in a local area network that can extend in range up to 200 km (124 miles).
- SNMP Version 3 http://rfc-2272.rfclist.com/rfc-2272-3.htm

References

- CSMA: http://webopedia.internet.com/TERM/C/CSMA CD.html
- 10Base-T: http://webopedia.internet.com/TERM/1/10BaseT.html
- 100Base-T: http://webopedia.internet.com/TERM/1/100BaseT.html
- ISO Standards http://www.ansi.org
- Stallings, William, Local and Metropolitan Area Networks (6th Edition),

5.3.5 Cable Plant

Cable plant services are primarily concerned with physical wiring that connect end-user devices like personal computer workstations, terminals, and telephones for communication. Cable plant wiring must be safe and should ensure that the transmitted and received signals are not degraded during transport. The cable plant services must support present and projected needs, and easily accommodate requests for physical infrastructure changes. Plant wiring should provide cabling capacity for user and application requests for voice, video, data, and messaging traffic. The growing use of 100BaseT connections to servers and desktop workstation has created a clear need for even more bandwidth at the backbone and server levels.

Goals

IT Goal 2: Implement a One-VA data network.

- Deploy an efficient and broadly defined network infrastructure
- Offer, and continuously evolve, a vast portfolio of value-added, tailorable, enhanced services
- Select and implement proven technologies

Rules

- The gigabit traffic shall be carried by upgraded unshielded twisted pair copper cabling or fiber optic cabling, depending on the operational requirements.
- The VA shall approve for use fiber optic cabling in building runs and LAN campus backbone networks. In addition, the VA shall approve for use unshielded Cat 5 and Cat 6 twisted pair cable in LAN installations.

- Cat 3 cable shall not be approved for use by the VA in any LAN installation for data. All LAN installation should contain or upgrade to Cat 5 or Cat 6 cable to ensure scalability for future requirements.

Guidelines

- New cable installations should consider Cat 6 provisions for core backbone installations and for multi-gigabit bandwidth requirements.

Standards

- Fiber Optic Cable: Fiber optic cable size is defined by a set of two numbers (e.g., 50/125). The first is the diameter of the core, and the second is the outer diameter of the fiber, both in microns. Most multimode devices operate with one of three commonly found sizes: 50/125, 62.5/125, or 100/140.
- UTP Category 5: A popular network cabling type: unshielded twisted pair (UTP, RJ-45, 10BT, 100BT) is copper cable typically used in an Ethernet environment. UTP cable is used in both 10BaseT and 100BaseT networks.
- UTP Category 6: This is the latest addition to the UTP category family of cables. Cat 6 can provide support for multi-gigabit applications, while maintaining backward compatibility with UTP Cat 5. As streaming media applications become commonplace, the demands for faster data rates can be satisfied by the capacity offered by Cat 6.

References

- ISO Standards http://www.ansi.org
- Fiber Optic Cables: http://www.blackbox.nl/techweb/cables/fiber.htm

5.3.6 IP Routing Services

IP routing services enable packet flow from network to network through routers. The path that a router uses to deliver a packet is defined in its routing table. Routers can statically or dynamically learn the location of traffic destinations from routing protocols. Dynamic routing allows routers to share routing information automatically. If a destination route changes, neighboring routers are informed of the change. The method the router takes to determine a route is described in the specifications of the routing protocol. The routing protocol attempts to find the best path between any source and destination pair in the network. IP routing services provide the capability for routers to find optimum routes, and alternate routes, in the case of network failure or congestion.

Network Address Translation (NAT) performs transparent routing services by performing IP address translation. Transparent routing services are defined as the forwarding of packets from one network to another, and do not require the exchange of routing information. IP address translation is needed when a network's internal IP addresses cannot be used outside the network either because they are private and not valid for use outside, or because the internal addressing must be kept private from the external network. NAT provides the capability to translate public and private addresses in both directions of traffic.

Goals

IT Goal 1: Implement a One-VA Enterprise Architecture

- Deploy an efficient and broadly defined network infrastructure
- Offer, and continuously evolve, a vast portfolio of value-added, tailorable, enhanced services
- Share network reachability information
- Standardize on routing services to ensure network efficiency
- Minimize WAN traffic and conserve network bandwidth

IT Goal 2: Implement a One-VA data network.

IT Goal 6: Implement an effective Command and Control, COOP, and COG infrastructure

Rules

- The Enhanced Interior Gateway Routing Protocol (EIGRP) is approved for VA use as a routing protocol. The Border Gateway Protocol (BGP) is approved for VA use as a routing protocol between autonomous systems.
- For Phase IV future regions, the IGP (Interior Gateway Protocol) will be EIGRP. This protocol applies to all VA region WAN access and distribution routers. All VA regional ASs (autonomous systems) shall use EIGRP as their IGP. BGP shall be used between the distribution and core components.
- The Open Shortest Path First (OSPF) is approved for VA use as a routing protocol between networks.
- The Routing Information Protocol (RIP) routing protocol is not approved for use as a routing protocol. Installations that are currently using RIP should begin an upgrade process.

Guidelines

- Campus IGPs may run another IGP, such as OSPF, within its own campus LAN environment. For design consistency and scalability, it is recommended that the IGP on the LAN be the same as the region WANs.
- To determine an IP routing path to a remote device, use a middleware operating system utility. The utility may be referred to as traceroute or tracert, depending on the operating system in use.

Standards

- Border Gateway Protocol (BGP) is defined in RFC 1771. BGP is an inter-autonomous system routing protocol. The primary function of a BGP speaking system is to exchange network reachability information with other BGP systems.
- Open Shortest Path First (OSPF) protocol is defined in RFC 1583. Open Shortest Path First (OSPF) protocol was developed due to a need in the Internet community to introduce a high functionality non-proprietary Internal Gateway Protocol (IGP) for the TCP/IP protocol family.

- Network Address Translation (NAT) RFC 2663

References

- Christian Huitema, Routing in the Internet, Third Edition, Prentice Hall PTR, 2000.

5.3.7 Network Protocols

For the transport of data to take place, each communications process must adhere to rules and procedures. Network protocols are the rules and technical procedures that enable application and middleware communications across the network. In a network, several protocols work together to ensure that the communication is prepared, transferred, received, and acted upon. The work of the Network Protocols must be coordinated so there is no disagreement. To minimize the potential for conflict, protocols operate in layers. Each layer specifies a different function of the communications process. The lower layer protocols specify how vendors can make their equipment connect to other equipment. Middle layer protocols provide session capability for the middleware layer and ensure that the data is able to move reliably between network devices. The upper layer protocols specify rules for application-to-application interaction.

The TCP/IP protocol suite enables transport, file transfer, terminal emulator, messaging, e-mail, and network management capabilities for core infrastructure system services at the middleware and application layers. The Hypertext Transfer Protocol (HTTP), an application level protocol, is the enabler for World Wide Web access.

Goals

IT Goal 2: Implement a One-VA data network.

- Deploy an efficient and broadly defined network infrastructure
- Offer, and continuously evolve, a vast portfolio of value-added, tailorable, enhanced services
- Select standardized protocols that require minimal support for ease of troubleshooting, upgrades, and manageability

Rules

- All protocols that belong to the TCP/IP suite are supported and approved for use in the VA.

Guidelines

- Use middleware applications that support the TCP/IP suite of protocols. The TCP/IP suite contains a range of protocols that support COOP, infrastructure applications, and services at the middleware layer. SNMP and ICMP provide network management capability for COOP. FTP provides file transfer services. SMTP provides e-mail capability. TELNET provides remote login capability.

Standards

- TCP (IETF RFC 793): The Transmission Control Protocol (TCP) is intended for use as a highly reliable host-to-host protocol between hosts in packet-switched computer

communication networks and in interconnected systems of such networks; reference at; reference at http://www.ietf.org/rfc/rfc0793.txt

- IP (IETF RFC 791): The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks. The Internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses; reference at http://www.ietf.org/rfc/rfc0791.txt
- UDP: User Datagram Protocol (UDP) is a communications method (protocol) that offers non-guaranteed service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP doesn't provide sequencing of the packets that the data arrives in.
- DHCP (IETF RFC 2131): The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network; reference at http://www.ietf.org/rfc/rfc2131.txt
- ICMP (IETF RFC 792): The Internet Protocol (IP) is used for host-to-host datagram service in a system of interconnected networks; reference at http://www.ietf.org/rfc/rfc0792.txt

References

- Douglas Comer, Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture
- William Stallings, High-Speed Networks TCP/IP and ATM Design Principles
- Srinivsan Keshav, et al, An Engineering Approach to Computer Networking
- Douglas E. Comer, Ralph E. Droms, Computer Networks and Internets, with Internet Applications

5.3.8 Domain Name Service (DNS)

The VA requires a mechanism that maps domain names to IP addresses for end systems to communicate easily within the VA network. The Domain Name Service (DNS) allows network devices to be identified and configured with a descriptive domain name. .

Network resources like routers, servers, and workstations can be identified with a host name, instead of an IP address. Domain names are part of the machine name used in e-mail addresses and in host names. DNS maps host names and domain names to IP addresses. Since domain names are alphabetic, they are easier to remember. The conversion from domain name to IP addresses is essential because the computer needs to process numeric information to complete the transaction.

Goals

IT Goal 2: Implement a One-VA data network.

- Maximize usability and manageability by deploying user-friendly host names

Rules

- The VA shall approve for use the Domain Name System to identify network devices.

Guidelines

- Configure DNS within the operating system or application residing at the middleware layer.

Standards

- Domain Name System (IETF RFC 1591) ; reference at http://www.ietf.org/rfc/rfc1591.txt

5.3.9 Remote Access (VPN, PPP)

Remote Access services enable users at remote locations to connect to enterprise network services and applications from almost anywhere. Remote access provides contact from telecommuter sites, mobile computing, as well as technical support. A telecommuter site is a small office with one to a few employees. It can also be a telecommuter's home office. Telecommuters can also refer to mobile users who travel. Mobile computing allows field representatives to access office resources on the road. Technical support can dial in to client systems to diagnose and correct problems remotely. One difference between a remote host and local-based workstations connected directly to the network is slower data transfer speeds. Users can access the network via a Virtual Private Network (VPN) or traditional dial-up. VPNs allow users and customer's access to the VA network while providing a secure connection. Private data is encrypted for routing through the service provider's network or the Internet.

Goals

IT Goal 1: Implement One-VA Enterprise Architecture

IT Goal 2: Implement a One-VA data network.

- Deploy an efficient and broadly defined network infrastructure
- Offer, and continuously evolve, a vast portfolio of value-added, tailorable, enhanced services
- Improve productivity by offering alternate means of remote access

Rules

- The VA network shall approve for use the point-to-point protocol (PPP) as a standard for transporting network layer protocols across dialup serial point-to-point links.

Guidelines

- For users who want higher speeds than analog, remote access can be accomplished with cable modems, DSL, or a router that has access to a WAN port.

Standards

- RFC 1661 - Point-to-Point Protocol (PPP); reference at http://www.ietf.org/rfc/rfc1661.txt
- RFC 2661 - Layer Two Tunneling Protocol (L2TP); reference at http://www.ietf.org/rfc/rfc2661.txt

- RFC 2888 - Secure Remote Access with L2TP; reference at http://www.ietf.org/rfc/rfc2888.txt
- RFC 3193 - Securing L2TP with IPSEC; reference at http://www.ietf.org/rfc/rfc3193.txt

5.3.10 IPv6 Stack Design

The IPv6 stack is configured in a corresponding manner to the v4 stack. However, there are a number of advanced capabilities within v6 that enhance its configuration, ease of use, and management. The IPv6 address is expressed differently from the IPv4 address. The IPv6 address contains eight sections, each separated by a colon (:). Each section contains 16 bits expressed in four hexadecimal numbers. There is additional information in RFC 2460 (http://www.faqs.org/rfcs/rfc2460.html), and an example of an IPv6 address can be seen in *Figure 5 - IPv6 address example*, below.

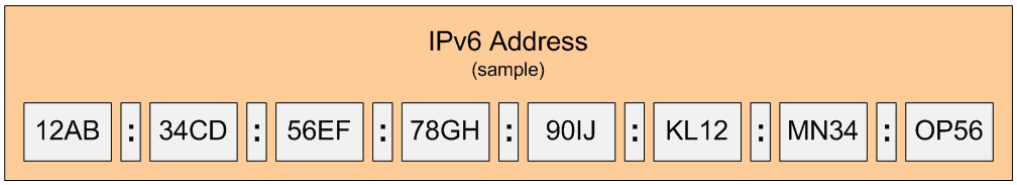

Figure 5 - IPv6 address example

The general header structure of IPv6 is specified in RFC 2460 (http://www.faqs.org/rfcs/rfc2460.html), and has a fixed-length of 40 bytes:

- 16 bytes for source address
- 16 bytes for destination address
- 8 bytes for general header information

Options in IPv6 are handled in an extension header. Extension headers can be inserted if they are needed, and left out, if they're not needed. The current IPv6 specification defines six extension headers:

- Hop-by-hop options header
- Routing header
- Fragment header
- Destination options header
- Authentication header
- Encrypted security payload header

Additional information regarding the IPv6 Header can be found in IETF RFC 2474 (http://www.faqs.org/rfcs/rfc2474.html) and a graphical presentation in *Figure 6 - IPv6 Header Structure*.

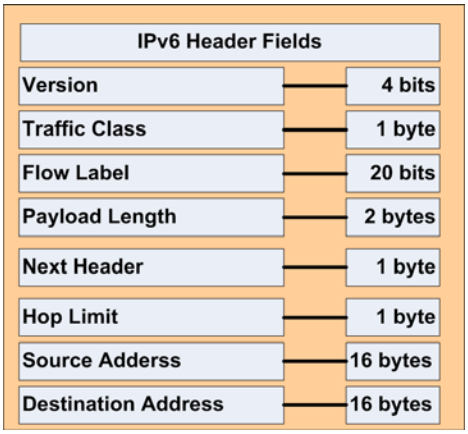

Figure 6 - IPv6 Header Structure

IPv6 and IPv4 will co-exist for an extended period of time. In order to develop a successful transition from one stack to the other, IPv6 hosts and routers need to interoperate with IPv4 hosts and routers. Detailed information regarding Basic Transition Mechanisms can be found IETF RFC 4213 (http://www.faqs.org/rfcs/rfc4213.html). The standards for IPv6 are:

- Dual Stack Transition Mode
- Configured Tunneling
- Quality of Service
- Peer-to-Peer Networking
- Dynamic Routing
- Source Routing
- Connectionless Services
- Unique Addressing
- Hierarchical Addressing

5.3.10.1 Client Services

Guidelines

- The implementation of IPv6 in Windows XP and Windows Server 2003 is a dual stack architecture, with separate protocol components for IPv4 and IPv6. Microsoft provides support for IPv6 implementations for Windows Server 2003, Windows XP with Service Pack 1 (SP1), Windows XP with Service Pack 2 (SP2), and Windows CE .NET 4.1 and later. The next generation TCP/IP stack for Windows is a single protocol component. Microsoft's next generation Windows operating system for the desktop is Windows Vista, and for the server is Windows Server "Longhorn". Further guidance can be found at: http://support.microsoft.com/?kbid=817778 and http://www.microsoft.com/technet/community/columns/cableguy/cg0905.mspx#ECAA, respectively.

Standards

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server - Longhorn
- Dual Stack Transition Mechanism (DSTM)

Guidelines

- DSTM provides IPv6 only networks the ability to reach IPv4 only networks, reducing the need to configure IPv4 addresses and routes within your IPv6 network. DSTM can work in conjunction with DHCP. There is further guidance for DSTM in RFC 4241 (http://www.faqs.org/rfcs/rfc4241.html).

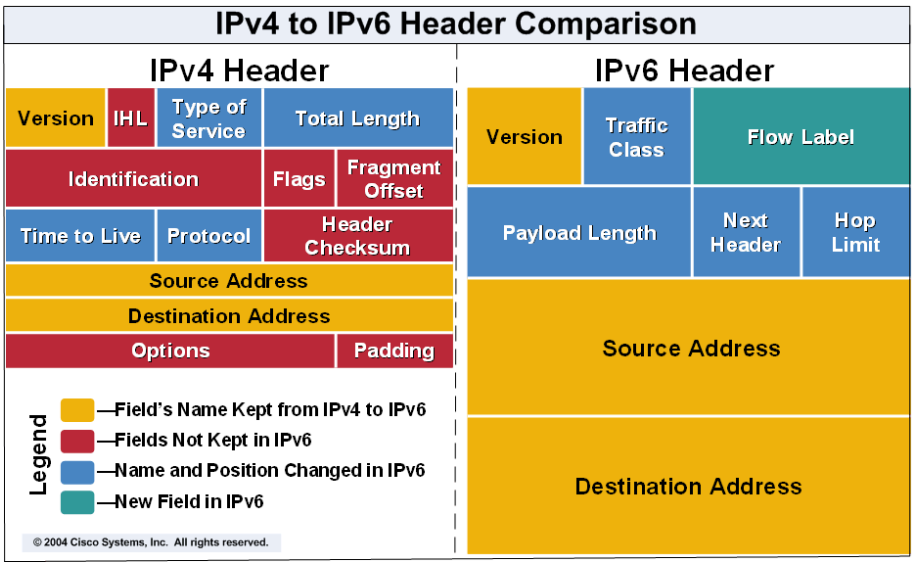

Figure 7 - IPv4 to IPv6 Header Comparison

Standards

- Network Interface (RFC 2472), at http://www.faqs.org/rfcs/rfc2472.html
- Prefix Delegation (RFC 3633), at http://www.faqs.org/rfcs/rfc3633.html
- Address Assignment (RFC 2461), at http://www.faqs.org/rfcs/rfc2461.html
- Routing (RFC 4241 ss 2.5), at http://www.faqs.org/rfcs/rfc4241.html
- Monitoring (RFC 4241 ss 2.8), at http://www.faqs.org/rfcs/rfc4241.html
- Security (RFC 4241 ss 4), at http://www.faqs.org/rfcs/rfc4241.html
- Dynamic Host Configuration and Domain Name Services (DHCP/DNS)

Guidelines

- DHCP is currently the standard host configuration protocol for TCP/IP. DHCPv6 is the emerging standard for host configuration on networks running IPv6. Further guidance on

DHCPv6 can be found in RFC-3315 (http://www.faqs.org/rfcs/rfc3315.html), and on DNS in RFC-3646 (http://www.faqs.org/rfcs/rfc3646.html).

Standards

- Dynamic Addressing (RFC 3646), at http://www.faqs.org/rfcs/rfc3646.html
- Stateless Addressing (RFC 3736), at http://www.faqs.org/rfcs/rfc3646.html
- Stateful Addressing
- Classless Addressing – CIDR
  - RFC 1518, at http://www.faqs.org/rfcs/rfc1518.html
  - RFC 1519, at http://www.faqs.org/rfcs/rfc1519.html
- Network Address Translation (NAT) (RFC 2766), at http://www.faqs.org/rfcs/rfc2766.html
- Virtual Private Networking (VPN)

Guidelines

- The current process for VPNs with IPv6 is to tunnel over an MPLS IPv4 backbone. Currently there is no ability to establish an MPLS IPv6 backbone. There is the ability to Overlap IPv6 VPNs through VRF.

Standards

- Transport Mode (RFC 3884), at http://www.faqs.org/rfcs/rfc3884.html
- Tunnel Mode (RFC 3456), at http://www.faqs.org/rfcs/rfc3456.html
- Multiple Protocol Label Switching (MPLS)

Guidelines

- With MPLS forwarding, the initial router labels the packet and assigns it to a FEC. Thus, subsequent routers do no additional header analysis, because the packet label drives all forwarding. This has a number of advantages over conventional network layer forwarding. Additional guidance on this MPLS can be found in RFC 3031 (http://www.faqs.org/rfcs/rfc3031.html).

Standards

- Forwarding Equivalence Class (FEC)
- Label Distribution Protocol (LDP)
- Label Merging
- Label Swapping
- Loop Detection
- Loop Prevention
- Edge Node

- Egress Node
- Ingress Node
- Security and IPsec

Guidelines

- Guidelines and Standards for IPv6 Security are still under review.

Standards

- Authentication (RFC 1826), at http://www.faqs.org/rfcs/rfc1826.html
- Encryption (RFC 2410), at http://www.faqs.org/rfcs/rfc2410.html
- Transport Mode (RFC 3884), at http://www.faqs.org/rfcs/rfc3884.html
- Tunnel Mode (RFC 3456), at http://www.faqs.org/rfcs/rfc3456.html
- Public Key Infrastructure (RFC 2585), http://www.faqs.org/rfcs/rfc2585.html
- Network Address Translation (NAT) (RFC 3715), at http://www.faqs.org/rfcs/rfc3751.html
- Teredo (http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx)

5.3.10.2 Performance

IPv6 performance test should be considered as a first step in creating a baseline, not only for all future IPv6 testing but also to understand any performance differences that may exist in any device that forwards IPv4 and/or IPv6 traffic. These performance tests should not be limited to Quality of Service (QoS), but should also include Quality of Experience (QoE), to show clear delineation between what is happening on the network, and what the end-user is experiencing. The Internet Engineering Task Force (IETF) Request for Comments (RFC) associated with IPv6, and referenced in this document, are listed below.

RFC	Title
1518	Architecture for IP Address Allocation with CIDR
1519	Classless Inter-Domain Routing (CIDR)
1825	Security Architecture for IP
1826	IP Authentication Header
2410	NULL Encryption Algorithm and IPsec
2460	Internet Protocol Version 6 (IPv6) Specification
2461	Neighbor Discovery for IPv6
2472	IPv6 over Point-to-Point Protocol (PPP)
2474	Definition of DF Field in IPv4 and IPv6 Headers
2585	PKI Operational Protocols: FTP and HTTP

RFC	Title
2764	Framework for IP Based VPNs
2766	Network Address Translation - Protocol Translation
3031	Multiprotocol Label Switching Architecture
3315	Dynamic Host Configuration Protocol version 6 (DHCPv6)
3456	IPsec Tunnel Mode for IPv4
3633	IPv6 Prefix Options for DHCPv6
3646	DNS Configuration Options for DHCPv6
3647	PKI Certificate Policy and Certification Framework
3715	IPsec NAT Compatibility Requirements
3736	Stateless DHCP for IPv6
3814	MPLS FEC to NHLFE MIB
3815	MPLS LDP
3884	IPsec Transport Mode for Dynamic Routing
4213	Basic Transition Mechanisms for IPv6 Hosts Routers
4221	MPLS Management Overview
4241	Dual Stack Internet Access Service IPv6/IPv4

6 Appendix - Patterns

A pattern is a design with prescriptive constraints that may apply to one or more TRMSP layers.

6.1 Wide Area Network

The VA EA is undergoing rapid and large-scale changes in its logical and physical topologies. The Telecommunications Modernization Project (TMP) represents state-of-the-art technology that is simple to administer and maintain using technology as the enabler. The TMP Mission is:

> *To provide state-of-the-art telecommunications infrastructure that transports information consistently, reliably, and accurately in a secure manner for veterans and their families, employees, and stakeholders. In parallel, TMP will improve telecommunications performance while providing service across all VA business lines at a competitive price. In this manner, veterans and their families, employees, and stakeholders will be assured that information will be delivered to the right place, at the right time, and in the right format.*

The project is being implemented in phases as follows: Phase I – Replacement of obsolete network equipment; Phase II – Reduction of unnecessary circuits; Phase III – Optimization of core and distribution layers; and Phase IV – Optimization of Access layer. The TMP is currently in its final phase (IV) which optimizes the fourth and final hierarchical layer of the TMP network design, or Access layer. This layer is composed of VA's major remote locations, i.e., medical centers, remote facilities, campus facilities, etc. The Phase IV initiative involves the extension of IP based services to these locations to complete the TMP integrated One VA network structure. The TMP Region 5 (VISN5) geographic area was selected to conduct a TMP Proof-of-Concept pilot as the first step in this process.

The VA Enterprise WAN is based on a three-layer hierarchy—Core, Distribution and Access—consisting of four Sprint hosted core routers, approximately 50 distribution routers for various regions (geographic) and corporate data centers. Each of the 19 regions consists of a number of access routers that provide L2 WAN campus interface into the enterprise network.

The access layer is the point at which local end users are allowed into the network. This layer may use access lists or filters to further optimize the needs of a particular set of users. In the campus environment, access-layer functions can include the following: shared bandwidth, switched bandwidth, MAC layer filtering and micro-segmentation. In the non-campus environment, the access layer can give remote sites access to the corporate network via wide-area technology, such as ATM, Frame Relay, ISDN or leased lines.

Access nodes that are classified as critical to business operations will be dual homed to increase their availability. These access nodes will have a connection to each one of the distribution nodes in heir particular region. All access nodes will use the distribution nodes for traffic outside their Autonomous System.

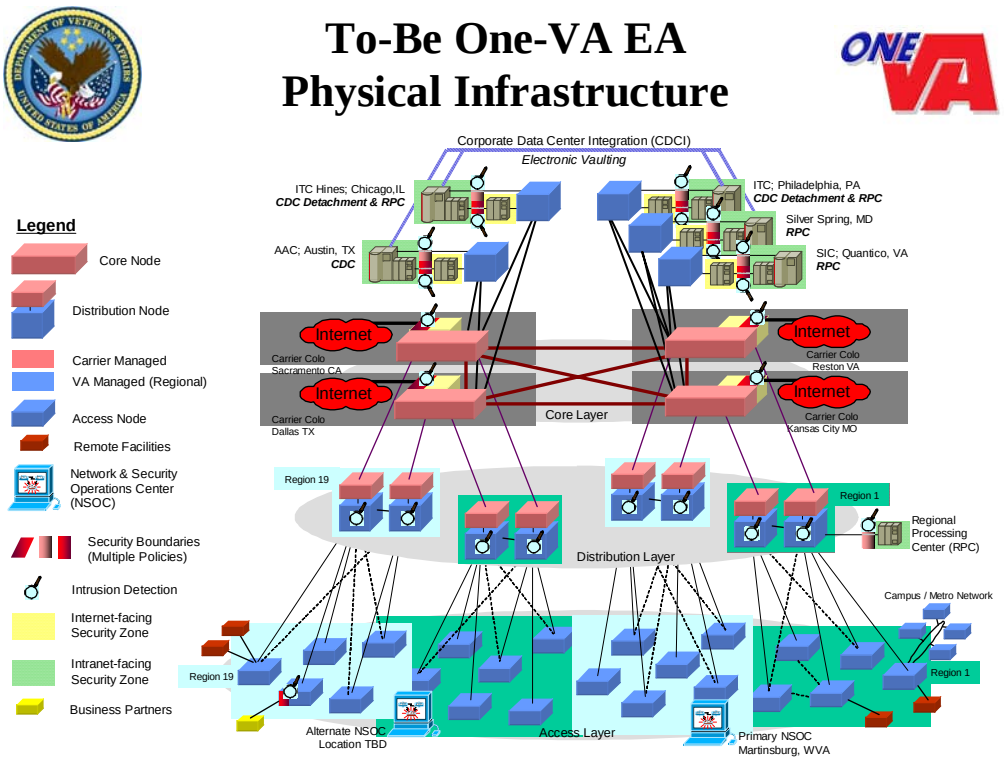

Figure 8 - "To Be" Physical Architecture

6.2 Local Area Network

Switching technologies that use layer 2 and 3 of the OSI model will provide the VA with a fast and reliable LAN backbone. The core, distribution, and access layer design will scale well for the growth the VA anticipates. The figure below depicts the three-layer LAN design model.

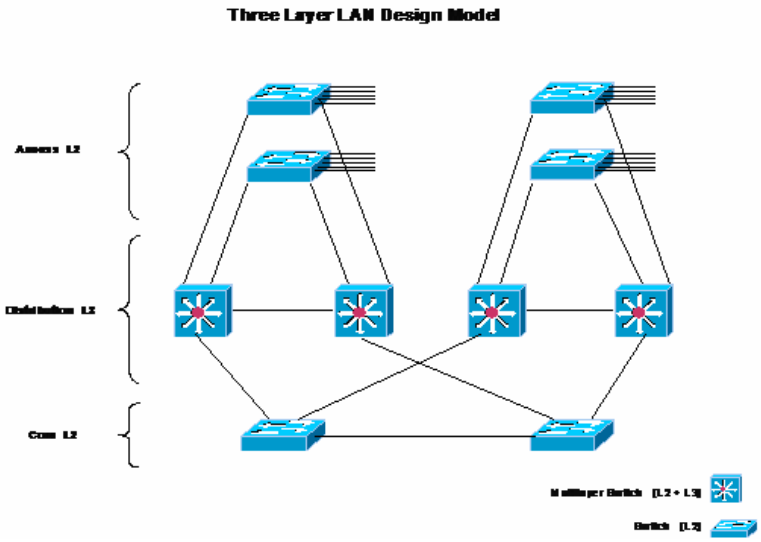

Figure 9 - LAN – Pattern

6.2.1 Access Layer

Access layer devices are based on layer 2 switching and replace the legacy role of layer 2 shared access hubs. Access layer devices provide workgroup/user access to the network and dedicated bandwidth to the user. Access layer switches also provide per port VLAN support, as well as trunking access to higher layer switches.

6.2.2 Distribution Layer

The distribution layer is the communication point between the access and core layers and can consist of layer 2 and layer 3 switches supporting 802.1q.

6.2.3 Core Layer

The core layer is dedicated to high speed switching, usually at layer 2, or switched layer 3. 100BaseT or 1000BaseT technology can be used as a foundation for the core backbone.

6.3 Campus Area Network

Numerous LAN technologies have been introduced to keep pace with the parallel growth of desktop, server, and shared services available across the campus infrastructure. With the convergence of voice, video, and data, coupled with the introduction of wireless LANs, campus infrastructure design and upgrades have become more complicated. The multilayer model is recommended for enterprise campus designs. This model combines the scalability and stability of traditional models with the benefits of the campus-wide VLAN model. This approach takes advantage of hardware based layer 3 routing and switching capabilities of the multilayer switch, while using the traditional VLAN switching capabilities of the layer 2 switches. Layer 4 switches are capable of identifying which application protocols are included with each packet, and use this information to hand off the packet to the appropriate higher-layer software. *Figure 10 – CAN - Pattern* shows the multi-layer model.

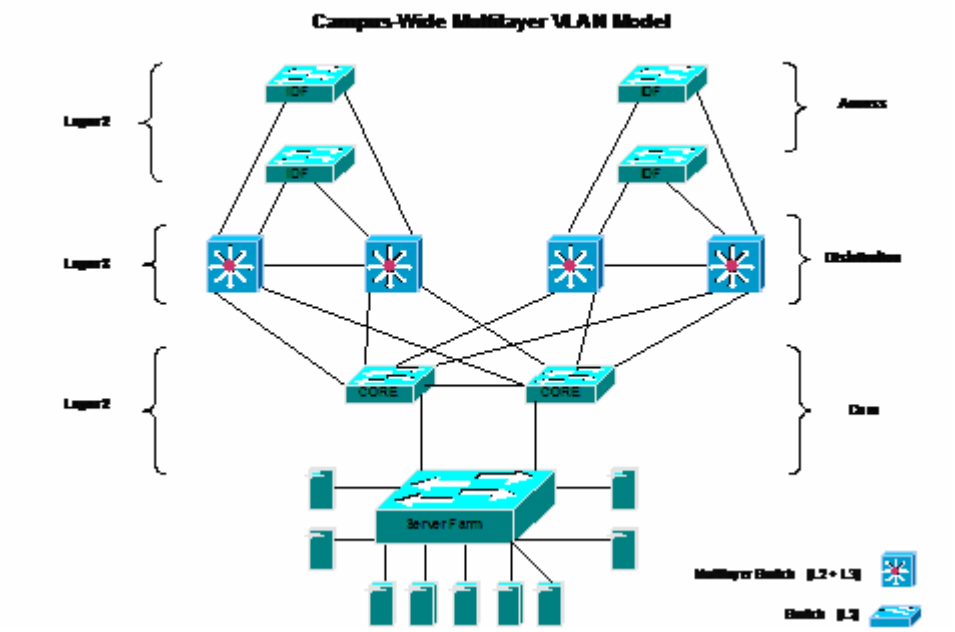

Figure 10 – CAN - Pattern

6.3.1 Access Layer

Access layer devices are usually deployed in wiring closets and provide direct connection to the end user. Access layer is generally based on layer 2 switching. Access layer switches provide per port VLAN support, as well as trunking access to higher layer switches.

6.3.2 Distribution Layer

Distribution layer devices may be made up of a combination of layer 2 switches and higher supporting 802.1q. Depending on the switch capability, multilayer switches can integrate layers 2, 3, 4, and beyond into a single chassis. A multilayer switch can handle Layer 2 functions as well as the Layer 3 and Layer 4 functions that have traditionally been found on a router.

6.3.3 Core Layer

Core layer devices are dedicated to high speed switching, usually at layer 2, or switched layer 3. 1 Gigabit or 10 Gigabit technologies can be used as a foundation for the core backbone. Core layer devices can connect to a farm of networked servers that are housed in one location. A server farm streamlines processes by distributing the workload between the individual components of the server farm while using the power of multiple servers.

6.4 Wireless LAN Architecture Pattern

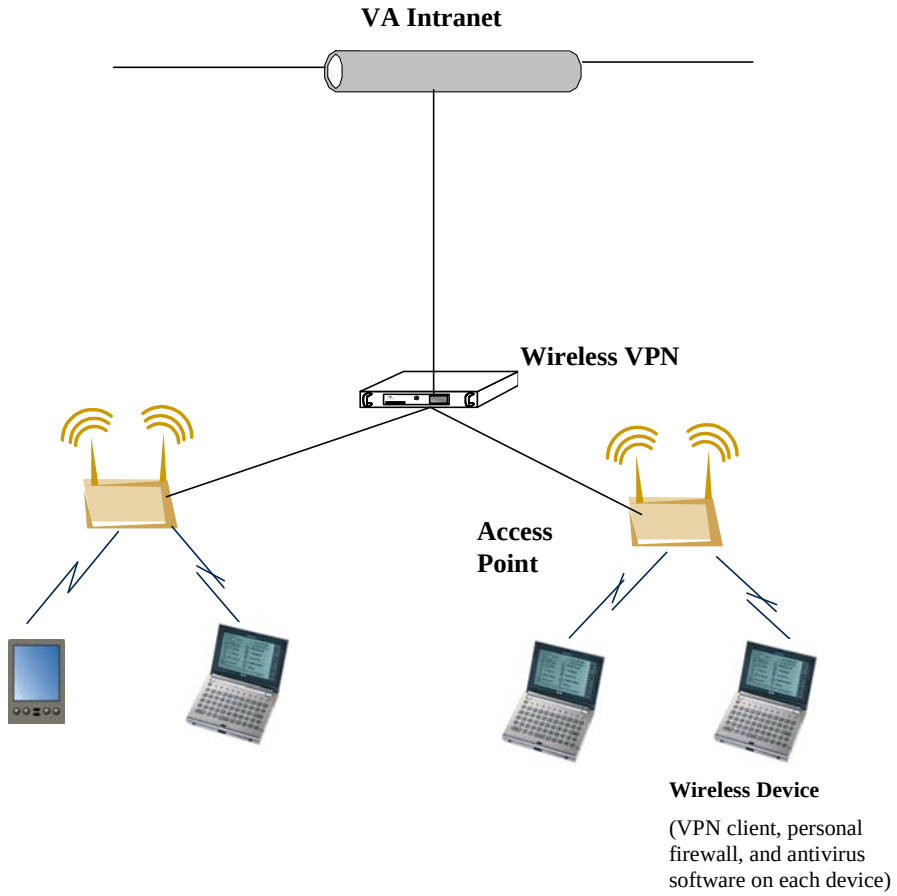

Figure 11 - Wireless LAN Pattern

6.5 Internet/Intranet Gateway (firewall, DMZ, VPN)

The Tier 1 CDC and RPC Security Zone shows the Internet-facing and Intranet-facing zones protected by Firewall, content filtering and IDS systems. Within these security zones services are provided to customers based on access control policies.

The Core Node Gateways are depicted in the lower portion of *Figure 12 - Tier 1 Gateways and Security Zones Target Architecture*. Here they show the boundary protection designed to meet the everyday threat from the Internet and other external networks. Within this depiction, the VPN-based secure access solution for Business Partners and RAS users is also shown distinguishing between the two uses of VPN tunneling; one to service VA staff and contractors accessing the VA Intranet securely from outside the perimeter of the One-VA Intranet via dialup or broadband access, and another to show business partner gateways subjected to more restrictive security policies tailored to the nature of the specific business partner relationship that exists.

Figure 12 - Tier 1 Gateways and Security Zones Target Architecture presents the establishment of One-VA VPN services. These VPN services will be employed to enable RAS services across external networks by enabling a cryptographic tunnel from a remote client to the corporate intranet through the carrier collocated Gateway location, or also to enable trusted interface channels with external organizations such as other governmental entities (e.g., the Department of Defense, the Internal Revenue Service, the Social Security Administration) or with suppliers in a Supply Chain Management (SCM) environment.

VPN services are also provided to dedicated business partners. These connections are established with key VA business partners and will replace current local gateways to external networks. Generally these connections are dedicated, private, high-bandwidth connections to transmit data, such as medical imagery, patient data, or medical research data between VA and non-VA facilities. The ECSIP program office specifies the supporting infrastructure for these connections. Actual procurement and installation is the responsibility of the VA agency and its business partner. However, the connection will be centrally monitored and managed by the NSOC.

The design depicted in *Figure 12 - Tier 1 Gateways and Security Zones Target Architecture* also provides external DNS, content and antiviral scanning, web caching, reverse proxying of internal web servers, One-VA-VPN (external remote VA users and trusted business partners), combined with multiple IDS, firewall and routing technologies providing a defense-in-depth architecture. As the deployment of corporate gateway capability is executed, backside Internet gateways on a local and regional basis will be taken down and their traffic rerouted over the intranet to use the corporate gateways. Upon completion of this process, no Internet gateways other than the four Enterprise Core gateways will be permitted to operate. Additionally, where appropriate, local or regional business partner gateway interactions will also be shifted to the core gateways and the local or regional business partner gateways shut down except where the nature of the business partner interactions and local infrastructure dictate otherwise.

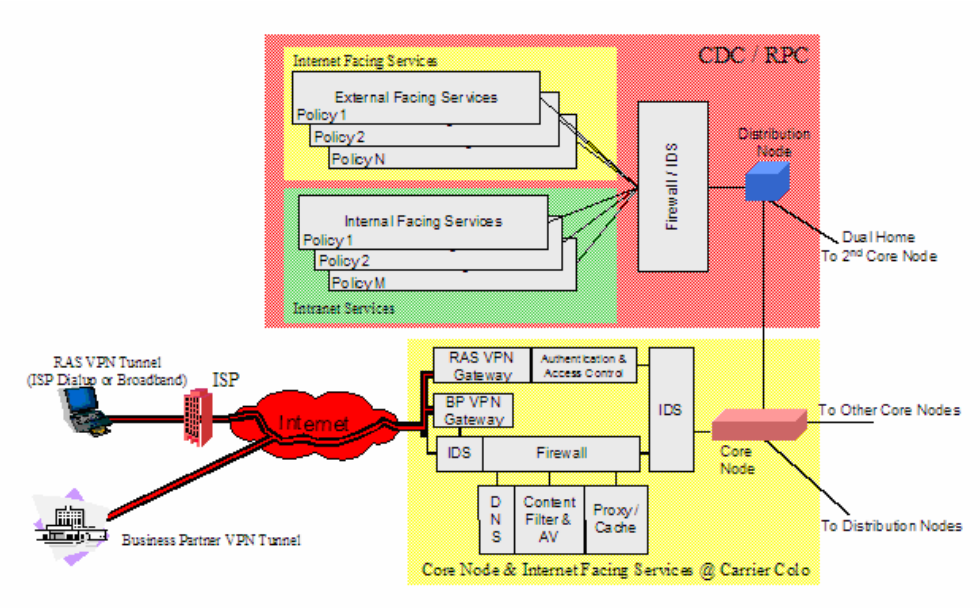

Figure 12 - Tier 1 Gateways and Security Zones Target Architecture

6.6 Java Application Architectures

The following pattern briefly outlines several example architectures implemented using the Java language specification (J2SE & J2EE) to build applications. As depicted in *Figure 13 - Java Application Architecture* the highest level divides the application into three tiers: Client, Middle, and Data.

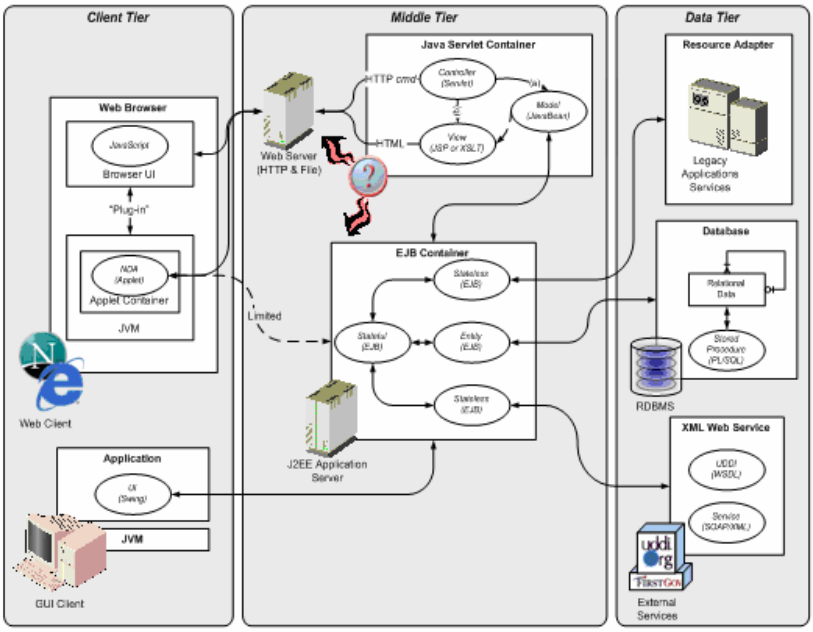

Figure 13 - Java Application Architecture

6.6.1 Client Tier

In this example architecture, the client tier is the logical layer of a distributed system that presents data to and captures input from the user through a Graphical User Interface (GUI). The example illustrates three options for building GUIs: web-client, network delivered application (NDA), GUI Application.

6.6.1.1 Web Client

A Web Client is the presentation portion of an application that is almost completely implemented in the middle tier. The only logic that is executed locally is written in JavaScript, which is used for simple tasks that enhance the user's experience (i.e., interactive menus for navigation, simple data validation for forms, simple graphics animation (rollovers) for esthetics, etc.). Since these clients contain so little logic, they are also referred to as thin-clients.

Technologies	Purpose
Cascading Style Sheet (CSS)	Used to format the HTML without embedding formatting tags in the document that further helps create a consistent look-n-feel across a site.
HyperText Markup Language (HTML)	Used to describe the document's structure so that the web browser can properly present it.
Hypertext Transfer Protocol (HTTP)	Used to connect the web browser to the web server and exchange information.
Hypertext Transfer Protocol, Secure (HTTPS)	Used to transmit documents in a secure manner be using a Secure Sockets Layer (SSL) or the newer Transport Layer Security (TLS).
JavaScript	Used to encode the limited process logic at the client's machine.
Web Browser	A commercial product that consistently formats the HTML into a User Interface (i.e., Internet Explore, Netscape Navigator, Opera, etc.).

Advantages:

- Portability

Disadvantages:

- Limited Local Logic

6.6.1.2 Network Delivered Application (NDA)

These applications are a special case of a Web Client where the HTML page contains a set of special tags (<APPLET>…</APPLET>) that trigger the NDA. These tags define a "window" within the page where a Java Applet can be run using the Java Virtual Machine (JVM) as a plug-in. The web browser begins the process by downloading the Applet, which can consist of a single class file or many files stored in a Java Archive (JAR) file; hence the term Network Delivered Application. It then passes control of that "window" along with any parameters defined by the <PARAM> tags to the JVM where the applet executes its life cycle, which corresponds to the five key applet methods:

- Init() - executes once at initialization when the applet is loaded
- Start() - executes when the applet becomes visible
- Stop() - executes when the applet becomes invisible
- Destroy() - executes once when the browser exits
- Paint() - executes each time the applet frame needs to be displayed

These types of applications are gaining in popularity because they have most of the advantages of a GUI Application without the drawbacks of distributed installation and administration. However, due to an applet's security limitations, they are generally restricted from:

- Loading libraries or defining native methods
- Reading or writing local files
- Making network connections to any server except for its host
- Starting a local program
- Reading most system (local) property

Some of these limitations can be overcome by signing the applet, which can grant it extra privileges.

Technologies	Purpose
HyperText Markup Language (HTML)	Used to define where in the page the applet window runs and any of its startup parameters.
Hypertext Transfer Protocol (HTTP)	Used to deliver the applet to the client, optionally in a secure (HTTPS) manner.
J2SE Applet	The specific packages that enable the application to interact within the browser & HTTP Server and exposes its life cycle events.
Java 2 Enterprise Edition (J2EE)	The packages that enable the application to interact with middle or data tier resources (i.e., JDBC, JAX-RPC, JDNI, etc.) assuming they are running on the same host or the applet is signed.
Java 2 Standard Edition (J2SE)	The collection of packages that provide higher-level functionality to the Java language (i.e., presentation items, remote procedure calls, interactions with the JVM, etc.).
Java Virtual Machine (JVM)	A commercial product for the runtime plug-in that interprets the compiled Java byte-codes stored in a ".class" file. However, the plug-in must be downloaded and installed separately depending on the operating system (see a recent court ruling that requires Microsoft to distribute Sun's latest VM with Windows), regardless it free and widely available.
Web Browser	A commercial product that consistently formats the HTML into a User Interface (i.e., Internet Explore, Netscape Navigator, Opera, etc.).

Advantages:

- Portability
- Locally Executed Logic
- Central Administration

Disadvantages:

- Bandwidth Intensive
- JVM Installation

6.6.1.3 GUI Application

Functionally, these programs are very similar to the Java Applets without any of the security limitations. Technically, they differ by (a) having a separate life cycle, (b) running outside of a web browser, and (c) are installed permanently on the user's local machine. Since these clients are installed locally and contain processing logic, they are also referred to as fat- or heavyweight-clients.

Technologies	Purpose
Java 2 Enterprise Edition (J2EE)	The packages are used exclusively to enable the application to interact with middle or data tier resources (i.e., JDBC, JAX-RPC, JDNI, etc.) they are not meant enabling transaction processing in the client tier. Also, the draft of the next J2SE specification is moving them into the standard edition.
Java 2 Standard Edition (J2SE)	The collection of packages that provide higher-level functionality to the Java language (i.e., presentation items, remote procedure calls, interactions with the JVM, etc.).
Java Virtual Machine (JVM)	The runtime application that interprets the compiled Java byte-codes, which is stored in a ".class" file. However, the plug-in must be downloaded and installed separately depending on the operating system (see a recent court ruling that requires Microsoft to distribute Sun's latest VM with Windows), regardless it free and widely available.

Advantages:

- Portability
- Rich Interactive UI

Disadvantages:

- JVM & Application Installation
- Distributed Administration

6.6.2 Middle Tier

In this example architecture, the middle tier is the logical layer of a distributed system between the client and data tiers where business objects are instantiated. This tier is a collection of business rules and functions that generate and operate upon information. The example shows the three typical enabling technologies: web server, Java servlet container, and EJB container.

6.6.2.1 Web Server

This technology component is a commercial product that bridges the gap between the web clients and the various levels of application logic. Its basic functionality is to provide static content (HTML files & Images) in response to a web browser's HTTP(S) GET or POST request for a specific Uniform Resource Identifiers (URIs; a.k.a. URLs). The content for these requests are stored in a file server's directory structure that can be on the same server as the host, but not necessarily. By default, the web server monitors Port 80 (unsecured) and Port 443 (secured) for these requests; however, the ports can be overridden on the HTTP request.

Setting up URI pattern matching that directs the HTTP request to another process can extend the Web Server's functionality. In the case of Java based services, these requests are directed to a Java Servlet Container.

Technologies	Purpose
Web (HTTP) Server	A commercial product that is used to service the HTTP request from a web browser (i.e., Microsoft's Internet Information Server, Sun's ONE Web Server, Apache's HTTP Server, etc.).

6.6.2.2 Java Servlet Container

A container that implements the Java Servlet & Java Server Page component contracts of the J2EE architecture, which specifies a runtime environment for them and includes the following services:

- Instantiates the servlet
- Invokes the init method to initialize a servlet
- Invokes the service method to respond to requests from the user
- Invokes the destroy method to destroy the servlet
- Manages a similar life cycle for JSP files
- Deploys and creates Web Archive (WAR) files

6.6.2.2.1 Java Servlet Technology

Java servlet technology provides Web developers with a simple, consistent mechanism for extending the functionality of a Web server and for accessing existing business applications. The servlet technology provides a component-based, platform-independent method for building Web-based applications, without the performance limitations of Common Gateway Interface (CGI) programs.

6.6.2.2.2 Java Server Pages (JSP) Technology

JSP is a presentation layer technology that sits on top of the Java servlets model—JSPs are actually pre-compiled into servlets. It allows developers to rapidly develop and easily maintain information-rich, dynamic pages that leverage existing business applications. The technology's approach differs from the servlets' component-based approach by being page-centric where the Java code is embedded around the HTML. This approach makes it easier to combine fixed or static template data with dynamic content.

A well-designed Web Application will take advantage of each technology's strengths. Servlets and JSPs focus on different types of programming problems, where servlets are process-centric and JSPs are document-centric. The Model-View-Controller design pattern lends itself to exploiting these strengths.

6.6.2.2.3 Model-View-Controller (MVC)

The MVC design pattern is used to separate the application logic (model) from the way it is presented to the user (view) from the way it is invoked (controller).

The controller component is the centralized traffic-cop between the user and the application; it knows how to map a user's request to the application's components. Additionally, since it centralizes all requests, it is easy to extend through a Command Pattern (encapsulating and parameterizing requests) or Intercepting Filter Pattern (pre- or post-processing requests). The model components know all about the data and how to manipulate it. However, it knows nothing whatever about the GUI, the manner in which the data are to be displayed, nor the GUI actions that are used to manipulate the data. The data are accessed and manipulated through methods that are independent of the GUI.

The view transforms the model's raw data into a presentation format. Typically, there are many views of the same data, which can be used to support different physical devices or different GUI formats.

Technologies	Purpose
Extensible Markup Language (XML)	This tag-based markup language can be used as the communications format between the Model and View components, which would allow XLST to easily format it.
Extensible Stylesheet Language Transformations (XSLT)	A standard for transforming XML documents into other formats, in this case HTML.
J2SE & J2EE Implementations	These are commercial software development kits (SDKs) and run-time implementation of the Java2 Standard Edition (J2SE) and Enterprise Edition (J2EE) specifications. For example, IBM's Developer Kit Package, Sun's Java2 Platform, Standard & Enterprise Edition, etc.
Servlet Container	A commercial product that is used in conjunction with the Web Server to execute the Java code. The application that is the servlet container is sometimes an integrated component of either the Web Server or the J2EE Application Server. Otherwise, it can be an in or out of process addition to a third-party server. Examples of standalone products include Jakarta's Tomcat (open-source), Mort Bay's Jetty (open-source),

Technologies	Purpose
	etc.

6.6.2.3 EJB Container

A container that implements the Enterprise JavaBean (EJB) component contract of the J2EE architecture, which specifies a runtime environment for EJBs that includes concurrency, deployment, life cycle management, security, transaction, and other services. There are three kinds of enterprise beans: session beans, entity beans, and message-driven beans.

- **Session Bean** – An EJB created by a client and that, normally, exists only for the duration of a single client-server session. A session bean is not recoverable in the event of a system crash, even though it may be transactional. Session bean objects can be stateless or stateful—maintaining conversational state across methods and transactions. If they do maintain state, then the EJB container manages this state if the object must be removed from memory.
- **Entity Bean** – An EJB that represents persistent data maintained in a database and identified by a primary key. Entity bean persistence can be managed either by the bean itself or its container (Container Managed Persistence-CMP). If the host container of an entity bean crashes, the entity bean, its primary key, and any remote references survive the crash.
- **Message Bean** – An EJB that is similar to a stateless session bean, but it does not have public interfaces; instead it is associated with a JMS topic or queue and is triggered by receiving a JMS messages sent by EJB clients or other beans.

Technologies	Purpose
EJB Container	A managed runtime environment for EJBs that includes concurrency, deployment, life cycle management, security, transaction, and other services.
J2EE Application Server	These commercial products provide the managed environments – containers – for various J2EE components. For example, BEA's WebLogic, IBM's WebSphere; Sun's ONE, JBoss (Open-Source), etc.
J2SE & J2EE Implementations	These are commercial available software development kits (SDKs) and run-time implementation of the Java 2 Standard Edition (J2SE) and Enterprise Edition (J2EE) specifications. For example, IBM's Developer Kit Package, Sun's Java2 Platform, Standard & Enterprise Edition, etc.

6.6.3 Data Tier

In this example architecture, the data tier is the logical layer of a distributed system that maintains persistent data. Additionally, it provides services to interact with legacy applications to integrate their functionality (logic & data) into the enterprise.

6.6.3.1 COTS & Legacy Systems Integration

Viewed 2-dimensionally, these systems would fall in both the middle tier (processing) and data tier. However, viewed 3-dimensionally where time ("as-is", transition, and "to-be") are added, the legacy systems become the "as-is" data providers for the "to-be" middle tier when their "as-is" technologies are being retired. Therefore, the integration approach is to follow the Java Connector Architecture (JCA) to isolate and abstract a specific set of functions and provide a standardized access methods. Additionally, the architecture proves several common functions:

- **Connection management** - supports connection pooling and management; optimizing application performance; and increasing scalability.
- **Transaction management** - supports the concept of all-or-nothing multiple operations, typically expressed as ACID (Atomic, Consistent, Isolation, and Durable).
- **Security management** – supports authentication and reliability – interacts with connection management.

Technologies	Purpose
J2EE Application Server	These commercial products provide the managed environments – containers – for various J2EE components (i.e., BEA's WebLogic, IBM's WebSphere; Sun's ONE, JBoss (Open-Source), etc.)
Resource Adapter	These are commercial available system level software drivers used by the EJB container to connect to the target system. It is available as a library and is used within the address space of the calling server. It implements the targeted system's side of the standard functions for connection, transaction, and security management. The adapter is analogist to a JDBC or ODBC driver for a database (i.e., COMPORSYS's connectors for CICS, IMS, or MQ; ASAP Solution's connector for SAP/R3, etc.)

6.6.3.2 Data Services

These Data services represent persistent information that's stored in a relational structured to enforce referential integrity rules. These rules preserve the defined relationships between tables when records are modified or deleted. Additionally, the data should be normalized to a minimum of third normal form (3NF) where

- **First normal form (1NF)** - eliminates duplicative columns from the same table.
- **Second normal form (2NF)** - removes subsets of data that apply to multiple rows of a table and place them in separate rows.
- **Third normal form (3NF)** - removes columns that are not dependent upon the primary key.

Technologies	Purpose
Container Managed Persistence (CMP)	Is the process of allowing the EJB Container to interface with the RDBMS to store and retrieve objects.

Technologies	Purpose
JBDC	The commercial products that implement the Java API for database access on a specific vendor's database where they are categorized by: • JDBC-ODBC Bridge - provides JDBC access via ODBC drivers where system drivers must be loaded on each client machine. • A native-API - converts JDBC calls into calls on the client API for the targeted database where system drivers must also be loaded on each client machine. • Pure Java Driver for Database Middleware - translates JDBC calls into the middleware vendor's protocol, which is then translated to a DBMS protocol by a middleware server. • Direct-to-Database Pure Java Driver - converts JDBC calls into the network protocol used directly by the DBMSs, allowing a direct call from the client machine to the DBMS server.
Relational Database Management System (RDBMS)	A commercial database management product following the relational model that allows the definition of data structures, storage and retrieval operations, and integrity constraints (i.e., Oracle's 9i, MySQL AB's MySQL (open-source), Microsoft's SQL Server, etc.)
Structured Query Language (SQL)	SQL is a standard interactive and programming language for getting information from and updating a database.

6.6.3.3 External Services

External services are functions supplied by entities outside of the VA's control and exposed through XML Web Services Technologies. These technologies are an emerging architecture for allowing applications to discover and access functional capabilities of other applications using Internet based standards. XML Web Services were designed from the beginning for the loosely coupled, inter-enterprise world of the Internet. Thus, they focus on 1) using Internet standard HTTP for transport through fire walls, 2) using XML as the standard data format, and 3) providing standard mechanisms for describing and finding available XML Web Services.

XML Web Services are most often used to link web applications such as E-Gov solutions, portals, or external web sites or e-systems. However, they can also be used to link to legacy applications and Message Brokers – tying together the web world and the message broker's integration of back-end applications. Unlike Message Brokers, XML Web Services generally provide direct synchronous connections between the client and server application, rather than asynchronous connection through a central hub.

Typically, three parties make up an XML Web Service transaction:

- Providers - deploy and publish services by registering them with the Broker using a UDDI API Web Service (UDDI, WSDL/SOAP)
- Brokers - maintain the registry of all available services using UDDI and WSDL/SOAP
- Requesters - bind to the Provider and consume the available services using SOAP

Technologies	Purpose
Simple Object Access Protocol (SOAP)	SOAP is a lightweight remote procedure call protocol that uses XML for message formats and HTTP for transport. A SOAP method is simply an HTTP request and response that complies with the SOAP XML encoding rules. A SOAP endpoint is simply an HTTP-based URL that identifies a target for method invocation. While SOAP is typically implemented as a synchronous protocol based on HTTP, it can be implemented over other transports such as sockets or messaging systems if more robust or asynchronous communications are required.
SOAP Listener	A commercial product or add-on to a HTTP Server that intercepts SOAP messages and forwards them to the processes for execution. For example, Sun's Web Services Developer Pack, IBM's Web Services Toolkit, etc
Universal Description Discovery and Integration (UDDI)	A commercial product that provides a registry of available XML Web Services that applications can search to find a desired service and obtain its reference location (URL). For example, Novell's Enterprise UDDI, HP's E-Speak, etc.
Web Service Description Language (WSDL)	WSDL provides an XML based description of XML Web Services and how to interact with them – it is the Interface Definition Language (IDL) of XML Web Services. WSDL Clients obtain the WSDL file for an XML Web Service from UDDI, parse the XML with an XML parser, and use the information and the URL to call the Web Service using SOAP. WSDL Servers take SOAP messages from the SOAP Listener, parse the XML, and pass the Web Service request to the server application.

6.7 Messaging Consolidation

The VA Exchange network is a critical component of the VA Enterprise. The VA Enterprise is co-dependent with the VA wide area network and component local area networks. These distinct infrastructures provide VA customers with operating functionality including essential office automation tools, electronic mail, connectivity to all VA resources, the Internet/Intranet and the resources of other Government agencies. Currently, the VA Enterprise is undergoing a migration from a Microsoft NT platform to a Microsoft Windows 2000/2003 platform, with the component infrastructures and their respective efforts at varying stages in migration lifecycles. The VA messaging infrastructure currently has over 200 sites, most with obsolete hardware. Although there are some exceptions, the hardware platform is several years past its expected life; most of it is more than eight years old, and the existing messaging system is failing rapidly as a result.

The migration/consolidation effort is being managed under a chartered effort by the VA NT Enterprise Workgroup. As established in the Conference Report, H.R. 2673, Consolidated Appropriations Act of 2004, which directs "VA to consolidate critical applications including all business/corporate applications, messaging, office automation, and relevant medical systems applications at no more than six sites nationwide for the purpose of providing business continuity capabilities between each site to ensure continuity of operations of mission critical VA activities" as outlined in the March 24, 2004 memorandum by the Department of Veteran's

Affairs Assistant Secretary for Information Technology. This effort is intended to reduce the number of Exchange servers and sites through the VA Enterprise; provide a centralized management capability for VA Messaging; and upgrade the VA Messaging Environment (Exchange) to Microsoft Exchange 2003.

Figure 14 - VA Messaging Consolidation Conceptual Design (Phase One) represents the consolidation conceptual design to achieve this goal in Phase One. This will reduce the number of Exchange sites by approximately 245 into a configuration of 24 sites identified as: Austin (RDPC), Hines (RDPC), Philadelphia (VBA)(RDPC), Salt Lake City (RDPC), Silver Spring (RDPC), Albany, Bedford, Brooklyn, Pittsburgh, Martinsburg, Durham, Dublin, Bay Pines, Mountain Home, Cincinnati, Detroit, Kansas City, North Little Rock, Mesa, Vancouver, Sacramento (Mather), Long Beach, Minneapolis and Quantico (NCA). This effort is mostly funded with the initial award made to GTSI on January 3, 2005 for IBM X-Series servers. Completion of this phase is anticipated by September 2005. All future acquisitions for in-progress efforts will be monitored and coordinated to ensure they will support the consolidation strategy.

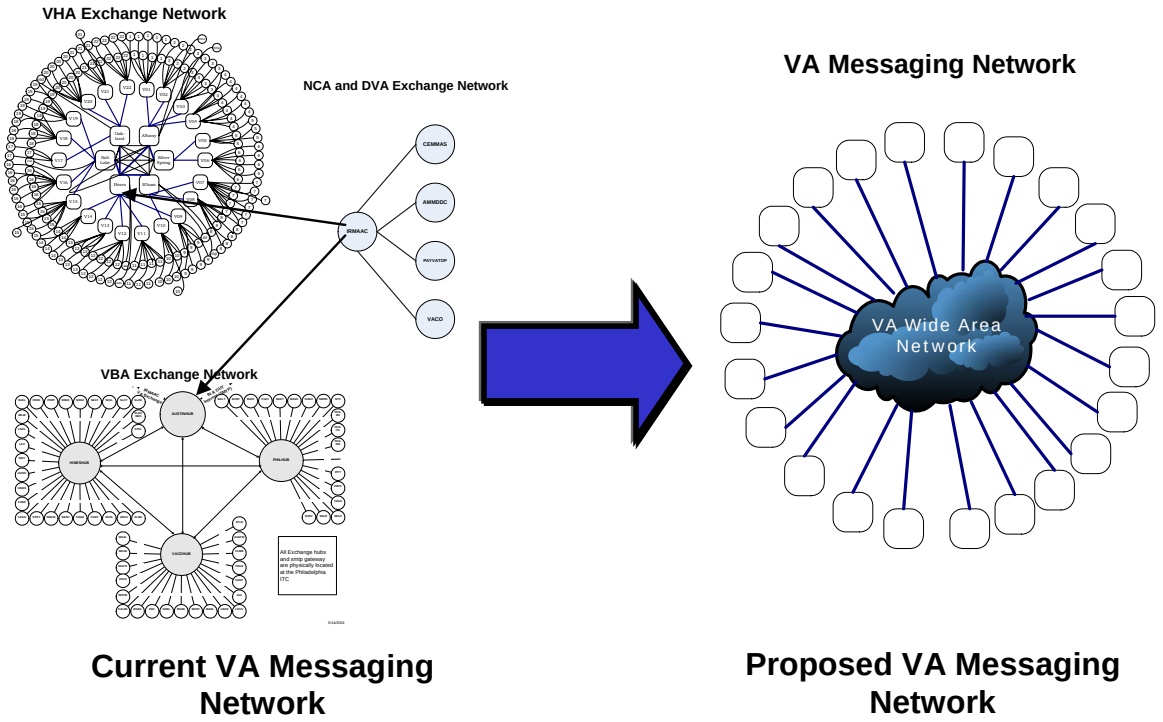

Figure 14 - VA Messaging Consolidation Conceptual Design (Phase One)

Phase Two, represented by Figure 2 (below) with further consolidate Messaging Services to six Regional Data Processing Centers (RDPCs). Standardization and manageability will be ensured during Phase II as well as Operations and Maintenance. This phase, which is unfunded, is expected to start during FY-05 and complete by September 2008. The final location of all RDPCs is pending.

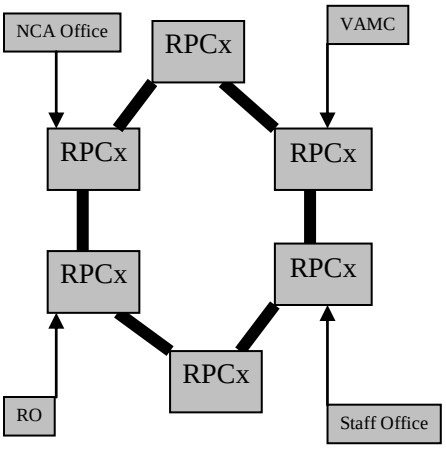

Figure 15 - Consolidation of Messaging Services to Six RDPCs (Phase Two)

6.8 Enterprise Telephony Agenda

The development of a Department-wide policy on future directions in telephony is essential to assure the survivability of VA's telephony infrastructure and operational capability; utilizing computer-telephone integration (CTI) to meet future VA business needs; assuring the cost effectiveness of VA's voice infrastructure investment; and assuring that VA's voice infrastructure can meet current and projected capacity and connectivity requirements. To support this effort, VA's Deputy Assistant Secretary for Information Technology Management chartered a VA Enterprise Telephony Council (ETC), an inter-administration working group. Their mission is to develop Department-wide policy on future directions in telephony. This will be accomplished by identifying and articulating VA business and Veteran service needs, which are impacted by voice transmission, and to develop and present appropriate technical solutions to the CIO for inclusion in a comprehensive telephony policy.

The ETC will address and investigate all matters concerning voice transmission capabilities and CTI by obtaining input and feedback from the VA community and understanding and acting upon issues and concerns voiced by the working group membership which relate to telephony and CTI policy. The figure below was included in this briefing as the "To Be" configuration.

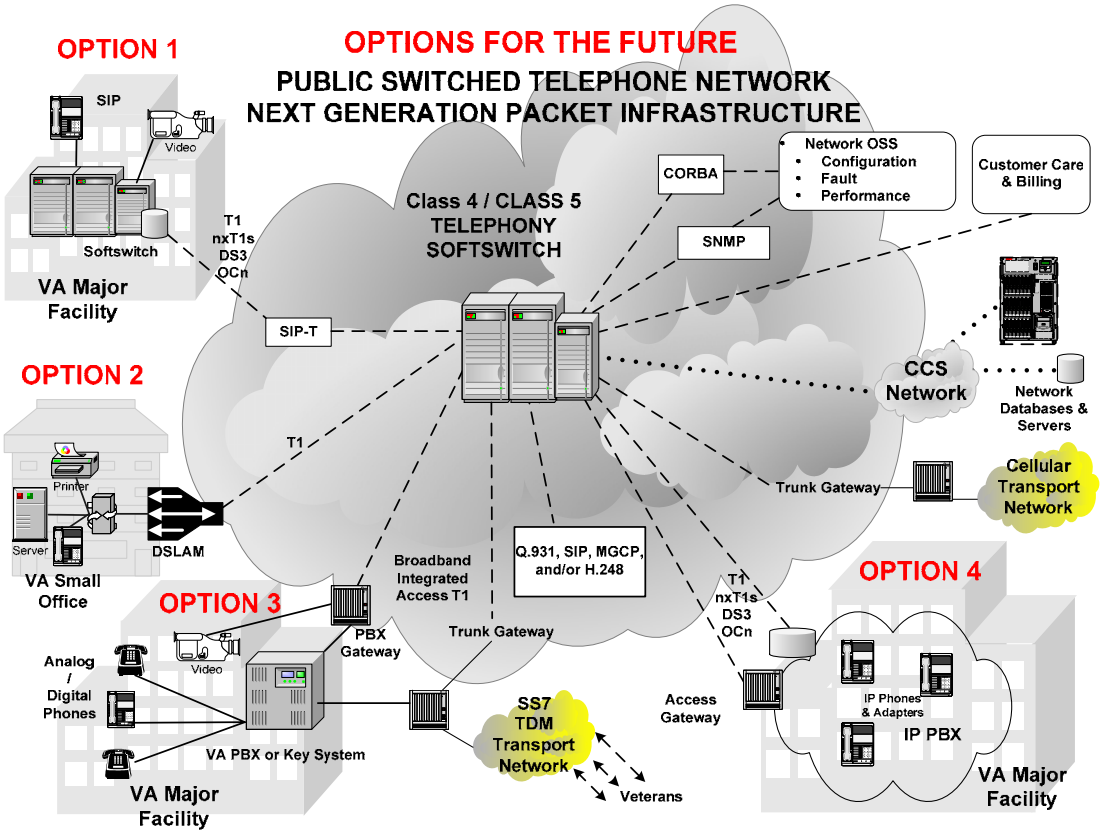

Figure 16 - PBX To-Be

The guiding principals of the ETA will be to:

- Develop solutions that are driven by VA strategic goals, VA business line requirements, and improvements in service to Veterans;
- Promote information and process consistency and reuse;
- Endorse interoperability, reusability and scalability and avoid redundancy in new technology investment and deployment;
- Promote the use of open standards and standards-based solutions, as opposed to proprietary solutions, in areas where standards-based products are mature, and, resort to broadly-based proprietary solutions only in areas where standards-based solutions have not developed; and
- Develop infrastructure that will integrate, with other VA business partners and Federal Departments.

Project Acquisition Strategy for the ETA involves Cost of Service assessments, voice infrastructure inventory update and cost benefit analysis activities from 1Q05 – 2Q06; field test VOIP telephony alternatives during 1Q06 – 2Q06; and system deployment during a two-phased acting during 1Q07 – 4Q08. Funding for the initial activities is anticipated during FY-05.

6.9 Wideband to Narrowband Radio Frequency Transition

Congress has mandated the National Telecommunications Information Administration (NTIA), of the Department of Commerce to establish and execute new goals and standards that ensure Federal government agencies use new land mobile technology and services, which encourage beneficial use of the radio frequency (RF) spectrum. To achieve this mandate, NTIA has directed that existing Federal government land mobile radio frequencies be transitioned from wideband 25 kilohertz (kHz) channels to narrowband 12.5 kHz channels. This will double the number of channels and accommodate more users.

Effective January 1, 1995, all orders for new or replacement radio equipment in the VHF and UHF frequency ranges must satisfy all NTIA narrowband standards. The target replacement schedule for VHF systems was January 1, 2005 and for UHF radio systems is January 1, 2008. Replacement refers to base station transceivers, controllers, pagers, hand-held items and mobile transceivers. This includes two-way radio equipment used by engineering, security, medical administrative staff, escort service and transportation as well as radio pagers used by medical personnel and administrative staff. During September 1998, VHA identified the final cost estimate of nearly $98 Million for VA to replace and upgrade VHA radio communication systems as a single project. This amount included site preparation, installation, certification and project management. As of January 2005, VHA has completed an average of 61.9% of all VHF equipment and 73.2% of all UHF equipment transitioned. VBA has one frequency and has completed the transition. As of December 31, 2004, NCA is 66.39% complete.

The charts below provide a graphic representation of the allocated frequency space that is achieved through this conversion process.

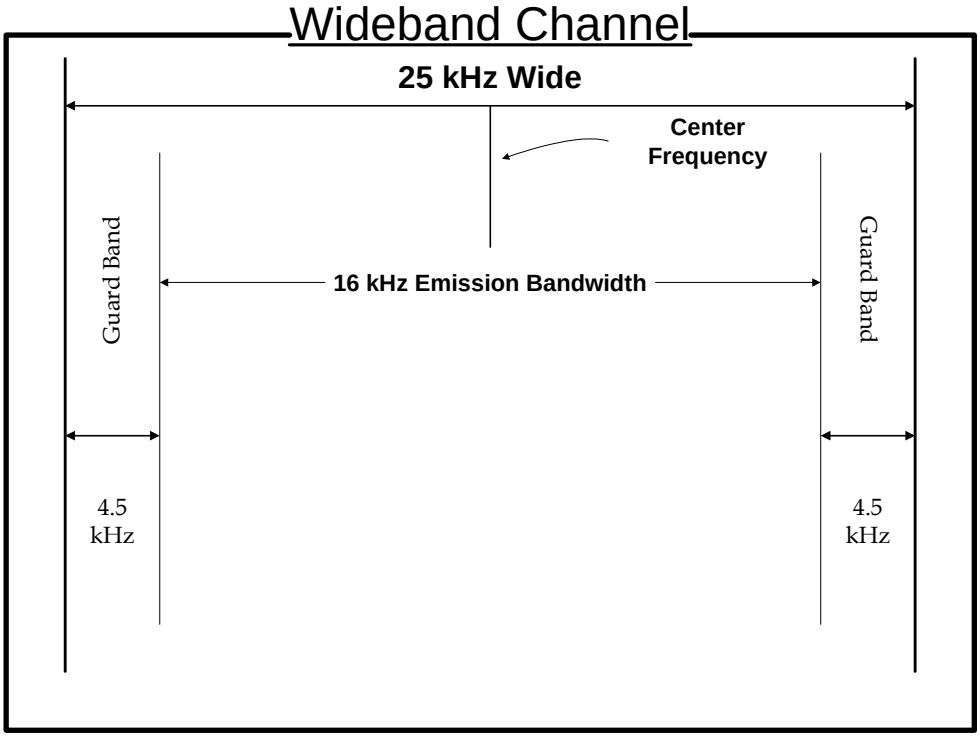

Figure 17 - Wideband Channel

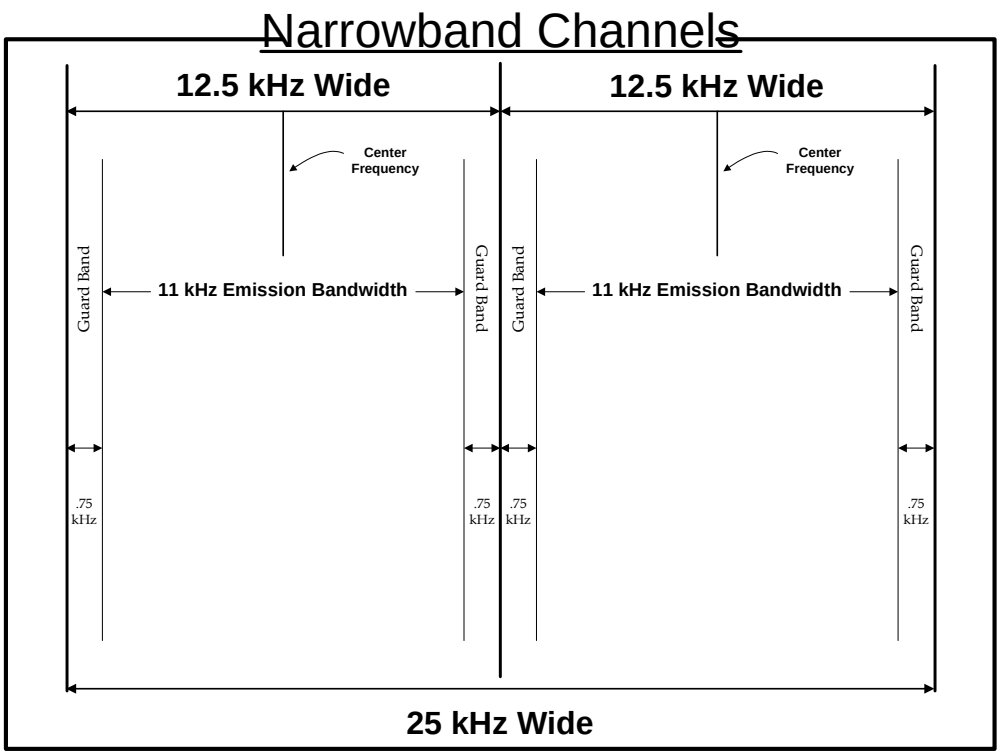

Figure 18 - Narrowband Channels

7 Appendix - Management & Planning Processes

These processes control the configuration of software components, test data, and libraries. This includes change control, versioning, release management, and requirements traceability.

Goals

IT Goal 1: Implement One-VA Enterprise Architecture.

- These technologies support a services based, component architecture thereby allowing common functionality to be consolidated into a single source.
- These technologies support loosely coupling of heterogeneous legacy systems thereby unifying business functions.
- These technologies are based on open interface standards that are compliant with FEAPMO guidelines thereby allowing VA to participate in E-GOV initiative with a unified front.

IT Goal 2: Implement a One-VA data network.

- These technologies are based on open, industry standards communications protocols thereby eliminating the need for proprietary networking hardware or software.

IT Goal 3: Secure the One-VA enterprise against Cyber Attack.

- These technologies ensure the integrity of artifacts through signature, auditing, and authentication for user access and automated as well as manual updates.
- These technologies can support a unified authentication and authorization service thereby enabling Cyber Security's Single Sign On (SSO) and Access Control functions.

IT Goal 5: Establish effective metrics to measure performance.

- These technologies establish a common technical baseline for measuring the impact of development efforts on productivity and mission effectiveness.

IT Goal 6: Implement an effective Command and Control, COOP and COG infrastructure.

- These technologies support a distributed, fault-tolerance application thereby reducing the risk associated with a data center failure or a denial-of-service attack.
- These technologies support a strong transaction-processing model thereby eliminating the risk associated with non-Isolated events.
- These technologies support an open interface standard, recommended by the FEAPMO, thereby promoting interoperability with internal and external systems.

IT Goal 7: Shape the VA IT workforce to support the target One-VA EA.

- These technologies can be used to consolidate user interfaces into a common view thereby reducing user training.
- These technologies employ a common technical approach that maximizes the flexibility of the VA IT workforce to address a wide variety of applications and leverages technical training.

- These technologies are based on industry best practices and open standards thereby providing many training sources for the workforce.

7.1 System Development Life Cycle

7.1.1 Introduction

This narrative describes the System Development Life Cycle (SDLC) methodologies for Information Technology (IT) projects at the Department of Veterans Affairs (VA). This SDLC, in concert with other VA governance initiatives, such as the VA IT Project Management methodologies and the Enterprise Architecture Project Milestone Review Process, help guide the management and process of IT projects.

7.1.1.1 Purpose

The VA has historically managed IT projects independently at the Administration level. Each Administration has adopted a different process in managing the life cycle of its IT project. The VA OEAM is publishing this guidance in an effort to standardize on life cycle methodologies across the VA for a more consistent management approach. OEAM recognizes that each Administration within the VA may want to tailor the methodology for its specific needs. The VA is adopting a segmented architecture for IT project SDLC methodologies. The SDLC methodologies presented in this document may be refined and customized at the Administration level as necessary, but subject to the Office of Enterprise Architecture Management approval.

The document describes the four IT project system development life cycle methodologies at the VA:

- Infrastructure Augmentation
- COTS/GOTS Implementation
- Small Custom Software Development – Waterfall
- Medium and Large Custom Software Development – RUP

7.1.1.2 Scope

The SDLC methodologies described in this document are applicable to all IT projects within the VA and its Administrations (VHA, VBA and NCA). The Methodologies described herein are relevant to the system development process, not the project management process. The Methodologies should be used in conjunction with the VA IT Project Management guidelines, as well as the VA EA Project Milestone Review process.

The SDLCs are NOT intended to supersede or negate other project management, governance or guidance activities. Deliverables and artifacts required and produced as a result of following the life cycle processes do not include deliverables and artifacts required by other governance, management and review processes.

7.1.1.3 References

- VA OIT Project Management Guide
- VA OEAM EA Project Milestone Review Process

- VHA HSD&D System Development Life Cycle Website
- VHA HSD&D Software Engineering Process Group and Software Quality Assurance Website

7.1.2 Infrastructure Augmentation

7.1.2.1 Guidance on use

Infrastructure augmentation projects typically consist almost entirely or mostly of readily available commercial services and commodity hardware devices, peripherals or appliances. Key characteristics that distinguish infrastructure augmentation projects are:

- The projects implement systems that are largely hardware centric
- The projects do not involve developing custom software components or interfaces

These projects often fall into one of these two categories:

- Communication services and devices

  Projects implementing or enhancing the VA's data communication services, whether Internet access, local area networks (LAN) or wide area networks (WAN), fall into this category and qualify as an infrastructure augmentation project. These projects may involve supplementing or upgrading existing physical cables within the VA or between the VA and service providers; reconfiguring or replacing network routers, switches and bridges; or purchasing increased throughput from service providers. Because so much of the VA computing environment is dependent on the communication backbone, sound architecture, design and implementation methodology is required for a successful implementation.

  Other communication services in this category may include telephone or public exchange systems, voice over IP, and wireless networks. Typically, only projects involving the laying of the foundation for the use of these technologies are considered infrastructure augmentation, not the building or implementing of applications that utilize these services.

  While these projects may involve configuring software embedded in the hardware devices, it does not typically involve developing custom software or interfaces that include business logic. Software enhancements to the hardware devices are typically available as part of an add-on module from the vendor or a third party partner.
- Office automation hardware devices, peripherals or appliances

  Projects deploying office automation hardware devices such as printers, scanners, and copiers qualify as infrastructure augmentation projects. These devices require specific configuration to function on the computing infrastructure, but do no involve designing custom software or interfaces.

  The deployment of servers and desktop PCs may be considered infrastructure augmentation even though these computers have significant software installed and specific configuration of both the software and the hardware is critical. The key determining factor that makes the deployment of computer hardware an infrastructure augmentation project is whether the focus of the project is the implementation of hardware based on an existing architecture and design, or is the focus the architecture and design of the operating environment. Projects focused on the implementation of hardware based on an existing architecture and design qualifies as an infrastructure augmentation project, whereas the architecture and design of the operating environment is considered a COTS Implementation project.

Should the project involve the development of custom software components or interfaces as part of the implementation of these hardware devices, whenever possible, the software development portions should follow the Small Custom Software Develop (Waterfall) methodology apart from the infrastructure augmentation focus.

7.1.2.2 Life Cycle Methodology

Phase	Activity	Responsible Person	Job Aides	Deliverables
Pre-Milestone 0 (Project Initiation Approval) Activities				
0	Create project management artifacts and deliverables	Project Manager	VA Project Management Guide	see VA Project Management Guide
0	Document high level requirements	Analyst	SRS Template	Draft System Requirements Specification
	Milestone 0 - Project Initiation Approval			
Pre-Milestone 1 (Prototype Development Approval) Activities				
1	Update project management artifacts and deliverables	Project Manager	VA Project Management Guide	see VA Project Management Guide
1	Develop system requirements	Analyst	SRS Template	Draft System Requirements Specification
1	Evaluate candidate products and select prototype finalists	Analyst; Project Manager	Product Evaluation Report Template	Product Evaluation Report
1	Develop prototype finalists evaluation plan	Analyst	Test Plan Template	Prototype Evaluation Plan
	Milestone 1 - Prototype Development Approval			
Pre-Milestone 2 (System Development Approval) Activities				
2	Update project management artifacts and deliverables	Project Manager	VA Project Management Guide	see VA Project Management Guide
2	Develop prototype	Analyst		Prototype Build

Phase	Activity	Responsible Person	Job Aides	Deliverables
2	Perform infrastructure impact analysis	Analyst	Infrastructure Impact Analysis Report Template	Infrastructure Impact Analysis Report
2	Finalize product selection	Analyst, Project Manager, Security Engineer, System Architect	Test Analysis Report Template	Prototype Evaluation Report
2	Perform hardware capacity analysis and planning	Analyst		Updated System Requirements Specification
2	Identify product customizations and enhancements	Analyst		Updated System Requirements Specification
2	Finalize system architecture	System Architect	SAD Template	System Architecture Document
2	Finalize system design	Analyst; System Architect	SDD Template	System Design Document
2	Develop test plan	Project Manager, SQA Analyst	Test Plan Template; Sample Test Case Matrix	Test Plan Test Case Matrix
2	Develop training plan	Analyst; Project Manager		Training Schedule and Plan
	Milestone 2 - System Development Approval			
Pre-Milestone 3 (System Deployment Approval) Activities				

Phase	Activity	Responsible Person	Job Aides	Deliverables
3	Update project management artifacts and deliverables	Project Manager	VA Project Management Guide	see VA Project Management Guide
3	Finalize system installation and configuration procedures	Analyst		Installation and Configuration Procedures
3	Finalize migration procedures	Analyst		Migration Procedures
3	Finalize test procedures	SQA Analyst		Test Procedures
3	Finalize training plan	Project Manager		Training Schedule and Plan
3	Complete system testing	SQA Analyst	Test Analysis Report Template; Test Execution Log Template; Test Incident Log Template	System Test Analysis Report; System Test Execution Log; System Test Incident Log
3	Complete integration testing	SQA Analyst	Test Analysis Report Template; Test Execution Log Template; Test Incident Log Template	Integration Test Analysis Report; Integration Test Execution Log Integration Test Incident Log
3	Finalize training curriculum	Analyst		Training Curriculum
3	Develop technical manual	Analyst		Technical Manual

Phase	Activity	Responsible Person	Job Aides	Deliverables
3	Arrange for vendor support and maintenance	Analyst; Project Manager		Vendor Support Service Level Agreement
3	Arrange for system administration and technical support and maintenance	Project Manager		Memorandum of Understanding with VA support organizations with specific Service Level Agreement for system administration, technical support and maintenance
3	Develop and implement VA support protocols	Project Manager		Technical Support Protocol
3	Arrange for security certification	Project Manager		C&A complete; Security Test Report; Exhibit 300 Security Addendum
3	Prepare Continuity of Operation Plan	Analyst; Project Manager		Continuity of Operation Plan
	Milestone 3 - System Deployment Approval			
Pre-Milestone 4 (Post Implementation Review) Activities				
4	Update project management artifacts and deliverables	Project Manager	VA Project Management Guide	see VA Project Management Guide
	Milestone 4 - Post Implementation Review			

Table 1 - Infrastructure Augmentation SDLC

7.1.2.3 Templates

- System Requirements Specification (SRS)
- Product Evaluation Report
- Infrastructure Impact Analysis Report
- System Architecture Document (SAD)
- System Design Document (SDD)
- Test Plan
- Sample Test Case Matrix
- Test Execution Log
- Test Incident Log
- Test Analysis Report

7.1.2.4 Milestone Deliverable Summary

Milestone	Deliverables
Milestone 0 - Project Initiation Approval	
	See VA IT Project Management Guide
	Draft System Requirements Specification
Milestone 1 - Prototype Development Approval	
	Draft System Requirements Specification
	Product Evaluation Report
	Prototype Evaluation Plan
Milestone 2 - System Development Approval	
	Prototype Build
	Infrastructure Impact Analysis Report
	Prototype Evaluation Report
	System Requirements Specification
	System Architecture Document
	System Design Document
	Test Plan Test Case Matrix
	Training Schedule and Plan

Milestone 3 - System Deployment Approval	
	Installation and Configuration Procedures
	Migration Procedures
	Test Procedures
	Training Schedule and Plan
	System Test Analysis Report; System Test Execution Log; System Test Incident Log
	Integration Test Analysis Report; Integration Test Execution Log Integration Test Incident Log
	Training Curriculum
	Technical Manual
	Vendor Support Service Level Agreement
	Memorandum of Understanding with VA support organizations with specific Service Level Agreement for system administration, technical support and maintenance
	Technical Support Protocol
	C&A complete; Security Test Report; Exhibit 300 Security Addendum
	Continuity of Operation Plan
Milestone 4 - Post Implementation Review	
	See VA IT Project Management Guide

Table 2 - Infrastructure Augmentation Milestone Deliverable Summary

7.1.3 COTS/GOTS Implementation

7.1.3.1 Guidance on Use

This methodology is employed for implementing pre-packaged software, whether it is commercially purchased or custom developed for use at the VA or another government agency. Key characteristics that distinguish COTS/GOTS Implementation projects are:

- The projects implement systems that are largely software centric

- The projects involve changing the configuration of operating environment at a software level

While the cost of the software, type of software or the size of the implementation may influence the complexity of the project, it does not necessarily deviate from this overall implementation methodology.

It is notable that implementation best practices are often available for software packages that have a sizeable impact on the organization. Best practices may be available from the software vendors or industry experts. For instance, many industry best practices exist for the implementation of corporate email, portal or Enterprise Resource Planning (ERP) systems. Project teams should study these available industry best practices and integrate them into the implementation plan, using this methodology as an overall project guide in principle. This methodology can also be applied to project rolling out new or upgrades to computer operating system, desktop utilities or applications.

In addition to implementing systems such as a corporate database or an ERP, software change to the existing operating environment also qualify as COTS/GOTS Implementation. For example, the change to using IPv6, or the change from using static IP addresses to Dynamic Host Configuration Protocol, which are software additions or changes to the operating environment, would qualify as COTS/GOTS Implementation.

COTS/GOTS implementation projects may sometimes involve changing the underlying infrastructure. For example, when the VA moved from a distributed email architecture to a consolidated architecture, the increase in network traffic over the wide area network necessitated an infrastructure augmentation increasing network throughput while decreasing latency. In such scenarios, the portion of the project to change the network configuration should be a sub-project following the infrastructure augmentation methodology. Similarly, if custom software components and interfaces are required as part of the COTS/GOTS implementation, the development effort should be managed as a sub-project following the other custom software development methodologies.

7.1.3.2 Life Cycle Methodology

Phase	Activity	Responsible Person	Job Aides	Deliverables
Pre-Milestone 0 (Project Initiation Approval) Activities				
0	Create project management artifacts and deliverables	Project Manager	VA Project Management Guide	see VA Project Management Guide
0	Develop use case model	Analyst	Use Case Model Template	Draft Use Case Model
0	Document business rules	Analyst	Business Rules Template	Draft Business Rules
	Document high level requirements		SRS Template	Draft System Requirements Specification
	Milestone 0 - Project Initiation Approval			
Pre-Milestone 1 (Prototype Development Approval) Activities				
1	Update project management artifacts and deliverables	Project Manager	VA Project Management Guide	see VA Project Management Guide
1	Finalize use case model	Analyst	Use Case Model Template	Use Case Model
1	Finalize business rules	Analyst	Business Rules Template	Business Rules
1	Develop system requirements	Analyst	SRS Template	System Requirements Specification
1	Evaluate candidate products and select prototype finalists	Analysts; Project Manager	Product Evaluation Report Template	Product Evaluation Report

Phase	Activity	Responsible Person	Job Aides	Deliverables
1	Develop prototype finalists evaluation plan	Analysts	Test Plan Template	Prototype Evaluation Plan
	Milestone 1 - Prototype Development Approval			
Pre-Milestone 2 (System Development Approval) Activities				
2	Update project management artifacts and deliverables	Project Manager	VA Project Management Guide	see VA Project Management Guide
2	Develop prototype	Analyst		Prototype Build
2	Perform infrastructure impact analysis	Analyst		Infrastructure Impact Analysis Report
2	Finalize product selection	Analyst, Project Manager, Security Engineer, System Architect	Test Analysis Report Template	Prototype Evaluation Report
2	Perform hardware capacity analysis and planning	Analyst		Updated System Requirements Specification
2	Identify product customizations and enhancements	Analyst		Updated System Requirements Specification
2	Define system supplementary	Analyst		Updated System Requirements Specification

Phase	Activity	Responsible Person	Job Aides	Deliverables
	specifications			
2	Document product data model		Data Model Template	Data Model
2	Finalize system architecture	System Architect	SAD Template	System Architecture Document
2	Finalize system design	Analyst; System Architect	SDD Template	System Design Document
2	Finalize infrastructure augmentation plan	Analyst		see Infrastructure Augmentation SDLC
2	Develop test plan	SQA Analyst; Project Manager	Test Plan Temple; Sample Test Case Matrix	Test Plan; Test Case Matrix
2	Develop training plan	Analyst; Project Manager		Training Schedule and Plan
	Milestone 2 - System Development Approval			
Pre-Milestone 3 (System Deployment Approval) Activities				
3	Update project management artifacts and deliverables	Project Manager	VA Project Management Guide	see VA Project Management Guide
3	Finalize infrastructure augmentation procedures	Analyst		Infrastructure Augmentation Procedures

Phase	Activity	Responsible Person	Job Aides	Deliverables
3	Finalize system installation and configuration procedures	Analyst		Installation and Configuration Procedures
3	Finalize migration procedures	Analyst		Migration Procedures
3	Finalize test procedures	SQA Analyst		Test Procedures
3	Finalize training plan	Project Manager		Training Schedule and Plan
3	Complete system testing	SQA Analyst	Test Analysis Report Template; Test Execution Log Template; Test Incident Log Template	System Test Analysis Report; System Test Execution Log; System Test Incident Log
3	Complete integration testing	SQA Analyst	Test Analysis Report Template; Test Execution Log Template; Test Incident Log Template	Integration Test Analysis Report; Integration Test Execution Log; Integration Test Incident Log
3	Finalize user training curriculum	Analyst		User Training Curriculum
3	Finalize administrator training curriculum	Analyst		Administrator Training Curriculum

Phase	Activity	Responsible Person	Job Aides	Deliverables
3	Develop user manual	Analyst		User Manual
3	Develop technical manual	Analyst		Technical Manual
3	Arrange vendor support and maintenance	Analyst; Project Manager		Vendor Support Service Level Agreement
3	Arrange user support	Analyst; Project Manager		Memorandum of Understanding with VA support organizations with specific Service Level Agreement for user support
3	Arrange for system administration and technical support and maintenance	Project Manager		Memorandum of Understanding with VA support organizations with specific Service Level Agreement for system administration, technical support and maintenance
3	Develop and implement VA support protocols	Project Manager		Technical Support Protocol
3	Arrange for security certification	Project Manager		C&A complete; Security Test Report; Exhibit 300 Security Addendum
3	Prepare Continuity of Operation Plan	Analyst; Project Manager		Continuity of Operation Plan
	Milestone 3 - System Deployment Approval			
Pre-Milestone 4 (Post Implementation Review) Activities				
4	Update project management artifacts and deliverables	Project Manager	VA Project Management Guide	see VA Project Management Guide
	Milestone 4 - Post Implementation Review			

Table 3 - COTS/GOTS Implementation SDLC

7.1.3.3 Templates

- Use Case Model
- Business Rules
- Data Model
- System Requirements Specification (SRS)
- Product Evaluation Report
- Infrastructure Impact Analysis Report
- System Architecture Document (SAD)
- System Design Document (SDD)
- Test Plan
- Sample Test Case Matrix
- Test Execution Log
- Test Incident Log
- Test Analysis Report

7.1.3.4 Milestone Deliverable Summary

Milestone	Deliverables
Milestone 0 - Project Initiation Approval	
	See VA IT Project Management Guide
	Draft Use Case Model
	Draft Business Rules
	Draft System Requirements Document
Milestone 1 - Prototype Development Approval	
	Use Case Model
	Business Rules
	Draft System Requirements Document
	Product Evaluation Report
	Prototype Evaluation Plan
Milestone 2 - System Development Approval	
	Prototype Build
	Infrastructure Impact Analysis Report
	Prototype Evaluation Report

Milestone	Deliverables
	System Requirements Specification
	Data Model
	System Architecture Document
	System Design Document
	see Infrastructure Augmentation SDLC
	Test Plan Test Case Matrix
	Training Schedule and Plan
Milestone 3 - System Deployment Approval	
	Infrastructure Augmentation Procedures
	Installation and Configuration Procedures
	Migration Procedures
	Test Procedures
	Training Schedule and Plan
	System Test Analysis Report; System Test Execution Log; System Test Incident Log
	Integration Test Analysis Report; Integration Test Execution Log Integration Test Incident Log
	User Training Curriculum
	Administrator Training Curriculum
	User Manual
	Technical Manual
	Vendor Support Service Level Agreement
	Memorandum of Understanding with VA support organizations with specific Service Level Agreement for user support
	Memorandum of Understanding with VA support organizations with specific Service Level Agreement for system administration, technical support and maintenance
	Technical Support Protocol

Milestone	Deliverables
	C&A complete; Security Test Report; Exhibit 300 Security Addendum
	Continuity of Operation Plan
Milestone 4 - Post Implementation Review	
	See VA IT Project Management Guide

Table 4 - COTS/GOTS Implementation Milestone Deliverable Summary

7.1.4 Small Custom Software Development – Waterfall

7.1.4.1 Guidance on Use

This software development life cycle methodology is most widely practiced and popular among software development teams. However, this methodology has been known to be less effective as projects and project teams get larger, as each phase of the development is typically regarded as a distinct process, which causes it to be somewhat less adaptable to change. This methodology is recommended for the development of applications characterized by the following:

- Small standalone applications with no external interfaces
- Non object-oriented development projects
- Application has fewer than eight to ten use cases
- Requirements and business rules are fairly well defined and understood by the user community

In line with the above recommendations, this methodology is ideal for developing software component or interfaces as enhancements to COTS/GOTS systems. Such components and interfaces typically have well-defined and limited functionality, allowing the development team to effectively and successfully capture and stabilize requirements and progress through the development life cycle.

This methodology can also be used effectively for developing applications of limited and well-defined use cases. The key to these applications is not necessarily the number of users, but the number and complexity of features, functions and business rules.

7.1.4.2 Life Cycle Methodology

The Waterfall software development life cycle methodology can be found at the Health Systems Design and Development System Development Life Cycle website.

7.1.4.3 Templates

Templates and other guidance material may be found at the Health Systems Design and Development Software Engineering Process Group and Software Quality Assurance website.

7.1.4.4 Milestone Deliverable Summary

Milestone	Deliverables
Milestone 0 - Project Initiation Approval	
	See VA IT Project Management Guide
Milestone 1 - Prototype Development Approval	
	Product Requirements Document
Milestone 2 - System Development Approval	
	System Requirements Specification
	System Design Document
	Data Dictionary Review
	Messaging Review
	Integration Agreement Review
	Capacity Planning Forms (ASSESS, PRE, PEMA, PUMA)
	Test Plan Test Case Matrix
Milestone 3 - System Deployment Approval	
	Security and Installation Guide
	Summary Test Report
	Summary Work Product Review Report
	Product Release Notes
	Training Materials
	User Manual
	Technical Manual
	Transition Document
	Memorandum of Understanding with VA support organizations with specific Service Level Agreement for user support
	Memorandum of Understanding with VA support organizations with specific Service Level Agreement for system administration, technical support and maintenance
	Technical Support Protocol

Milestone	Deliverables
	C&A complete; Security Test Report; Exhibit 300 Security Addendum
	Continuity of Operation Plan
Milestone 4 - Post Implementation Review	
	See VA IT Project Management Guide

Table 5 - Waterfall Milestone Deliverable Summary

7.1.5 Medium and Large Custom Software Development – Rational Unified Process

7.1.5.1 Guidance on Use

The Rational Unified Process (RUP) is an iterative software development process. Unlike the Waterfall methodology, RUP is not a single concrete prescriptive process, but rather an adaptable process framework describing how to develop software effectively using proven techniques. While the RUP consists of a many different activities, it is intended to be tailored to particular software projects or development organizations. It is widely recognized as particularly applicable to larger software development teams working on large projects.

Applications developed at the VA that is anticipated or expected to be business critical should follow this development process. Tailored by the Health Systems Design and Development organization of the Veterans Health Administration, two flavors of the RUP referred to as the Iterative Development Lifecycle (IDL) are available, one for medium sized projects and one for large projects. Selection of the medium or large flavors of the RUP should be determined by the software architect based on the following factors:

- Expected cost of the project
- Size of the project and project team
- Complexity of the system to be developed
- Criticality of the system to business and operations

7.1.5.2 Life Cycle Methodology

Both the medium and large Iterative Development Lifecycle can be found at the Health Systems Design and Development System Development Life Cycle website.

7.1.5.3 Templates

Templates and VHA's IDL Toolkit may be obtained from the following websites:

- Health Systems Design and Development IDL website

- Health Systems Design and Development Software Engineering Process Group and Software Quality Assurance website

7.1.5.4 Milestone Deliverable Summary

Milestone	Deliverables
Milestone 0 - Project Initiation Approval	
	Compliance Review Checklist
	Vision
	Business Case
	Iteration Plan
	Development Case
	Risk List
	Software Development Plan
	Executive Decision Memo or Project Approval Memo
	Recent Exhibit 300
	Glossary
	Use Case Models
	Supplementary Specifications
	Business Rules
	Iteration Assessment
	Software Architecture Document
	Domain Model (Business Analysis Model)
	Prototypes
	Development Infrastructure
	Interface Control Document
	Test Plan
Milestone 1 - Prototype Development Approval	
	Compliance Review Checklist
	Vision
	Business Case
	Iteration Plan
	Development Case
	Risk List
	Software Development Plan

Milestone	Deliverables
	Glossary
	Use Case Models
	Supplementary Specifications
	Business Rules
	Iteration Assessment
	Software Architecture Document
	Domain Model (Business Analysis Model)
	Development Infrastructure
	Design Model (and all constituent artifacts)
	Data Model
	Development Plan and Model
	Implementation Model (and all constituent artifacts, including Implementation Elements)
	Interface Control Document
	Test Plan
	Test Suite (“smoke test”)
	Test Automation Architecture
	Analysis Model
	End-User Support Material
Milestone 2 - System Development Approval	
	Compliance Review Checklist
	Iteration Plan
	Development Case
	Risk List
	Software Development Plan
	Glossary
	Use Case Models
	Supplementary Specifications
	Business Rules
	Iteration Assessment
	Software Architecture Document
	Domain Model (Business Analysis

Milestone	Deliverables
	Model)
	Development Infrastructure
	Design Model (and all constituent artifacts)
	Data Model
	Development Plan and Model
	Implementation Model (and all constituent artifacts, including Implementation Elements)
	Interface Control Document
	Test Plan
	Test Suite (“smoke test”)
	Test Automation Architecture
	Test Evaluation Summary Report
	End-User Support Material
Milestone 3 - System Deployment Approval	
	Compliance Review Checklist
	Iteration Plan
	Development Case
	Risk List
	Software Development Plan
	Glossary
	Use Case Models
	Supplementary Specifications
	Business Rules
	Iteration Assessment
	Software Architecture Document
	Domain Model (Business Analysis Model)
	Development Infrastructure
	Design Model (and all constituent artifacts)
	Data Model
	Development Plan and Model
	Implementation Model (and all constituent artifacts, including

Milestone	Deliverables
	Implementation Elements)
	Interface Control Document
	Test Suite (“smoke test”)
	Test Automation Architecture
	End-User Support Material
Milestone 4 - Post Implementation Review	
	N/A

Table 6 - RUP Milestone Deliverable Summary

7.2 Configuration Management

Configuration Management (CM) is both a discipline and a process. CM applies technical and administrative management and control for establishing and maintaining the integrity of a product, component (or set of components), and the documentation to design, build and maintain the product and its parts. This integrity is maintained by ensuring consistency between the functional and physical performance attributes and the requirements, design, and operations information throughout the life of the product. Through properly applied CM practices and activities, changes are controlled and tracked, impacts are assessed, and decision makers have the information needed to make sure the products are built and perform as intended. CM processes are also used to track product variances and waivers.

A “product” in this context:

- May be a system, an item, a component or group of components;
- May be in the form of or include equipment, computer hardware, software, firmware, facilities, networks, documents, interfaces, licenses, and others; and
- May be intended for delivery to the customer, designated for internal work, acquired from sources external to the organization, or tools and other items used in creating and describing other products.

CM includes five sub-functions – Planning, Identification, Configuration Change Management, Configuration Status Accounting, and Configuration Auditing.

1) Planning is the creation and execution of the CM system with assigned roles and responsibilities, and the development and adoption of CM procedures and instructions.

2) Identification involves the selection items to be controlled, providing unique identifications, assigning ownership authorities and responsibilities, and determining baselines and when they will be established.

3) Configuration Change Management is the function of controlling changes and variances to the product using systematic, measurable change processes.

4) Configuration Status Accounting provides the means for accurate, timely "views" of the configuration of the product at points in time, traceability along phases of product life, and traceability of modifications to changes.

5) Configuration Audits (physical and functional) verify conformance to specifications, drawings, interface control documents, and other contract requirements.

Benefits

Configuration management provides documented, full visibility of the product's present configuration and the status of achievement of its physical and functional requirements and ensures that everyone working on the project at any time in its life cycle has access to correct and accurate information.

Benefits of configuration management include the following:

- Product attributes are defined.
    a) Customer and provider have a common basis for acquisition and use of the product.
    b) Inhibits "feature creep."
    c) Provides measurable performance parameters
- The product is identified, defined, and documented.
    a) Established product configuration provides a known basis for making changes.
    b) Decisions are based on correct, current information for all parties.
    c) Production repeatability is enhanced.
- Products are labeled and correlated with their associated requirements, design, and product information.
    a) Facilitates tracking the correlation between requirements and the product.
    b) Ensures that the product conforms to requirements throughout the life cycle through acceptance and operations and maintenance.
    c) The applicable data (such as for procurement, design, or servicing the product) is accessible, avoiding guesswork and trial and error.
- Proposed changes are identified and evaluated for impact prior to making change decisions.
    a) Downstream surprises are avoided.
    b) Facilitates reductions in cost, risk, and liability.
    c) Cost and schedule savings are realized.
- Change activity is managed using a defined process.
    a) Provides proactive management and control of the product and changes to the product.

b) Product development and changes are planned and managed for the context and environment of the work being performed.

c) Costly errors of ad hoc, erratic change management are avoided.

- Configuration information captured from product definition through disposal processes is organized for retrieval of key information and relationships as needed.

  a) Timely, accurate information avoids costly delays and product down time, ensures proper replacement and repair, and decreases maintenance costs.

  b) Facilitates disaster recovery by providing an accurate, up-to-date baseline of the system.

- Actual product configuration is verified against the required attributes.

  a) Incorporation of changes to the product is verified and recorded throughout the product life.

  b) A high level of confidence in the product information is established.

- Assists IT security efforts.

  a) Configuration audits warrant against accidental, malicious or other unauthorized changes to the product during development or during operations.

  b) Enables the organization to reduce the use of unauthorized software that can increase complexity and support costs.

Guidelines

- CM planning may be included in a project plan or constitute a stand-alone document (CM Plan). In the latter case, the project plan should contain a reference to the CM Plan.
- CM planning and management is implemented and practiced over the entire life cycle of the product.
- CM functional responsibilities are assigned to organizational elements and individuals.
- CM and other personnel with CM-related responsibilities are properly trained.
- Adequate resources, including automated CM applications and facilities if appropriate, are determined and applied.
- CM planning addresses the performance of CM by contractors and VA-internal suppliers.
- Measurements are taken as indicators of CM performance and to provide a basis for improvement of CM processes and procedures.
- Selection of products for configuration control, as well as the degree and formality of CM activities to be applied, should be commensurate with product criticality, size, complexity, importance, urgency, cost, risk of product failure, and risk to other elements from product failure; however, the CM activities must be planned.
- CM planning includes procedures for conducting CM activities. The CM plan may include procedures or refer to procedures that are external to the plan.

- The TESS software application, available through the VA CIRC contract, shall be used to manage and track all security patches and fixes.
- Configuration management procedures should ensure that:
  a) The change is implemented in a orderly manner through formalized testing;
  b) The user base is informed of the impending change;
  c) It is possible to isolate and analyze the effect of the change on the system after implementation;
  d) Any negative impact on computing services and resources is reduced.
- Configuration management procedures should address the following steps:
  a) How to apply to introduce a change;
  b) Authority to approve and approval process;
  c) Cataloging of the intended change;
  d) Scheduling of the change;
  e) Implementation of the change;
  f) Post implementation review;
  g) Reporting the change to the appropriate parties.
- Any change request should include instructions on how to reverse the change in case problems develop.

Standards

- Carnegie-Mellon University/Software Engineering Institute, Capability Maturity Model Integration for Systems Engineering/Software/Integrated Products and Processes Development/Supplier Sources (CMU/SEI CMMI – SE/SW/IPPD/SS), March 2002.
- Electronic Industries Alliance (EIA) (Government Electronic and Information Technology Association Industries Alliance (GEIA)) Standard-649-A, National Consensus Standard for Configuration Management, April 2004.

7.2.1 Source Code Management

The purpose of Source Code Management (SCM) is to archive development files and serve as a single point of entry/exit when adding or updating development files. SCM supports concurrent development, consolidates source code bases, logs and documents file/release versions, and grants convenient yet controlled access to all previous revisions. At the heart of the SCM is a common database of source code, documentation, and build tools. Source code management is conducted in accordance with the principle and procedures of configuration management

Rules

- All VA application development facilities shall implement SCM. If the Department selects a common SCM, its use is required.

- The SCM shall permit authorized developers to access current and previous versions, make the changes, and update the database with revised source Code, documentation, test suites, and build tools. Tools are retained, as developers need old versions of the tools to build old versions of the software. This ensures software is rebuilt exactly as the customer received it. The SCM shall require the developer to provide supporting documentation of his/her actions and track these changes for subsequent audits.
- The SCM shall provide both locking and code sharing. Locking permits only one person can work on a file at a time. Locking is most effective when developers work on different areas of the project and do not routinely come into conflict. The SCM shall track and remind developers who forget to unlock files when they are done. The SCM shall prevent developers from avoiding locking by editing a private copy and checking in when the file is finally unlocked.
- The SCM shall permit code sharing, managing conflicts where multiple developers work on the same source base. It shall provide development managers the option to lock individual files so only one person at a time can modify it, or, alternately, allow multiple people to modify a source file, with the system automatically merge the changes. Merging enables several people can work on a file at one time. Before committing changes, each user merges their copy with the latest copy in the database. This is normally done automatically by the system, but developers shall be able to review and accept the result of the merge. The SCM shall permit developers to create personal versions to make changes against a stable source base and then merge in the latest version later. The SCM shall provide the option to control these merges.
- The SCM shall label all the files in the source base that make up a product at each milestone. The SCM shall require developers to label artifacts before and after changes, as well as when a new version deploys. Each file in the database shall have a version tree so developers can branch off the version tree to allow separate development paths. Typically a main path (trunk) for the next major version and branches off of deployed versions for maintenance.
- The SCM shall support branching. When a new version deploys, developers typically create a branch in the version tree for maintenance. The SCM shall support double updates to fix a defect in the latest version and then merge the changes into the maintenance version.

Guidelines

- TBD

Standards

- TBD

7.2.2 Hardware Management

Asset registries track hardware description, configurations, maintenance and scheduling routines, expected life span, economic upgrade and replacement schedules, and backup methods. To ensure hardware's proper working order, hardware management services document maintenance programs and schedule routine upkeep and inspection by trained technicians. Hardware can

become 'obsolete' in a year or two after purchase. Hardware management services enable timely assessments of hardware whether to continue to use technology after it has become obsolete, or whether it is worth upgrading the technology. Reliable server systems are a priority as networked systems rely on the smooth operation of servers. Server systems generally include a range of backup methods to ensure that network down time is minimized or eliminated and that data is regularly backed up.

Rules

- Hardware assets are bar coded and cataloged in a hardware management system.

Guidelines

- Backup methods should include using batteries of servers (or 'server farms') with data mirrored on various hard drives and computers, and alternative cabling routes from workstations to servers. See Enterprise Storage. Hardware management should be conducted in accordance with configuration management principles and procedures.

Standards

- TBD

7.2.3 License Management and Electronic Software Distribution

License management is the dynamic tracking of users and software licenses: it makes software a network resource and makes software pricing more equitable. Without license management technology, a system administrator of even a small network cannot track the number of licenses used concurrently. License management differs from software "copy protection" used in the PC marketplace by controlling execution instead of copying. License management facilitates the acquisition of software because it eliminates the need to deploy the software. All that the user requires is a "license key"—a brief string of data that describes the license plus some security codes. These license keys can be distributed by e-mail, FAX or verbally over the telephone. License managers employ one or more of the following types of licensing policies.

- Node locking, once the most popular form of licensing, parallels the view that software is licensed to a particular computer. Typically, users may remotely login to the licensed computer. This licensing model is typically found in computationally intense applications and with software used on workstations dedicated to a particular application.
- User-based licensing assigns licenses to a specific user-id. This is useful for products that are user dependent, e.g., an e-mail product, or business transaction applications -- applications in which "lending" someone a user-id is not consistent with the nature of the application.
- Site licensing software to a geographical site is another approach, one that generally has a high entry price for the customer. Both the software vendor and customer frequently spend a great deal of time negotiating over price, as site licenses generally don't match pricing to actual usage very well. Defining a "site" can also be difficult. For example, a company with a large corporate campus may be so large that multiple sites are defined.
- "Network licensing" and "floating licenses" fit well with networked computing, due to efficient matching of usage to the number of licenses sold. Many customers at a site can

have access to a software product for the price of one license. As the software becomes widely used, additional licenses are purchased.

Rules

- TBD

Guidelines

- VA systems administrators may use the latest recommended version of Microsoft Systems Management Server (SMS) to install and maintain operating systems and applications, discover system configurations, and perform helpdesk operations.

Standards

- TBD

References

- License Management: How developers control software licensing by Richard Mirabella, Globetrotter Software. http://www.globetrotter.com/art1.htm

7.2.4 Requirements Management

Requirements management, in system/software engineering, is the process of controlling the identification, allocation, and flow down of requirements from the system level to the module or part level, including interfaces, verification, modifications, and status monitoring. Requirements management is the set of activities that concentrate on assuring the specifications, i.e., requirements, are met to the customer's satisfaction. It is a process that begins at project inception and continues until the resulting product(s) is no longer needed. Requirements management includes the major requirements management phases, such as organizing, implementing and sustaining and the key requirements management activities, such as gathering, documenting, verifying and managing changes.

Rules

- Each requirement shall be traceable to a specific project objective described in the Software Requirement Specifications. This traceability assures that the software product will satisfy all requirements and will not include inappropriate or extraneous functionality. It is important to know the source of all requirements so they can be verified to be necessary, accurate and complete. The traceability is also a key element in establishing audit ability of the system during development, and maintaining it after the system is operational.

Guidelines

- Identify stakeholders of a software project in the Project Plan to facilitate decision-making and unified approval of the Requirement Specifications and other deliverables.
- The stakeholders should meet at logical checkpoints in the application development or maintenance project (e.g., at the beginning and end of each milestone) to review the progress and approve continuing the project.

- Management of requirements is best conducted according to the principles and procedures of configuration management.

Standards

- TBD

References

- Software Requirements Engineering, Second Edition Richard H. Thayer and Merlin Dorfman http://www.computer.org/cspress/CATALOG/bp07738.htm
- Software Engineering Institute (SEI) Capability Maturity Models, http://www.sei.cmu.edu/cmm/cmms/cmms.html
- Key Practices of the Capability Maturity Model, Version 1.1 Mark C. Paulk, Charles V. Weber, Suzanne M. Garcia, Mary Beth Chrissis, Marilyn Bush, Technical Report CMU/SEI-93-TR-025 ESC-TR-93-178, February 1993 http://www.sei.cmu.edu/pub/documents/93.reports/pdf/tr25.93.pdf
- SEI'S Capability Maturity Model - Version 1.1 Requirements Management, http://www.dfas.mil/technology/pal/cmm/lvl2/rm/
- Requirements Management Practices for Developers By Catherine Connor and Leonard Callejo http://www.rational.com/media/whitepapers/RM_developers.pdf
- Guidelines for Requirements Management, April 2000, United States Department of Energy, Albuquerque Operations Office http://cio.doe.gov/ITReform/sqse/download/rqtmg400.doc

7.2.5 Content Management

Content Management Systems (CMS) manage the creation and flow of documents through the help of databases and workflow engines that encapsulate metadata and business rules. Knowledge Management Systems (KMS) capture and distribute the knowledge held among individuals within a corporation to other co-workers and partners, according to set rules. KMS is especially well suited to the internal needs of organizations in knowledge-oriented organizations like VA. Content Management tools also add other functions such as templating, separation of content and presentation, web publishing, and syndication.

Goals

IT Goal 3: Secure the One-VA enterprise against Cyber Attack.

- CMS is a tool for deployment of policy, procedures, and training.

IT Goal 5: Establish effective metrics to measure performance.

- CMS provide statistics on the utility and usability of VA's knowledge base.

IT Goal 7: Shape the VA IT workforce to support the target One-VA EA.

- CMS is a tool for deployment of coordination, education and training.

Rules

- TBD

Guidelines

- VA should obtain complete CMS solutions that cover content creation, content delivery, and business analytics. It should also integrate content management, data management, and records management into one set of components. Careful sizing and configuration management is necessary to ensure that the CMS will support the web servers in production. VA has prepared requirements at
    a) http://www.va.gov/cosset_study/
    b) http://vaww.va.gov/cms/docs/Key_Technical_and_Functional_Criteria.doc
    c) http://vaww.va.gov/cms/docs/CMS_-_Top_15_Technical_Evaluation_Criteria.xls

Standards

- TBD

7.3 Capacity Management and Capacity Planning

Capacity Management involves balancing capacity with load. Capacity is the amount of load (needed space, traffic, processing, and "safety margin") that a resource is capable of supporting. Capacity planning is the process used to evaluate current trends in resource usage and plan for growth and changes before problems occur.

Generally, capacity planning involves gathering and analyzing current data and making short-term adjustments and then incorporating estimated future needs (that may cover months to years) as a predictive element for planning future asset acquisitions or divestitures. Considerations for future needs include but are not limited to: current performance, performance requirements, currently planned acquisitions, currently planned modifications or enhancements, future manpower projections, geographic changes in the user base, available physical space, emerging technologies, and many others. Also of considerable importance are the impacts these considerations may have on each other. These considerations may be applied to such systems or subsystems as software, hardware, facilities, infrastructure, communications, room space, file space (physical or electronic), etc.

Benefits

The major benefits of capacity management and planning for One VA are:

- Controlled infrastructure size
- Improved IT management staff efficiencies
- Improved internal end-user satisfaction
- Improved alignment of IT to business goals
- Improved support of new and existing applications
- Reduced brownouts and outages attributed to over-utilization
- Improved bandwidth and infrastructure utilization

- Improved efficiencies of scale
- Improved cost efficiencies

Capacity planning can serve as a reality check, prompting an organization to come to terms with its current business plan and its goals for the future.

Guidelines

The following is a high-level view of the capacity planning process:

- Combines information including:
  - Current system baseline (software, hardware, network, connectivity, etc.),
  - Current usage or load (people, transactions, processor utilization, line traffic, etc.),
  - Current performance measures, and
  - Current performance requirements;
- Uses the information to determine the current needed capacity;
- Considers estimates of system impacts resulting from:
  - Expected changes to the baseline,
  - Expected changes to usage or loading,
  - Expected required performance improvements, and
  - Expected capacity constrictions;
- Determines projected capacity needs; and
- Proposes changes to meet those needs.

Capacity management procedures should include the following provisions (at minimum):

6) New assets (purchased or built in-house) are processed in accordance with the approved capacity planning methodology;
7) The impact on the existing environment is identified and defined;
8) How the integration of the new asset with the current infrastructure will occur;
9) Determining the upper and lower limits of existing capacity;
10) Determining the surplus capacity;
11) Determining best estimate of new resource usage;
12) Estimating the difference between hard upper capacity limits and estimated future loadings;
13) Feedback of modeling information to the infrastructure model...

References

- VA Capacity Planning Plan (to be provided)

- ITIL (The IT Information Library maintained by the Department of Commerce-UK) Capacity Management

Standards

- TBD

7.4 Deployment Planning

The successful deployment of a VA Enterprise Systems' installation is a complicated task which requires reviewing customer/system requirements, integration of numerous products and resources, proper training of users/administrators, and extensive integration testing in the customer environment. Early-on in the system development life cycle, the Systems Development Program Manager conducts a set of meetings to assess the systems' deployment strategies and documents the deployment requirements to ensure the resources and intended configuration of those resources at the customer location can adequately meet the expectations required of the system. This early-on assessment of the Enterprise installation environment must also assess all other current parallel development efforts to determine their expected impact on the installation environment. The next step in this process is to help the user community coordinate the availability and readiness of the identified resources before the actual installation of the designated Systems begins. Each one of the products/resources that the Systems' uses require must be installed, configured and tuned correctly for the final System to function and perform as expected in the designated operating environment. Once installed, a series of operational tests must be planned and performed to verify that the System can meet the demands of the final production environment. Finally, proper training of Systems' administrators, as well as Systems' users, is necessary to make a smooth transition to the final production environment.

To help the Systems' administrators in all of these tasks, a set of procedures, in addition to this technical requirement, must be developed to assist those involved in this process, as established in the referenced Deployment Planning plan. The Deployment Planning plan contains detailed requirements, deployment strategies, and planning guidelines of what is required to bring the newly developed System online from an initial introduction and review of the customer environment to the time the system is ready for production use. The deployment procedures include a time line plus checklists that the user installation/system administration team should use to keep the deployment of the System on track. This is the same Deployment Plan that the System support/deployment team uses to monitor and check the progress of an installation in the user environment.

The Deployment Planning plan is written to conform to the systems development life cycle and identifies various deployment planning checklists that facilitate navigating the life cycle process stages.

Benefits

The major benefits of deployment planning for One VA are:

- Controlled and structured user introduction
- Improved IT management staff efficiencies
- Improved Internal end-user satisfaction

- Improved support of new and existing applications
- Reduced costs for systems deployments
- Reduced disruptions of the production environment during systems installations
- Improved user preparation for systems utilization
- Improved efficiencies of scale
- Improved cost efficiencies
- Reduced or eliminated systems reinstallations

Deployment planning provides opportunities to perform pilot installations, pre-staging, user community preparation, administrator preparedness, etc. prompting an organization to come to terms with its current business plan and its goals for the future.

Guidelines

Deployment planning should include the following provisions:

- New assets (purchased or built in-house) are introduced to the production environment in accordance with the approved Systems Deployment Plan;
- The impact on the existing environment and the Systems user is identified and defined;
- The deployment integration of the new asset with the current infrastructure is managed and controlled;
- Systems administrators and users are trained in preparation for the systems introduction;
- Determining the deployment shortfalls and critical installation requirements;
- Feedback of modeling information to the infrastructure model.

References

- VA Deployment Planning plan (provided separately)
- Information Technology Information Library (ITIL) Release Management - maintained by the UK Department of Commerce

Standards

- TBD

7.5 Workflow/Event Management (EAI)

Workflow is the set of relationships between all the activities in a project, from start to finish. Workflow is the movement of documents around an organization for purposes including sign-off, evaluation, performing activities in a process and co-writing. Enterprise Application Integration (EAI) provides the necessary mechanisms to connect with the variety of software environments, integrate with the native applications, and transform data into the required form. Sales order entry, order fulfillment, order status, product support, or account inquiry can be handled by separate business applications, but the customer is shown a unified view.

Rules

- EAI shall provide for activities to be triggered by external events or by other activities. Additional functionality shall include validation (syntax), translation, and routing. EAI shall keep updates synchronized and provides normalized views of disparate application databases. EAI shall provide data extraction and transformation, application adapters to packaged applications, environment adapters to computer resources, message brokers to support many-to-many communication, and rules- and content-based routing.

Guidelines

- Changes to workflows and event-driven actions are made through the principles and procedures of configuration management.

Standards

- TBD