Department of Veteran Affairs Technical Reference Model

July 8, 2002

Version 1.2

Department of Veteran Affairs
Technical Reference Model

Table of Contents

1. INTRODUCTION 2

1.1 Background 2
1.2 Scope 2
1.3 Purpose 2
1.4 Goals 2
1.5 Audience 2
1.6 Approach 2
1.7 Commercial off-the-Shelf (COTS) and Government off-the-Shelf (GOTS) 2

2. TRM OVERVIEW 2

2.1 VA Enterprise Architecture Summary 2
2.2 Relationship of the VA Enterprise Architecture, TRM, and Standards Profile 2
2.3 Overview of EA Implementation Knowledge Base 2
2.3.1 Standards Submission and Adoption Process 2
2.3.2 Standards Compliance and Waiver Policy 2
2.3.3 Technology Refresh Process 2
2.4 TRM Structure 2
2.4.1 Standards Profile View 2
2.4.2 Best Practices Compendium View 2
2.4.3 Service and Function Taxonomy View 2
2.4.4 Integrated Project Development Views 2
2.5 TRM Document Management 2

3. TRM SERVICES AND TAXONOMY 2

3.1 System Services 2
3.1.1 Language Services 2
3.1.2 Operating System Services 2
3.1.3 Supporting Application Services 2
3.1.4 Software Engineering Services 2
3.2 Communications Services 2
3.2.1 Transparent Network Services 2
3.2.2 Network Management Services 2
3.2.3 External Environment Interface 2
3.3 Information Services 2
3.3.1 Document Management Services 2
3.3.2 Data Management Services 2
3.4 User Services 2
3.4.1 Usability and Accessibility 2

3.4.2 User Interface 2
3.4.3 Windowing Systems 2
3.4.4 Graphics 2
3.5 Security Services 2
3.5.1 Technical Security Services 2
3.5.2 Physical and Environmental Control 2
3.5.3 Administrative Security Services 2
3.5.4 Security Management Services 2
3.5.5 Security Mechanisms 2

Department of Veteran Affairs
Technical Reference Model

List of Figures

Figure 1: Enterprise Architecture Model Front View 2
Figure 2: Relationship of the One-VA EA, TRM, and Standards Profile 2
Figure 3: Relationship of EA Implementation Knowledge Base Components 2

1. Introduction

The VA Technical Reference Model (TRM), along with the VA Standards Profile and the VA Best Practices Reference, is intended to form a knowledge-base to provide a common conceptual framework, and define a common vocabulary and a set of services and interfaces that are, or will be, common to VA systems. This will enable the diverse components within VA to better coordinate acquisition, development, and interoperability, and accomplish the goals set forth in the One-VA Enterprise Architecture. The TRM is a source of knowledge from which project managers and developers can obtain useful information about the standards, techniques and technologies that are approved for use or are currently applied at VA. In addition to the typical discussion of IT services, functions and associated standards, found in most TRMs, the VA TRM attempts, where possible, to develop integrated views across orthogonal IT disciplines, so that project managers may integrate many technologies in order to deliver a complete solution to satisfy a VA business requirement.

The TRM is also a tool for the dissemination of technical information across the widely dispersed VA IT community. It is intended to promote integration and interoperability within the VA information technology infrastructure, to facilitate component reuse, to share lessons learned, and to help increase development efficiency.

The TRM document is accessible on the VA intranet. In its Web-enabled form, the TRM provides a vehicle for soliciting reviews and comments on proposed standards and best practices from the vast VA technical community. The TRM is intended to function, in general usage, as a paperless system.

A TRM hardcopy is produced for audit and oversight purposed on a semi-annual basis. The hardcopy is not published for wide dissemination; it provides only a limited subset of the information and functionality available from the Web site.

The VA TRM, Standards Profile and Best Practices Reference are the collaborative product of the VA IT and Business Communities, developed within the Enterprise Architecture governance process. These documents reflect the Department's agreement on the standards to be used in building and acquiring information systems and they will evolve with changes in technology and VA business objectives.

1.1 Background

The Clinger-Cohen Act of 1996 (Public Law 104-106) assigns the Chief Information Officer (CIO) with the responsibility to develop, maintain and facilitate the implementation of an information technology architecture. The Department of Veteran Affairs has embarked on this challenge to deliver a One-VA enterprise architecture through the auspices of the Information Technology Board (ITB) and the Enterprise Architecture Council (EAC). The members of the ITB and EAC are VA business and technology managers, who have been charged with the development and definition of the

enterprise architecture. A key component of the enterprise architecture is the Technical Reference Model.

The Technical Reference Model (TRM) is an integral component of an enterprise architecture and is required by the Office of Management and Budget (OMB) as part of a Federal Information Technology Architecture (OMB M-97-16). The purpose of the TRM is to provide a common technical vocabulary so that VA, its three Administrations and its two hundred major facilities can efficiently coordinate acquisition and development, and support VA's information systems.

The TRM provides a taxonomy for identifying a discrete set of conceptual layers, entities, interfaces and diagrams which, in turn, direct the reader to the specifications of related standards. The VA TRM is rooted in the concept of an open systems environment and through its application supports portable, scalable, and interoperable applications through standard services, interfaces, data formats, and protocols.

The OMB Memorandum of June 1997, concerning IT architectures calls for a technical reference model and a profile of standards.

> "The Technical Reference Model identifies and describes the information services used throughout the agency.... The standards profile defines a set of IT standards that supports the services articulated in the Technical Reference Model; they are the cornerstone of interoperability... Together with the Technical Reference Model, the Standards Profile enables the development and acquisition of standardized systems to cost effectively meet the business needs of the agency."

1.2 Scope

The VA TRM is intended to be applied to all VA information systems and information technology applications at all VA organizational levels and environments. The VA TRM provides insight and guidance in the development of technical and system architectures that satisfy requirements across missions, and in particular where interoperability, reuse, and open systems, which are desirable. The TRM guides the selection of interfaces, services and products in support of the VA Enterprise Architecture. The scope of the VA TRM is sufficiently broad to assist in addressing a wide range of problems and system configurations.

Exceptions to this policy may be granted, by waiver, after the project sponsor has obtained the approval of the VA Chief Information Officer. The waiver must develop compelling business and technical arguments for consideration by the VA CIO.

1.3 Purpose

The purpose of this Technical Reference Model is to provide guidance on use of approved and emerging technology, information technology standards, industry best practices and implementation models that define the VA target environment. This guidance supports the acquisition, development, integration, deployment and support of

information systems and infrastructure at the Department of Veteran Affairs. This will enable interoperability, reusability, and information sharing across the VA enterprise, and thereby will improve service to veterans and enhance accountability and efficiency in the use of IT resources. Additionally, the focus on the strategic insertion of emerging and appropriate technologies into the VA target environment provides potential for cost savings associated with replacing older, cumbersome and less supportable technology.

This Technical Reference Model is also intended to provide information on technologies, configurations and standards in use or being considered within VA and to provide additional sources for reference.

1.4 Goals

Establishing and communicating a comprehensive set of approved standards and best practices, consistently applied across the VA enterprise, will enable VA to

- Promote vendor independence through the use of standards based products and interchangeable components;
- Improve operational productivity through the use of consistent interfaces;
- Improve interoperability, system reuse and information sharing across business units and administrations;
- Improve compliance with security requirements;
- Improve development efficiency; and
- Improve scalability.

1.5 Audience

This document is intended for use by information technology managers, project sponsors, information architects, developers and their supporting contractors.

It will provide guidance in:

- Understanding the existing and emerging VA IT infrastructure and application development environment; and in
- Acquiring, developing and deploying systems that are consistent with that infrastructure and environment.

1.6 Approach

The fundamental constructs upon which this TRM has been developed are a series of widely accepted, complementary models that are central to contemporary IT system development:

- The System Development Lifecycle Model;
- The IEEE Open System Environment (OSE) reference model;
- The Open Systems Interconnection (OSI) Seven Layer Reference Model; and
- The Three-Tiered Architecture Model for application design.

1.7 Commercial off-the-Shelf (COTS) and Government off-the-Shelf (GOTS)

The TRM provides consistency of user and support application by a broader VA community to address interoperability, open systems, acquisition, and management issues associated with Commercial off-the-Shelf (COTS) and Government off-the-Shelf (GOTS) products.

The TRM promotes use of both GOTS and COTS to achieve the goals for developing applications and promoting software reuse to support the broad range of activities integral to any VA organization. To satisfy these goals, functional user and support applications development may include previously developed reusable code that could satisfy the new functional requirements. Such use of COTS and GOTS reusable code and applications is encouraged. It is recognized that the preference for COTS or GOTS will depend on the specific history and future requirements for development, assessed on a case-by-case basis.

2. TRM Overview

This section presents an overview of the Technical Reference Model and its relationship to the Enterprise Architecture. The TRM is one component of a larger knowledge base of resources that architects will use to implement the VA EA.

2.1 VA Enterprise Architecture Summary

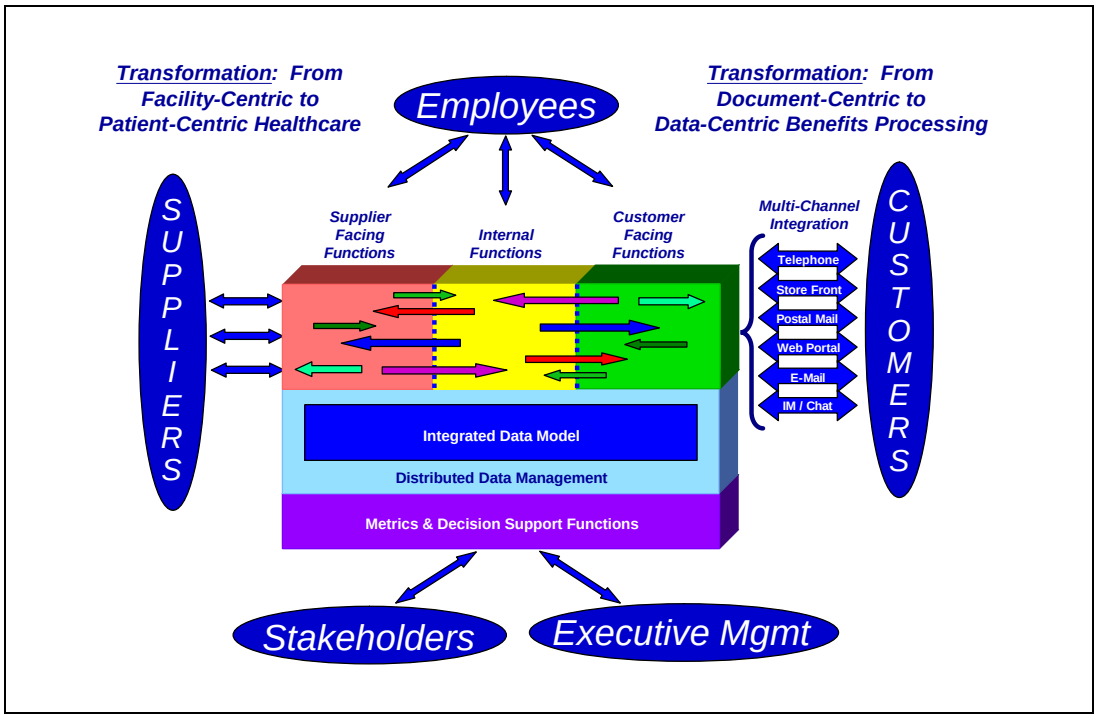

Figure 1: Enterprise Architecture Model Front View

The purpose of this subsection is to highlight and summarize the VA EA model shown in Figure 1. The explanation below discusses the interactions, interfaces, and information management between the following parts of the EA model: People, Enterprise Functions, Information Data Model, Decision Support Function Metrics, and Cross functional Applications between VA's lines of business. This is shown in the top layer of the model. The three layers below the top layer, (green, purple and red), represent examples of cross cutting applications or projects in VA.

People are represented by ovals in the diagram that interact with VA lines of business using functions implemented through VA IT systems.

- Suppliers are vendors of products and services to VA.
- Employees include those in VHA, VBA, NCA and associated staff offices.
- Customers can include internal and external personnel who interact with VA employees, veterans, beneficiaries, third-party advocates, agents or the general public.

- Stakeholders include governance parties, program managers, intra-departmental personnel, citizens, and other key entities that have a particular interest in VA.
- Executive management is senior management and decision makers within VA.

The three functions shown in the model, Supplier Facing Functions, Internal Functions and Customer Facing Functions, map to the Enterprise Business Functions (EBFs) and Key Enabling Functions (KEFs) in the EA Document. VA employees interface to all three of these functions. Suppliers and Customers interface with their respective functions.

Within the Supplier Functions, Internal Functions and Customer Facing functions, shown on the top layer of the model, interactions, processes and transactions occur dynamically to provide VA services.

The Information Data Model section of the top layer represents the logical data classes required to characterize the enterprise as a whole. These data classes form the basis for any solution implementation for the three functions: Supplier Functions, Internal Functions and Customer Facing Functions.

Metrics and Decision Support Functions shown on the top layer of the model represent how well and to what extent the stated goals of the VA and executive management are achieved.

Distributed Applications and Data shown on the top layer of the model are cross functional applications, projects or initiatives, in the EA. Through the use of this integrated data model and common IT system infrastructure the objectives of the EA are achievable.

2.2 Relationship of the VA Enterprise Architecture, TRM, and Standards Profile

On Wednesday, April 4, 2001, the Secretary of Veterans Affairs (VA) testified before the House Veterans' Affairs Subcommittee on Investigations and Oversight and promised to reform the current out-of-date information technology architecture in use at the VA. Subsequently in April 2002, the VA published the "One-VA Enterprise Architecture Implementation Plan: FY 2002."

This One-VA EA Implementation Plan serves as the critical reference tool for the VA enterprise architects, executives, program/business managers, and information technology managers and workers involved in the development and execution of the One-VA EA. In addition, the plan details how the Department will evolve its One-VA EA on an incremental basis each fiscal year.

The primary purpose of the One-VA EA is to inform, guide and manage the decisions of the enterprise, especially as they pertain to IT investments. The VA's Enterprise Architecture mission is to "develop and implement an evolutionary, high-performance

One-VA information technology architecture aligned with our program/business goals that enables enterprise-wide data integration."

The One-VA EA is the "blueprint" for systematically defining and documenting the organization's desired (target) environment. Development of the One-VA EA is an evolutionary process that spans multiple years. As a result, this Enterprise Architecture provides the overarching architectural guidance for this evolutionary process and the near term opportunities for incrementally evolving the "As Is" architecture to the "To Be" architecture.

The VA TRM relates directly to the VA EA in two ways. First, the EA defines the overall enterprise architecture and what the architecture is to accomplish. It thus serves as a source of requirement for the TRM. Secondly, the TRM defines, describes, and integrates the technology service descriptions and standards that should be used by anyone involved in developing systems that must exchange information or interoperate with other systems within the VA. The TRM is a guide to developing and implementing the EA.

The TRM also provides a common framework and a common vocabulary (i.e., services, interfaces, relationships and reference to preferred standards) to assist in identifying interoperability relationships and resolution of open systems issues. The TRM is not an architecture, but is to be used with the VA Enterprise Architecture to build the One-VA.

The Standards Profile is the set of standards to be used in implementing the EA. It is the set of "building codes" for constructing the One-VA. The TRM provides a taxonomy for categorizing services to be provided while the Standards Profile defines the various standards against which services are to be built.

Figure 2 shows how these components are inter-related. As described earlier, there are periodic reviews of business needs and technology advances that will trigger updates to each of these components. Thus, Figure 2 should be seen as a ongoing process where a changes in one component may trigger an update to another.

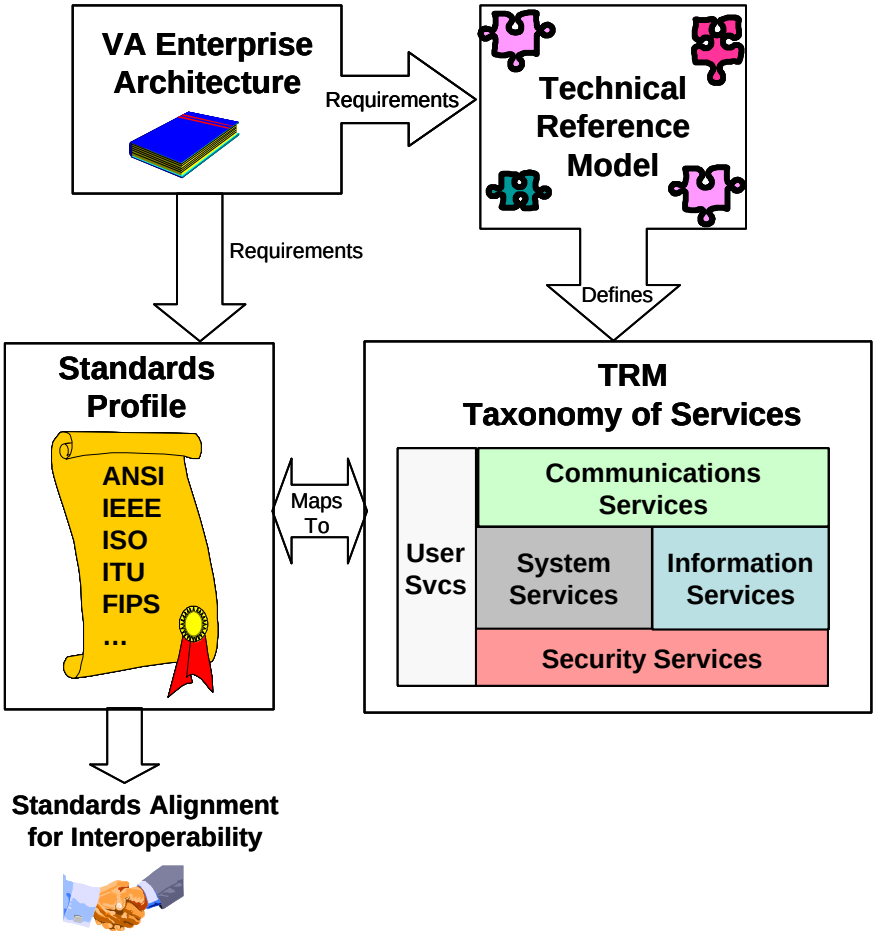

Figure 2: Relationship of the One-VA EA, TRM, and Standards Profile

2.3 Overview of EA Implementation Knowledge Base

The VA Technical Reference Model is intended to provide a rich variety of views into the standards, design conventions and best practices implemented or preferred at VA. These views are intended to support the needs of the project designers, developers and managers involved in IT infrastructure development.

Figure 3 depicts the relationship between the TRM elements and their supporting processes.

The three-part TRM knowledge base, consisting of the Technical Reference Model, the Standards Profile and the Best Practices Compendium, is shown without background coloring. The three-column configuration in the TRM view is analogous to the organization of the TRM web site in which:

- The left column organizes general background information;

- The center column consists of detailed views, in the form of a service and function taxonomy; and
- The right column consists of integrated views which cross function and service boundaries to address the requirements of typical IT development projects.

The **gray** schematic illustrates the initial seeding of the knowledge base from predecessor TRMs developed by VA and other departments. This process calls for development of a TRM recommendation by the Enterprise Architecture Council for approval by the Information Technology Board.

The **green** schematic illustrates the ad-hoc process of project developers referring to the TRM, standards profile and best practices compendium. Over the course of the project's development lifecycle, developers will also contribute to the best practices portion off the knowledge base.

The **yellow** schematic illustrates a semi-annual technical refresh process, which will be the source of technology infusion and technology retirement. At the end of this semi-annual cycle, every standard in the standards profile is assessed as either emerging, mature, retiring, or obsolete. This process is driven by two input sources:

- An independent industry technology assessment, which is used to identifies every standard in the standards profile as either emerging, mature, retiring, or obsolete; and
- A VA business assessment which inserts the consequences of business and policy determinations into the TRM.

The process illustrated in **blue** is an ongoing content management task, performed by the Office of the Chief Architect to maintain the TRM database and web site. Through this process:

- The web site TRM document is updated whenever a significant content change occurs; and
- The hardcopy TRM synopsis is updated semi-annually, in conjunction with adopting changes from the technology refreshment process.

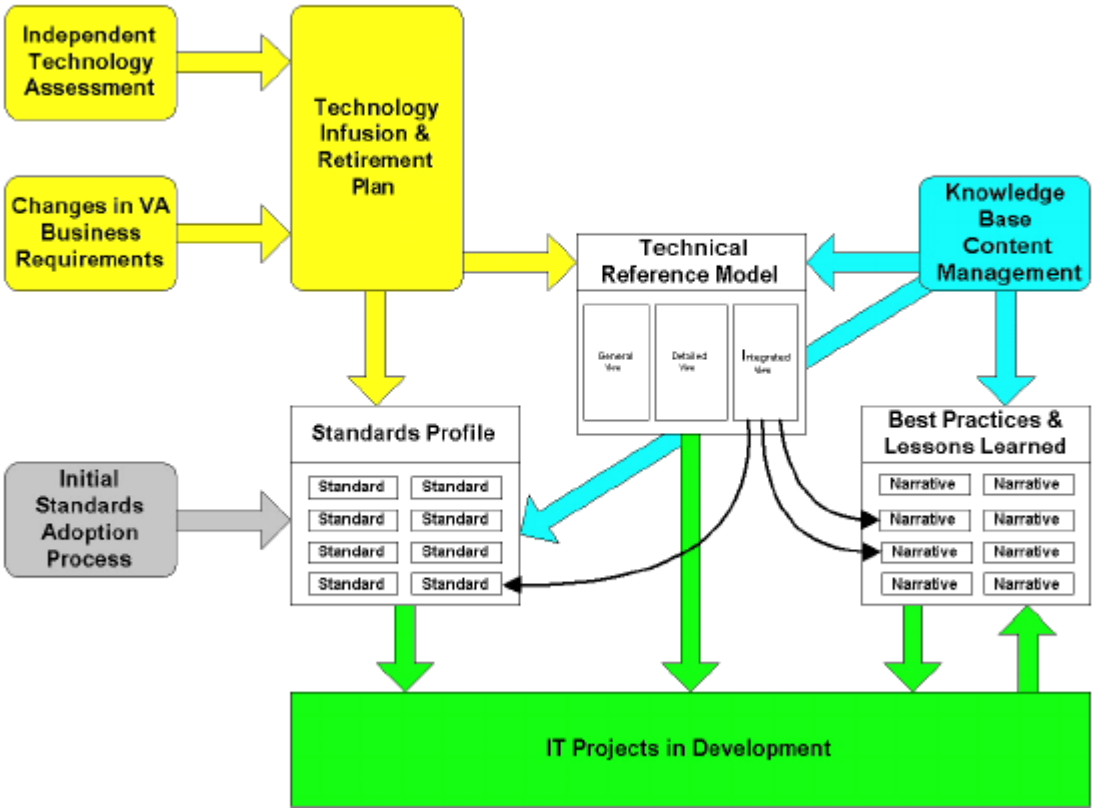

Figure 3: Relationship of EA Implementation Knowledge Base Components

2.3.1 Standards Submission and Adoption Process

Proposed standards may be submitted to the VA Chief Information Officer by any interested party for review and for consideration of adoption by VA. The standards adoption procedure is derived from the VA IT governance process.

The proposed standard is reviewed by the Enterprise Architecture Council and then forwarded, with recommendations, to the Information Technology Board for possible adoption.

2.3.2 Standards Compliance and Waiver Policy

Project sponsors and designers are required to adhere to the applicable standards, policies and mandatory best practices, established by the Information Technology Board, when proposing and developing IT initiatives within VA. Exceptions to this policy may be granted, by waiver, after the project sponsor has obtained the approval of the Chief Information Officer. The waiver request must present compelling business and technical arguments for consideration by the CIO.

2.3.3 Technology Refresh Process

The TRM and Standards Profile is maintained and periodically upgraded by the Office of the Chief Architect. Changes to the TRM and standards profile are posted, as they occur, to the VA Intranet.

The TRM and VA standards are formally reviewed in conjunction with a semi-annual independent industry technical assessment and a semi-annual business requirement review. Emerging technologies will be assessed for strategic insertion into the target VA enterprise.

These periodic reviews are evaluated by the Enterprise Architecture Council for consideration and adoption by the Information Technology Board. Changes resulting from this Technology Refresh Process are then published on the Intranet and in the hardcopy version of the TRM.

2.4 TRM Structure

2.4.1 Standards Profile View

The VA Standards Profile may be viewed directly by Standard Number within Standards Organization. Abstracts of each standard are maintained within the VA EA Implementation Knowledge Base, along with links to the actual standards text on the standards organization's web site. Standards may also be viewed from various links within the TRM.

2.4.2 Best Practices Compendium View

Best Practices may be derived from industry sources or may be internal to VA. VA's Best Practices may be viewed directly, in the sequence of adoption by VA, or they may be viewed through links within the TRM.

2.4.3 Service and Function Taxonomy View

The TRM decomposes IT functions and services into a detailed taxonomy based on the models described in section 1.6 above. This taxonomy appears in the center column on the web site and in the table of contents of the hardcopy document. Function and service entries provide links to the related abstracts for each function and service which, in turn, provides a link to each related standard.

2.4.4 Integrated Project Development Views

The TRM also supports a series of integrated views, which cut across technical disciplines, to illustrate typical configurations and planning issues that must be addressed for the development of various system configurations.

2.5 TRM Document Management

The VA TRM document is available on the VA TRM Intranet web site. This web site will be updated on an ad-hoc basis, as significant changes occur, throughout the year.

The TRM document is revised in conjunction with the semi-annual technical assessment and business requirement review. The TRM document is submitted to the EA Council and IT Board for approval and release.

The VA TRM knowledge base is designed to be a paperless process, with the hardcopy produced in very limited distribution to satisfy oversight, review and audit requirements.

3. TRM Services and Taxonomy

This section categorizes and describes the various interfaces and services that are to be supported. As defined by the IEEE OSE Reference Model, an interface is a boundary across which two systems or domains communicate. An interface might be a hardware connector used to link one or more devices, or it might be a convention used to allow communication between two software systems. Interface definitions are usually expressed as a particular protocol that defines how two systems will communicate. As defined by IEEE, a service is a collection of components organized to accomplish a specific function or set of functions. an action or function performed by one entity at the request of another.

3.1 System Services

3.1.1 Language Services

Language services provide tools, syntax, and definitions for professional system developers to develop and maintain applications. Language services include the following:

- Programming Languages – A programming language is a formally defined language in which computer programs are written.
- Scripting Languages – Scripting language is a loose term for any language that is weakly typed or untyped and has little or no provision for complex data structures.
- Graphical User Interfaces – Graphical User Interface (GUI) is the use of pictures rather than just words to represent the input and output of a program.

3.1.2 Operating System Services

Operating systems 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 will shield applications from the implementation details of the machine, and efficiently distribute hardware and operating system services among various contending application tasks.

An operating system typically includes the following services:

- Process and Thread Management – This service relates to the creation, management, and deletion of processes, tasks and threads.
- Environment Management – This service provides applications with access to a variety of information that relates to the application environment.
- Internal Communications and Synchronization – This service coordinates and synchronizes applications and components that run independently and simultaneously on an application platform.

- Input Output Facilities – This service provides generalized synchronous and asynchronous device input/output operations, often through language services.
- File Storage Management – This service enables mass storage in the form of directories, sub-directories, and files that are available within an application platform.
- Event, Error and Exception Management – This service provides a common facility for the generation and communication of asynchronous events within the application platform and with application programs.
- Time and Timer Services – The time-related services provide a site-independent, machine-readable date and time, including absolute and relative time.
- Memory Management – Memory management is a collection of techniques for providing sufficient memory to one or more processes in a computer system, especially when the system does not have enough physical memory to satisfy all processes' requirements simultaneously.
- System Management Facilities – This service allows system administrators to manage users, configurations, licenses, performance, availability, fault tolerance, security, capacity, and backup and restore services.

3.1.3 Supporting Application Services

3.1.3.1 Shared Services

Shared Services are infrastructure applications that are used to provide common office functions for day-to-day operations. These services are standardized across multiple VA business areas to ensure interoperability across the business lines. Such applications are typically office automation COTS products or other applications that automate information flow within the VA. Shared services include the following types of services:

- Directory Services – Directory services help people and applications find the names and addresses of objects and services available to an application.
- Electronic Mail Services – Electronic mail services provide the capability to send, receive, forward, store, display, and manage electronic messages.
- Calendar Services – Calendar services include the capability to manage personal tasks and time and to coordinate multiple personal schedules via an automated calendar.
- Naming Services – Naming services allow the use of system resources through logical names instead of hardware device naming conventions.
- File Sharing Services – File Sharing is the public or private sharing of computer data or space in a network with various levels of access privilege.
- File Transfer Services – File transfer services support the movement of text and other file structures between applications and applications systems.
- Virtual Terminal Access Services – A terminal is an electronic or electromechanical device for entering data into a computer or a communications system and displaying data received.

- Remote Command Execution Services – Services in this category allow a user or application on one machine to execute commands on another machine just as if the user or application were actually running on the remote machine.
- Remote Authentication Services – Services in this category serve to authenticate users or applications that request Remote Command Execution Services. These services are required as part of an overall security policy to protect services and systems from unauthorized remote access.
- Remote Data Access Services – Remote Data Access Services is the ability to access remotely located data as if it were on the local hardware platform.
- Remote Status Services – Remote network monitoring devices, often called monitors or probes, are instruments that exist for the purpose of managing a network.
- Multimedia Services – Multimedia services manage the human-computer interaction including text, graphics, voice and video.
- Web Access Services – Web servers are World Wide Web platforms for creating, managing, and intelligently distributing information and on-line applications.
- Web Server Support – A server process running at the web site which sends out web pages in response to HTTP requests from remote browsers.
- Web Authoring – Creating a hypertext or hypermedia document.

3.1.3.2 Desktop Services

Desktop services are generally supplied by commercial office automation products. They include:

- Spreadsheet Support – Spreadsheet services, including the capability to create, manipulate, and present information in tables or charts.
- Project Management Support – Project management services, including tools that support the planning, administration, and management of projects.
- Calculation Services – Calculation services, including the capability to perform routine and complex arithmetic calculations.
- Word Processing Services – Word processing services, including the capability to perform spell checking, document templates, formatting, etc.
- Presentation Services – Presentation services provide a look-and-feel interface to users.
- Web Browser Services – A browser for the World-Wide-Web; a program that allows a person to read hypertext.

3.1.4 Software Engineering Services

Application development projects require tools to enable efficient development, integration, and maintenance of applications. Computer-Aided Software Engineering (CASE) systems and programs assist in the automated development and maintenance of software. CASE services include tools for requirement specifications and analysis, design work and analysis, creating and testing program code, documentation, prototyping, and group communication. An adjunct to these capabilities is the ability to manage and control the configuration of software components, test data, and libraries.

3.1.4.1 Software Development Services

Application development services support the activities of software development efforts, to include the management and technical aspects of these efforts.

- Project Management – Project management services provide utilities for managing an application development effort, to include project planning, scheduling, costing, monitoring, and reviews.
- Quality Assurance – The quality assurance (QA) is to ensure that the end product is of the highest quality possible.
- Capability Maturity Model – The Capability Maturity Model for Software (SW-CMM), spearheaded by the Carnegie Melon Software Engineering Institute, provides a model for assessing the maturity of the software processes of an organization and for identifying the key practices that are required to increase the maturity of these processes. SW-CMM may be adopted and applied to application development projects as necessary to assure product quality. Document management tools exist to facilitate the tracking of CMM work products
- Software Design Tools – Design tools, generally called CASE tools, are used to create and document design and retain product artifacts.

3.1.4.2 Software Development

These services provide for developing or adapting application and system software programs and for testing, evaluating, and integrating the developed or adapted software elements into cohesive software packages. The services include source code creation and maintenance, execution preparation, and application execution at both the API and EEI levels.

Design Techniques are ways of accomplishing some aspect of a development method as compared to methods that are ways of accomplishing the entire development phase. Example techniques include the following:

- Object-Oriented
- Component-Based
- Structured
- Rapid Application Development
- eXtreme Programming
- Information Engineering.

3.1.4.3 Software Testing

Testing services support the tasks necessary in testing applications from unit, integration, regression, and performance perspectives. These services enable test data generation, dynamic analysis, simulation, and file comparison functions that support the stages of application testing. Products or programs that support these activities may be commercially available or internally developed.

Project development generally includes several forms of testing.

- Unit Testing – Unit testing is performed to ensure that the individual components meet the requirements.
- Integration Testing – Integration testing insures that collections of modules in the aggregate meet the requirements.
- Performance/Stress Testing – Stress testing utilities push the system to discover its capacity limits. These tests allow for the early detection of system performance faults so that corrective measures can be put in place.
- User Acceptance Testing – Testing at this stage may show that the system does meet the anticipated performance and functionality from the user's perspective.

3.2 Communications Services

3.2.1 Transparent Network Services

Transparent network services are typically provided by the core system services but can be extended across a network with no modifications to the applications.

3.2.2 Network Management Services

Network managed services provide system administrators with the ability to configure, control, and maintain the enterprise network. Typical services include the following:

- Performance Management – The goal of performance management is to measure and make available various aspects of network and systems performance so that performance can be maintained at an acceptable level.
- Fault Management – The EA must be robust and fault tolerant. Fault Management services provide the ability to monitor the enterprise to detect and correct fault conditions, such as restarting failed processes or switching over to a standby system when a primary server fails.
- Account Management – Account management allows the system administrator to create and manage user accounts.
- Configuration Management – The goal of configuration management is to monitor network and system configuration information so that changes that may impact the enterprise performance will be tracked and managed.
- Security Management – The goal of security management is to control access to network resources according to local guidelines so that the network cannot be sabotaged (intentionally or unintentionally) and sensitive information cannot be accessed by those without appropriate authorization.

3.2.3 External Environment Interface

- Network Protocols – The network will support standard protocols such as TCP/IP, UDP, HTTP etc. Wireless protocols will also be supported.
- Network Services – The network will support LAN, WAN, MAN configurations. These services also include satellite communications and wireless

communications services and are grouped with Network Services because the specific physical makeup of the network should in general be transparent to applications.

- Remote Access Services – Remote Access refers to any technology that enables geographically dispersed users to connect to enterprise network services and applications. This access is typically over dial-up connection, although it can include WAN connections.
- Network Multi-Media Services – The EA will support multi-media, voice, video, and data applications that require multi-casting and streaming protocols. This requires that the network routers be capable of supporting, and be configured to support, these types of protocols.

3.3 Information Services

Information services manage information across an application platform. Information can be managed through supporting applications, document management services, data management services, data interchange services, and transaction processing services.

3.3.1 Document Management Services

Document Management Services manage and track correspondence and other important documents at the office level. Document management includes:

- Document Repository
- Document Registry
- Records Management
- Document Interchange
- Scheduling
- Monitoring
- Workflow
- Distribution.

3.3.2 Data Management Services

A general term that collectively describes those functions of a system that provide access to hardware, enforce data storage conventions, and regulate the use of input/output devices. This also refers to a major function of operating systems that involves organizing, cataloging, locating, retrieving, storing and maintaining data. Data management services include:

- Database – A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures such as retrieving information, drawing conclusions, and making decisions.
- Data Administration – Data administration defines the standardization and registration of individual data element types to meet the requirements for data sharing and interoperability among the information systems throughout the enterprise. Data administration functions include procedures, guidelines, and

methods for effective data planning, analysis, standards, modeling, configuration management, storage, retrieval, protection, validation, and documentation. These services often include mechanisms for schema definition, data access, data manipulation, and data integrity services. Data administration also refers to an organization within a company that is charged with the definition, organization, management and control of data, not its processing. Data administration facilitates common methods and techniques in the development and use of data standards.

- Database Utilities – A Database Utility usually refers to tools/applications (usually provided by a specific database vendor) for the data transfer, maintenance and database administration of the data records maintained within a database. They provide the capability to retrieve, organize, and manipulate data extracted from a database management system.
- Database Management Systems – A database management system provides logical, physical, interrogation and system control.
- Data Registry and Repository – The registry provides information about the object, including the location of the object. A repository is where the object resides.
- Data Warehouse – A repository of consistent historical data that can be easily accessed and manipulated for decision support. It is typically a subject database that allows users to tap into a company's vast store of operational data to track and respond to business trends and facilitate forecasting and planning efforts.
- File Management – The maintenance and administration of records on a system, network or workstation.
- Transaction Processing – A database transaction is a "unit of work" consisting of a series of operations that must be completed in total. Typically, this involves predetermined sequences of data entry, validation, display, and update or inquiry against a file or a database. It also includes services to prioritize and track transactions. These services may include support for distribution of transactions to a combination of local and remote processors.

3.4 User Services

User services enable users to share information with the application via the external environment interface. They also define how users may interact with an application. They provide a consistent way for developers, users, and administrators to use a system to gain access to application programs, operating systems, and various system utilities. The user interface is a combination of menus, screen design, keyboard commands, command language statements, and help screens, which control the way a user interacts with a computer. A user interface also includes the use of mice, touch screens, and other pieces of input hardware that control interaction with a computer.

3.4.1 Usability and Accessibility

Section 508 of the Rehabilitation Act Amendments of 1998 requires that electronic and information technology developed, procured, maintained, or used by the Federal

government be accessible to people with disabilities. Detailed information can be found at http://www.access-board.gov/508.htm and http://www.section508.gov/.

3.4.2 User Interface

These services facilitate user interaction with applications. Services provided typically include:

- Command I/O
- Error Detection/Suppression
- Command Abortion/Suspension
- Shells and Utilities
- Character-Based User Interface
- Presentation Management
- Forms Management
- Screen Management
- Input Device Management.

3.4.3 Windowing Systems

Most modern computer systems include a windowing system as a more convenient interface mechanism than older command line, character-based interfaces. Such systems usually include the following services:

- Window Management Services
- Desktop Management
- Event Handling
- Error Handling
- Inter-Client Communications
- Input Device Management
- Screen Management
- User Preference Management.

3.4.4 Graphics

These services provide functions required for creating, storing, retrieving, and manipulating two- and three-dimensional images in a device-independent manner.

3.5 Security Services

3.5.1 Technical Security Services

- Identification – The process to identify the user, typically via a user ID. Identification enables one subject to recognize another subject or object.
- Authentication – The process of confirming an identity claimed by or for an entity. Reliable authentication is needed to enforce access control, to determine

who is authorized to receive or modify information, to enforce accountability, and to achieve non-repudiation.

- Access Control and Authorization – Controlling access to system data and resources based on a user's identity or operational role. Access control services protect against unauthorized access to resources, such as processing, communications, or information resources. Access control is the primary means for enforcing authorization.
- Accountability – Accountability is a fundamental principle underlying any security policy. Individuals who take actions that are governed by a security policy must be accountable for their actions. Accountability services assist in providing accountability and the audit of users and their actions, the protection of authentication data, active user status information, and password authentication
- Data Integrity – Data integrity provides proof that data has not been altered or destroyed in an unauthorized manner while en route from a sender to its intended recipient. Data integrity applies to data in permanent data stores and to the data embedded in communications messages.
- Non-Repudiation – A cryptographic situation in which someone who digitally "signs" a document using his/her digital signature, ensuring document integrity and authenticity, cannot claim that he didn't originate the document, or that the document was altered after he signed it.
- Availability – The assurance that authorized users will have reliable and timely access to required resources (including information, system services, communication services, etc.). Availability applies to both uptime and access time.
- Confidentiality and Data Encryption – Confidentiality refers to keeping data in an electronic exchange private; i.e., preventing unauthorized individuals or processes from gaining access to documents, transactions or messages.
- Malicious Code Detection – Malicious code refers to programs that are written intentionally to carry out annoying or harmful actions.. Types of malicious code include Trojan horses, computer viruses, and worms.
- Auditing – The process of collecting data generated by system, network, application, and user activities. Auditing is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

3.5.2 Physical and Environmental Control

Physical and environment control refers to that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard against espionage, sabotage, damage, and theft. An organization's physical and environmental security program should, at a minimum, address the following topics:

- Physical Access Controls
- Fire Safety Factors
- Failure of Supporting Utilities
- Structural Collapse

- Plumbing Leaks
- Interception of Data
- Electrical
- Media Storage
- Mobile and Portable Systems.

3.5.3 Administrative Security Services

3.5.3.1 Enumeration of Individuals

This refers to individuals identified as having access rights and/or authorization to access an information system, usually based on roles and responsibilities of the individual.

3.5.3.2 Certification

The process of certification is a comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements. Certification of the system is based on the documented results of design reviews, system tests, and the recommendations of the testing teams. Certification is a requirement for all VA systems.

VA Directive 6214, VA IT Security Certification and Accreditation Program (ITSCAP) is the certification and accreditation program of VA and has officially been added to the VA's information security policy. It is compatible with other Federal, national and international certification and accreditation methodologies. The VA ITSCAP process is based on the National Information Assurance Certification and Accreditation Process (NIACAP).

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:

- It meets all Federal and agency-specific policies, regulations, and standards.
- All installed security safeguards are adequate and appropriate for the protection requirements of the system.

Systems will be re-certified whenever 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.

- 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.

- 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 will be re-accredited when major changes occur to the system or every 3 years, whichever occurs first.

3.5.3.3 Chain-of-Trust Partnership Agreement

A chain-of-trust partnership agreement is a contract entered into by two business partners in which it is agreed to exchange data and that the first party will transmit information to the second party, where it is agreed that the data transmitted will be protected between the partners. The sender and receiver depend upon each other to maintain the integrity and confidentiality of the transmitted information. Multiple such two-party contracts may be involved in moving information from the originator to the ultimate recipient. For example, a provider may contract with a clearing house to transmit claims to the clearing house; the clearing house, in turn, may contract with another clearing house or with a payer for the further transmittal of those same claims. Chain of trust agreements are required by the Health Insurance Portability and Accountability Act (HIPAA).

A Chain of Trust Agreement’s purpose is to ensure that a uniform level of security is applied at every "link" in the chain where information passes from one party to another. Verification of uniformity at each link is necessary for optimal protection of transmitted data. The VA ITSCAP program requires interface agreements between a VA network and any other network that wants to connect to it.

It is very important that the parties to these contracts agree to security mechanisms that:

- ensure that all transmissions of data are authorized;
- protect the integrity and confidentiality of patient information; and
- protect business records and data from improper access.

The Agreement should obligate each party to adopt some form of electronic identification (electronic signatures are an example) that unequivocally attributes data transmissions and to agree upon procedures for acknowledging the proper receipt of data. Without these contractual obligations, the parties can't assume any reasonable level of comfort regarding the integrity of transmitted data. Likewise, without a mechanism to authenticate the origin of transmitted data, it is impossible to establish that the data has not been compromised.

In order to maintain the integrity of the data passed along this chain, the Agreement should state that the parties will take reasonable measures to maintain equipment, software and other materials that have the potential to negatively impact data and/or the ability to transmit data.

3.5.4 Security Management Services

3.5.4.1 Event and Alarm Monitoring and Reporting

Event monitoring and reporting is the process of recording specific events in an audit log by an operating system, IDS, firewall, or other system component. This activity provides an audit trail that is used to detect unauthorized activity. It is possible to configure an alarm or notification when certain events occur.

Information about failed logins, failed file accesses, planted Trojan Horses, and other system events can be found easily in the audit logs. However, system audit logs contain limited information about network activities. Attacks such as Ping of Death and SYN Flood are not surfaced in the audit trail. Instead, these attacks must be detected at the IP layer itself by the operating system, a firewall, or a separately attached network IDS. Conversely, information about buffer overflow attacks and higher-level system abstractions (UID, GID, file, and printer) does appear in the audit trail. Therefore, a system-level IDS can detect intrusions and record events that a network-level IDS cannot and vice versa.

A layered or defense-in-depth approach is necessary for event monitoring. Network intrusion detection is the process of monitoring events occurring in the network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network and is accomplished by the use of an Intrusion Detection System. The IDS should not be the first line of defense. Firewalls and filtering routers may also be configured to monitor specific events. Operating systems should be configured to monitor system, application, and security events.

Audit logs are the most comprehensive source of system activities. Network logs are equally important. Logs generated by applications also must be kept.

3.5.4.2 Reviews and Audit Trails

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 trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.

The following considerations should be taken into account for review of audit trails:

- 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.
- Guidelines should be developed 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.
- Audit trail review can be easier if the audit trail function can be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.
- 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.

3.5.4.3 Security Policy and Procedure Development/Enforcement

Security policy provides overall governance for a particular organization as a whole or a component of it. It defines security posture, provides a framework for lower level procedures and creates a benchmark for assessing security posture. Security policy is a high level document that should not be affected by changes in technology. It contains an organization's security mission statement and defines consequences of failure to comply. Security policy may be published on an organization's web site or physically distributed to employees, partners, etc.

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.

Policy Development:

1. Identify participants, i.e., who develops, who implements, and who authorizes.
2. Determine drivers, i.e., government requirements
3. Review existing policy documentation
4. Establish categories for policy:
    - Based on ISC2 domains
    - Based on RFC 2527 (or other standards)
    - Based on Common Criteria
    - Based on ISO 17799
5. Establish policy components:
    - Policy number
    - Date of issuance
    - Status
    - Revision history
    - References and related documents
    - Purpose
    - Applicability and scope
    - Policy
    - Responsibilities
    - Policy change procedure

Procedures Development:

1. Identify participants, i.e., who develops, who implements, and who authorizes.
2. Identify affected system(s)
3. Determine drivers, i.e., government requirements, applicable standards, etc.
4. Review existing documentation
5. Establish procedural components:
    - ID number
    - Date
    - Status
    - Revision history
    - References and related documents
    - Purpose
    - Detailed procedures
    - Responsibilities
    - Change (configuration management) procedure

3.5.5 Security Mechanisms

3.5.5.1 Network Boundary Protection

3.5.5.1.1 Firewalls

A firewall is a collection of hardware and software components that is used to selectively allow external entities (e.g. users on the Internet) access to information systems located "behind" the firewall. A firewall is installed between an information system (or intra-netted systems) and a public network.

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. There are three primary categories of network firewalls:

- Packet filter
- Stateful packet filter
- Application layer gateway

A firewall intercepts and controls traffic between networks with differing levels of trust. It is part of the network perimeter defense of an organization and should enforce a network security policy and provide an audit trail. A firewall is a good place to support strong user authentication as well as private or confidential communications between firewalls.

There are several types of firewalls, ranging from boundary routers that can provide access control on Internet Protocol packets, to more powerful firewalls that can close more vulnerabilities in the TCP/IP protocol suite, to even more powerful firewalls that

can filter on the content of the traffic. Traditional firewalls are gateways between trusted and un-trusted networks.

Refer to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-41 Guidelines on Firewalls and Firewall Policy at http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf for recommendations.

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.

3.5.5.1.2 Intrusion Detection Devices

Intrusion detection systems (IDSs) are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems. Distinguishing features of an IDS are the type of engine that makes decisions about intrusions, whether analysis occurs in real time as the events are received, and the source of data for events.

Network Intrusion Detection Systems (NIDS) analyze network traffic for attacks that exploit the connections between computers and the data that can be accessed via a network connection. NIDS can detect the broadest range of attacks on corporate information assets that may include Denial of Service attacks that are aimed at stopping the enterprise or its customer's from accessing corporate IT assets. The role of the network IDS is to flag and sometimes stop an attack before it gets to information assets or causes damage. NIDS are effective for monitoring both inbound and outbound network traffic.

The National Institute of Standards and Technology has released guidance on intrusion-detection systems, outlining all the factors agencies need to consider when integrating these security systems into their networks. Refer to NIST Special Publication on Intrusion Detection Systems located at: http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf.

The IDS should not be 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 outside the firewall provides a pre-emptive capability in identifying the threat in the early stages of reconnaissance (i.e. scanning and probing).

Best Practice dictates the following for an intrusion detection system design:

- Use correlation engines to customize the analysis and investigation
- Use taps (splitters) or port spanning on switches to collect data on switched networks
- Configure DMZ filters so they do not ignore internal systems' traffic
- Implement egress filtering (allow only outbound traffic if addresses correspond to your reserved internet addresses) Refer to www.sans.org/y2k/egress.htm
- Deploy Network Intrusion Detection Systems at high volume locations
- Pace additional sensors from time to time on networks as random spot checks
- At the very least deploy Host-Based Intrusion Detection Systems on all server systems

The preferred implementation of an enterprise IDS is to deploy a combination of both Network and Host-Based IDS as part of a balanced and layered in-depth defense.

3.5.5.1.3 VPN Encryption

VPN encryption can be used to provide confidentiality and integrity of data transmitted across a public inter-network. In addition, VPN encryption can provide authentication of the remote system that encrypted the data. When integrated into suitable system architectures, VPN encryption allows secure “tunnels” to be established across insecure inter-networks. This allows a private intranet to run (securely) over a public internet.

The National Institute of Technology and Standards (NIST), after approval of the Secretary of Commerce, issues standards that specify security requirements for federal government information processing systems that process sensitive but unclassified information. The Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules (FIPS PUB 140-2) specifies the standards that the cryptographic module in a VPN system must be validated against before the system can be selected for the network.

Many commercial vendors produce software and hardware that can provide VPN encryption for unclassified or sensitive but unclassified data. VPN encryption based on the IP security (IPSEC) standard is now the most commonly used VPN protocol. IPSEC can provide data confidentiality, integrity, and authentication by encrypting packets at the IP layer. The IPSEC standard has been designed to allow for “drop-in” employment of encryption algorithms. For data confidentiality, IPSEC currently supports various algorithms including DES, 3DES, RC5, IDEA, CAST128, and Blowfish. (CAST, RC-4, and IDEA are not accepted NIST algorithms.) Support for the AES algorithm was approved with FIPS PUB 187. For data integrity and authentication, IPSEC currently supports keyed MD5 and SHA-1. The IPSEC standard also allows for employment of various key management and distribution schemes. The simplest is based on manual pre-placement of a shared key on the VPN server and on each client. The Internet Security Association and Key Management Protocol (ISAKMP)/Oakley provides more automated and scalable key management and distribution. In addition, many VPN systems will now support PKI for user authentication.

COTS VPN mechanisms may be used for encryption of unclassified data, and of classified data that will be handled at its original level (e.g., for privacy of secret data across the classified networks). To provide for interoperability, IPSEC/IKE based mechanisms should be used if available. IPSEC mechanisms will utilize 3DES (with at least a 128 bit key) or AES for encryption. FIPS 140-2 certification of 3DES and AES implementations is recommended, for both the server and client components. Keyed SHA-1 for data authentication and integrity is preferred, but keyed MD5 is an acceptable substitute if SHA-1 is not available. An acceptable option for key management and distribution is a pre-placed secret key shared by both the server and client.

All VPN systems should support both user ID and password authentication and two-factor authentication based on the Public Key Infrastructure (PKI). PKI authentication is the preferred implementation. Details of all remote user connections shall be logged for audit purposes and all remote user connections to internal networks will allow screening by gateway firewalls, IDS, and anti-virus software as required by security policy. In addition, it is recommended that time-out safeguards be established and enforced by the VPN gateway.

All VPN systems should meet security certification and accreditation requirements and be validated by a third party.

3.5.5.1.4 Virus Detection

The process of using anti-virus software to detect viruses in resources such as e-mail messages and hard drives and eliminates any that are found. This software must be updated regularly in order to defend against new viruses.

All PC-based workstations and servers (including those using the Windows 2000, Windows NT, Windows 95, Windows 98, and Macintosh operating systems) should employ anti-virus software. Most large organizations use an anti-virus detection tool site license, enabling employees to install the software for office as well as home use. Anti-virus software should be configured to run in a background mode and scan files upon access. Updated virus detection signatures should be downloaded and installed monthly. 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.

3.5.5.1.5 Routing Authentication

By default, a router uses a Null authentication, which means that routing exchanges over a network are not authenticated. Two other authentication methods exist: Simple password authentication and Message Digest authentication (MD-5).

Simple password authentication allows a password (key) to be configured per area. Routers in the same area that want to participate in the routing domain will have to be configured with the same key. The drawback of this method is that it is vulnerable to passive attacks. Anybody with a link analyzer could easily get the password off the wire.

Message Digest authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a "message digest" that gets appended to the packet. Unlike the simple authentication, the key is not exchanged over the wire. A non-decreasing sequence number is also included in each OSPF packet to protect against replay attacks. This method also allows for uninterrupted transitions between keys. This is helpful for administrators who wish to change the OSPF password without disrupting communication. If an interface is configured with a new key, the router will send multiple copies of the same packet, each authenticated by different keys. The router will stop sending duplicate packets once it detects that all of its neighbors have adopted the new key.

When using a dynamic routing protocol that supports authentication, it is generally considered to be good security practice to enable that authentication. This prevents malicious attacks on the routing infrastructure, and can also help to prevent damage caused by misconfigured "rogue" devices on the network.

3.5.5.2 Host Protection

3.5.5.2.1 Operating System Configurations

Computer operating systems include features that allow the operating systems to provide access control for all information stored or processed. Operating systems that host services available externally through the internet, as well as those that host proprietary data internally, must be protected from unauthorized access. Operating systems are not configured, by default – that is, out of the box – for security. Additional steps must be taken to “harden” operating systems and protect them from unauthorized access.

Computer operating systems should include security profiles. The definition of the profile is established before procurement. Vendors are advised that the profile requirements are part of the procurement and test, or provide test documentation if already tested, as a part of the procurement. Test results are used in accreditation of the information system.

NSA (NSA.gov) publishes security configuration guidelines for popular operating systems. These guides are currently being used throughout the government and by numerous entities as a security baseline for their information systems.

Additionally, vulnerability scanning and penetration testing can provide valuable insight and strategies for protecting the operating system from unauthorized access. Testing should be performed externally as well as internally for a comprehensive view of vulnerabilities and the associated risk.

3.5.5.2.2 VPN Encryption

VPN encryption can be used to provide confidentiality and integrity of data transmitted across a public inter-network. In addition, VPN encryption can provide authentication of

the remote system that encrypted the data. When integrated into suitable system architectures, VPN encryption allows secure “tunnels” to be established across insecure inter-networks. This allows a private Intranet, including one containing classified material, to run (securely) over a public Internet.

VPN clients generally act as an IPSec peer that uses a specific protocol along with IPSec to negotiate, then establish an encrypted tunnel to another IPSec peer.

Many commercial vendors produce software and hardware that can provide VPN encryption for unclassified or sensitive but unclassified data. VPN encryption based on the IP security (IPSEC) standard is now the most commonly used VPN protocol. IPSEC can provide data confidentiality, integrity, and authentication by encrypting packets at the IP layer. The IPSEC standard has been designed to allow for “drop-in” employment of encryption algorithms. For data confidentiality, IPSEC currently supports various algorithms including DES, 3DES, RC5, IDEA, CAST128, and Blowfish. Support for the AES algorithm is expected to be available before the end of 2001. For data integrity and authentication, IPSEC currently supports keyed MD5 and SHA-1. The IPSEC standard also allows for employment of various key management and distribution schemes. The simplest is based on manual pre-placement of a shared key on the VPN server and on each client. The Internet Security Association and Key.

3.5.5.2.3 Personal Firewall Configuration

Host based firewalls can be software / hardware in end-systems, that provide a "security wrapper" around the host or application on that host. They provide additional security controls by limiting services to a particular host.

They provide an alternative to a gateway enclave boundary. A host-based firewall sits at one of the lowest levels within the operating system and provides an envelope that encompasses the server and all NICs – and inspects all packets going in and out. It can be managed by a security console. These firewalls are suitable for all servers attached to the internal network. Host based firewalls provide an additional layer of defense for servers located behind a traditional firewall.

Personal firewalls can be configured to allow software applications located on the host to access the local network or to act as a server, etc. Personal firewalls can also be configured to disallow access from unauthorized sources, provide event logging and alerts, and generally to protect information on the local host.

Use host-based firewalls:

- With large web portals or web farms.
- With servers that provide critical services, i.e., database servers, e-mail servers, etc
- With services that process and store critical or proprietary information, i.e., payroll, accounting, human resources, etc.

Use personal firewalls on:

- All client workstations

3.5.5.2.4 Host Intrusion Detection

Host-Based Intrusion Detection Systems (HIDS) monitor specific files, logs and registry settings on a single PC 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 PC and automatically replace altered files when changed to ensure data integrity.

Host-based IDS' provide supplemental application level detection and protection. Critical servers usually have host-based IDS' installed as a supplement to logging processes provided by the operating system. Host-based IDS' detect specific patterns associated with known security vulnerabilities. These rule-based systems are prone to obsolescence and thus require regular updates. Maintained in the same manner as virus detection, host-based IDS software is reliant on system administrator prudence.

The host based IDS should be platform independent. It should interpret all log data and the rule and filter management should not be cumbersome. It should have a wide range base of intrusion signatures. The IDS software itself should not compete too much with system memory and CPU usage. It should allow for automatic restarts. The configuration needs to be extremely flexible so that it could be deployable in a vast range of environments.

3.5.5.2.5 Virus/Mobile Code Detection

The process of using anti-virus software to detect viruses in resources such as e-mail messages and hard drives and eliminates any that are found. This software must be updated regularly in order to defend against new viruses.

All PC-based workstations and servers (including those using the Windows 2000, Windows NT, Windows 95, Windows 98, and Macintosh operating systems) should employ anti-virus software. Most large organizations use an anti-virus detection tool site license, enabling employees to install the software for office as well as home use. Anti-virus software should be configured to run in a background mode and scan files upon access. Updated virus detection signatures should be downloaded and installed regularly. 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.

3.5.5.3 Application Protection

3.5.5.3.1 Configuration Controls

Application configuration controls protect the application and the data it processes from unauthorized access and vary dependent on the application. Guidelines exist for the secure configuration of most COTS applications through NSA, the Common Criteria, and should be consistent with the requirements of the accreditation and certification process utilized.

- Computer operating systems should include security profiles
- Use application layer data at rest encryption
    - Information systems that make use of data at rest encryption products should only employ products that use the following symmetric data encryption algorithms: DES, Triple DES (3DES), or Skipjack.
- Use E-mail encryption, but avoid proprietary solutions that preclude interoperability.
    - Deploy only S/MIME-based solutions (currently S/MIME v2, possibly S/MIME v3 in the future). In order to ensure that Administrations can trust the digital signatures in S/MIME messages, the digital certificates used must come from a recognized Certificate Authority (CA) as conforming to acceptable certificate issuance practices. The S/MIME clients should be configured to recognize only the conforming certificate authorities.
- Use the Secure Sockets Layer (SSL) protocol on web servers to provide for fine-grained access control to web sites (by requiring a user to provide a valid certificate) and signatures, authenticity and privacy for transactions involving web browsers and servers. For the transaction in which the browser user's identity is not important, but encryption of the transaction and the authenticity of the web server are, only the server needs a valid certificate.

3.5.5.3.2 Secure Code Design Practices

To aid in designing a secure information system, NIST compiled a set of engineering principles for 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.

Refer to NIST Special Publication 800-27, Engineering Principles for Information Technology Security at http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf .

Use NIST SP 800-27 for guidance on establishing secure code design practices

3.5.5.3.3 Data Encryption Services

The official U.S. government standard for the protection of unclassified information by cryptography is the Data Encryption Standard (DES). DES is the most widely used cryptographic algorithm in the world. Many other symmetric algorithms have been developed commercially, often to meet a perceived need for algorithms that are stronger than DES. However, only a very few of these algorithms have been intensively crypt analyzed and few have existed long enough to have confidence in their security.

Triple DES (or 3DES) is a scheme that encrypts by applying the DES algorithm three times, with three different keys in an attempt to make the key size larger (DES key size is 56 bits, triple-DES is 168 bits) and the cryptography harder to break. The security of the scheme may be better than normal 56 bit DES and is almost certainly no worse. NIST FIPS PUB 46-3 is the FIPS approved algorithm of choice. Single DES is only allowed for legacy applications, with all new systems development to use 3DES. However, for compatibility with legacy systems, 3DES implementations should be capable of operating in the single DES compatibility mode.

3.5.5.3.4 Virus/Mobile Code Detection

The process of using anti-virus software to detect viruses in resources such as e-mail messages and hard drives and eliminates any that are found. This software must be updated regularly in order to defend against new viruses.

All PC-based workstations and servers (including those using the Windows 2000, Windows NT, Windows 95, Windows 98, and Macintosh operating systems) should employ anti-virus software. Most large organizations use an anti-virus detection tool site license, enabling employees to install the software for office as well as home use. Anti-virus software should be configured to run in a background mode and scan files upon access. Updated virus detection signatures should be downloaded and installed regularly. 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.