The Technical Reference Model (TRM) Version 1.1

A Foundation for Government-wide Improvement

The Federal Enterprise Architecture Program Management Office

The Technical Reference Model Version 1.1:

A Foundation for Government-wide Improvement

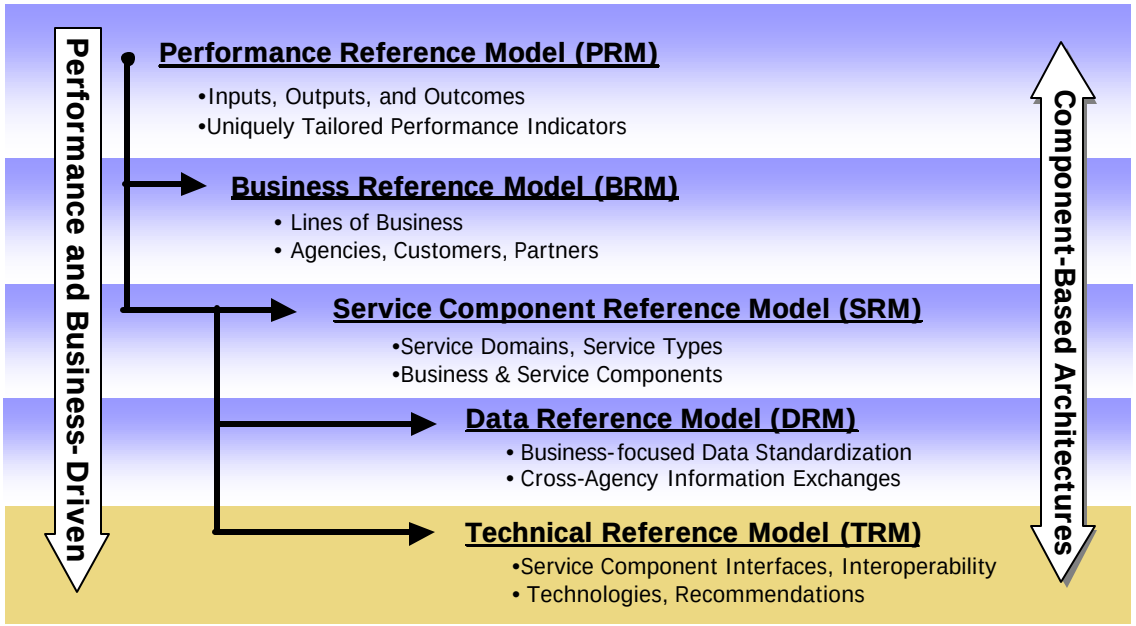
August 2003

TABLE OF CONTENTS

EXECUTIVE SUMMARY

To facilitate efforts to transform the Federal Government into one that is citizen-centered, results-oriented, and market-based, the Office of Management and Budget (OMB) is developing the Federal Enterprise Architecture (FEA), a business-based framework for Government-wide improvement. As illustrated in Figure 1, the FEA is being constructed through a collection of interrelated "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across Federal Agencies.

Figure 1 – The Federal Enterprise Architecture (FEA)



The FEA Technical Reference Model (TRM) provides a foundation to describe the standards, specifications, and technologies supporting the secure delivery, exchange, and construction of business (or Service) components and e-Gov solutions. The FEFA TRM unifies existing Agency TRMs and electronic Government (e-Gov) guidance by providing a foundation to advance the re-use of technology and component services from a Government-wide perspective.

TARGET AUDIENCE

- **Program Managers –** responsible for assembling components and technology to support the implementation of a project or program that may require cross-agency collaboration and the re-use of agency assets

- **Chief Architects –** responsible for the definition and target planning of an Agency's Enterprise Architecture

- **System / Solution Architects / Developers –** responsible for building / assembling systems, and selecting technologies and standards that leverage existing assets and services across the government and industry

SUMMARY OF CHANGES – VERSION 1.0 TO VERSION 1.1

The TRM Version 1.1 constitutes a minor revision to the TRM Version 1.0. Nomenclature revisions were made to provide consistency between illustrations, diagrams, and definitions throughout the document. Specifications previously dissected into a 5th layer have been merged into the Specification layer of the TRM. The specifications affected by this merge are Database Access, Privacy, Message-Oriented Middleware, and Object Request Broker. Mac OS X and Linux have been added to Supporting Platforms Service Category of the Service Platform and Infrastructure Service Area.

SUMMARY OF TRM VERSION 1.1

The TRM, as illustrated in Figure 2, outlines the standards, specifications, and technologies that collectively support the secure delivery, exchange, and construction of business and application components (Service Components) that may be used and leveraged in a Component-Based or Service Orientated Architecture. The TRM identifies the core technologies that support the Federal Government information technology (IT) transition towards interoperable e-Government solutions.

Figure 2 – FEA Technical Reference Model (TRM)

The TRM is comprised of four (4) core Service Areas. Service Areas represent a technical tier supporting the secure construction, exchange, and delivery of Service Components. Each Service Area aggregates and groups the standards, specifications, and technologies into lower-level functional areas. There are four (4) Service Areas within the TRM which are described as follows:

- ***Service Access and Delivery*** **-** refers to the collection of standards and specifications to support external access, exchange, and delivery of Service Components or capabilities. This area also includes the Legislative and Regulatory requirements governing the access and usage of the specific Service Component.

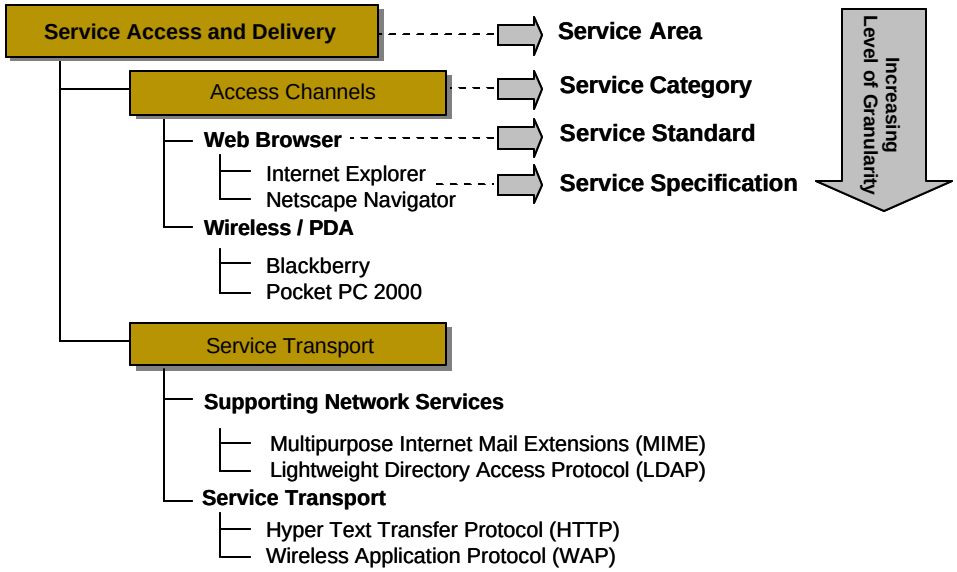
- ***Service Platform & Infrastructure*** **-** refers to the collection of delivery and support platforms, infrastructure capabilities and hardware requirements to support the construction, maintenance, and availability of a Service Component or capabilities.

- ***Component Framework*** - refers to the underlying foundation, technologies, standards, and specifications by which Service Components are built, exchanged, and deployed across Component-Based, Distributed, or Service-Orientated Architectures.

- ***Service Interface and Integration*** **-** refers to the collection of technologies, methodologies, standards, and specifications that govern how agencies will interface (both internally and externally) with a Service Component. This area also defines the methods by which components will interface and integrate with back office / legacy assets.

Each Service Area, as illustrated in Figure 3, consists of multiple Service Categories, Service Standards, and Service Specifications that provide the foundation to group standards, specifications, and technologies that directly support the Service Area.

Figure 3 – Service Categories, Service Standards, and Service Specifications



ORGANIZATION OF THE DOCUMENT

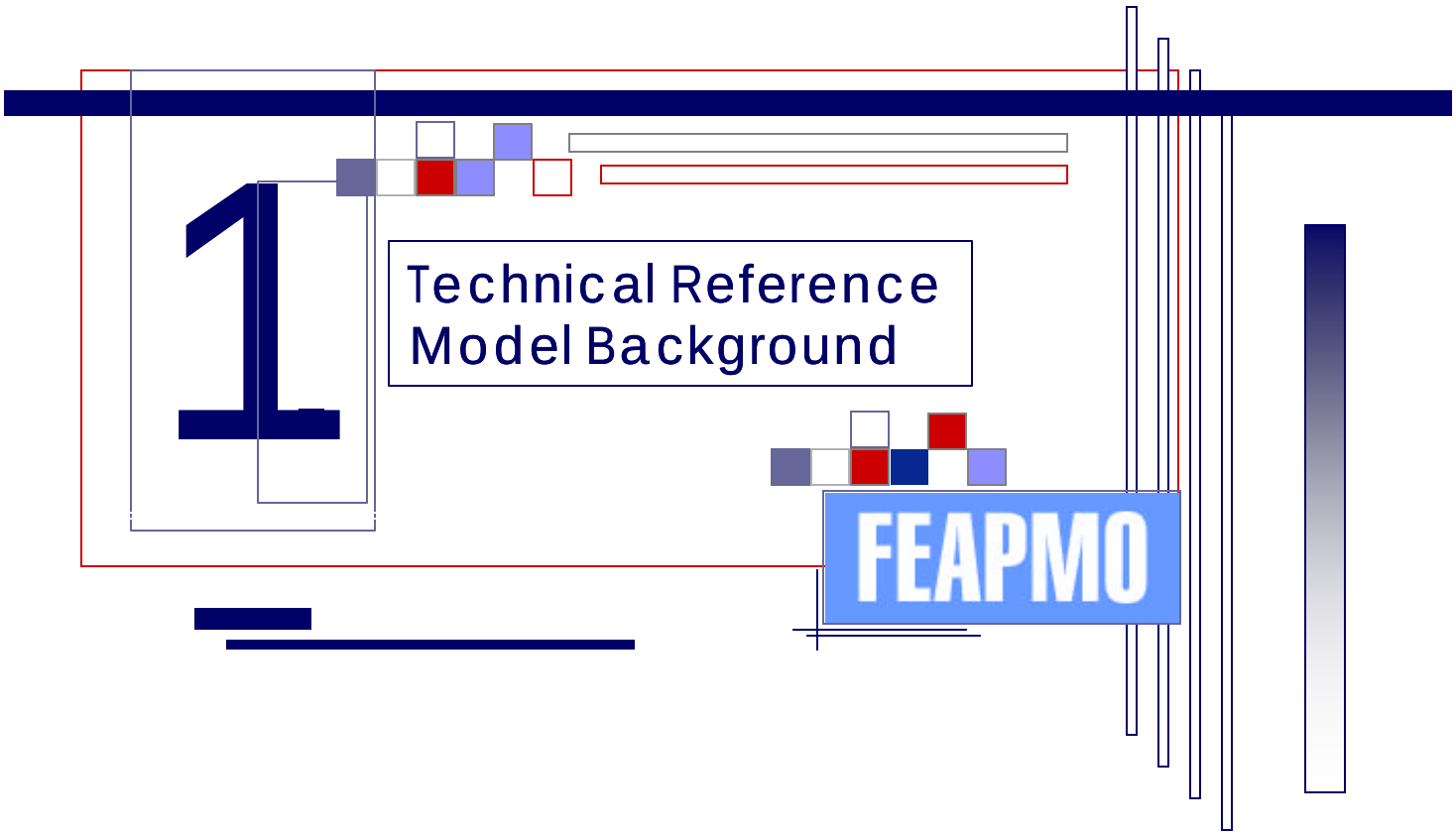
The remainder of this document is organized according to the following chapters and appendices:

- ***Chapter 1:*** **The Technical Reference Model Background -** provides the definition, purpose, development, and validation process for the TRM.

- ***Chapter 2:*** **The Technical Reference Model v1.1 -** provides a complete overview of version 1.1 of the Technical Reference Model, including definitions of each Service Area, Service Representation, Service Category and Service Specification.

- ***Chapter 3:*** **Use and Maintenance -** describes, at a high level, how the TRM should be used by the agencies in their EA and Capital Planning processes; how an online repository will facilitate these efforts, and how the TRM will be modified and updated.

- ***Appendix:* The Federal Enterprise Architecture** - provides a high-level overview of the Federal Enterprise Architecture and its benefits, the Federal Enterprise Architecture Program Management Office (FEA-PMO), and supporting committees.



TECHNICAL REFERENCE MODEL BACKGROUND

Definition

The TRM is a component-driven, technical framework used to identify the standards, specifications, and technologies that support and enable the delivery of service components and capabilities.

Purpose

The TRM serves to outline the technology elements that collectively support the adoption and implementation of component-based architectures. The model provides the foundation to advance the re-use of technology and component services across the Federal Government through standardization. Aligning Agency capital investments to the TRM leverages a common, standardized vocabulary, allowing inter-Agency and intra-Agency discovery, collaboration, and interoperability. Agencies, and the Federal Government, will benefit from economies of scale by identifying and re-using the best solutions and technologies to support their business functions, mission, and target architecture.

Specifically, the TRM was created to:

- Create a government-wide reference model that unifies agency TRMs and existing e-Gov guidance

- Focus technology standards, specifications, and recommendations on those that embrace the Internet and related approaches

- Create a foundation that focuses heavily on the secure delivery and construction of Service Components and their interfaces

- Identify the layers of a Component-Based Architecture, the supporting technologies, and recommendations for each

KEY CONCEPTS AND DEFINITIONS

Technologies – refers to a specific implementation of a standard within the context of a given specification.

The following describes for illustrative purpose the use of the term 'technologies' as used in the TRM.

- PL/SQL is an Oracle implementation of the SQL Standard

- ISQL/w is a Microsoft implementation of the SQL Standard

- ODBC is an implementation of a data access standard within various Microsoft specifications

- JDBC is an implementation of a data access standard within the Sun Microsoft specifications

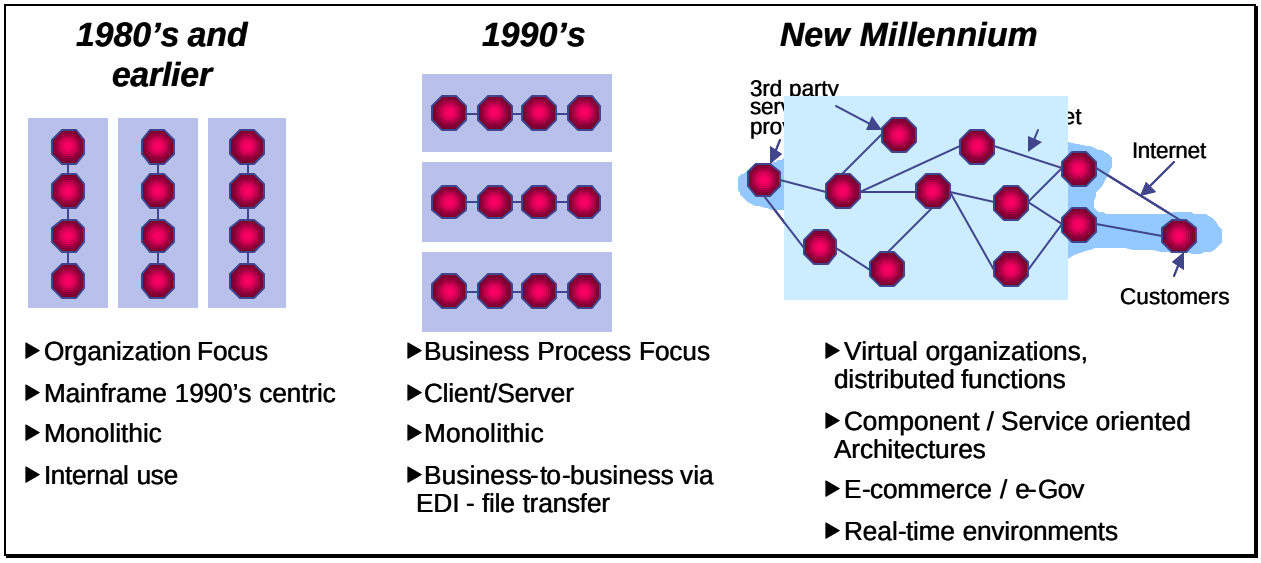
While all are based on an Open Standard, each vendor has their own implementation of the standard based on their specific technologies.

Legacy – refers to both software and/or hardware from previous technology generations. From a software perspective, legacy in the TRM refers to any technologies that are not Internet-enabled and not component-based.

Component **-** a self-contained business process or service with predetermined functionality that may be exposed through a business or technology interface.

Component Based Architecture **(CBA)** – a technology architecture comprised of run-time services and control structures together with an application infrastructure. The CBA consists of the component model and the architecture services that are built around the model. As illustrated in Figure 4, solutions based on a CBA are more dynamic, flexible, and maintainable than traditional monolithic solutions.

Figure 4 – Lifecycle of Monolithic and Component-Based Solutions



Service Area – is a technical tier that supports the secure construction, exchange, and delivery of business or service components. Each Service Area groups the requirements of component-based architectures within the Federal Government into *functional* areas.

Service Category – is a sub-tier of the Service Area to classify lower levels of technologies, standards, and specifications in respect to the business or technology function they serve.

Standard – hardware, software, or specifications that are widely used and accepted (de facto), or are sanctioned by a standards organization (de jure). Standards are typically categorized as follows:

- Programming Language Standards
- Character Code Standards
- Hardware Interface Standards
- Storage Media Standards
- Operating System Standards
- Communication and Networking Standards
- Machine Language Standards
- File System Management Standards
- Database Management System Standards
- Text Systems Standards
- Graphic Systems Standards
- Internet Standards

Specification – a formal layout/blueprint/design of an application development model for developing distributed component-based architectures.

Developing components based on a specification simplifies enterprise applications by basing them on standardized, modular components, and by providing a complete set of services to those components.

Two *specifications* for Agency use that promote the concept of Internet-enabled distributed component-based architectures are described in this TRM: Microsoft.NET and Sun Microsystems J2EE.

DEVELOPMENT OF THE TRM

In developing the TRM, the FEAPMO leveraged previous Federal architecture efforts, such as the Federal Enterprise Architecture Framework (FEAF) to guide the design of the government-wide model. The FEAPMO then performed extensive research on industry and government standards, specifications, and technologies to further refine and enhance the model.

The information contained within these sources provided thorough documentation of the many services, capabilities and technologies that industry and government applications and IT initiatives deliver. The FEAPMO used this information to normalize and categorize standards, specifications, and technologies that support the business and service components and capabilities. Once a list of Service Areas, Service Representations, Service Categories and Specifications was developed, definitions were given to each of the layers of the model and their contents.

Continued refinement of the TRM will include factoring in additional Agency architectures, such as DoD's C4ISR architecture and their Core Architecture Data Model (CADM).

VALIDATION

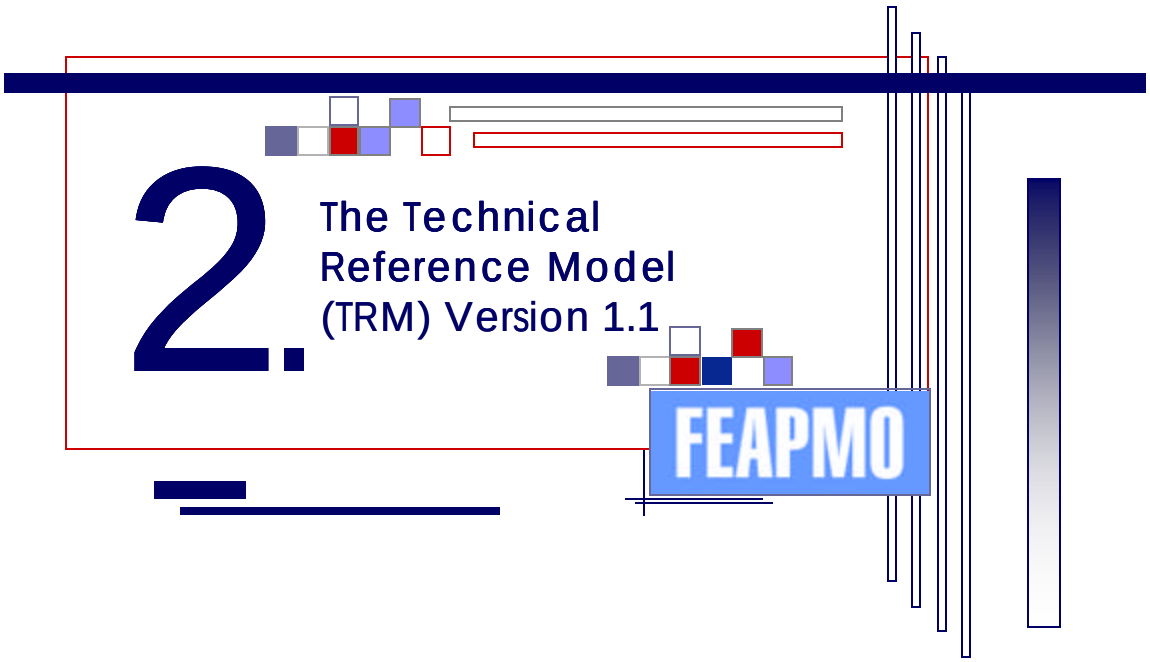
The TRM Version 1.0 was reviewed, validated and revised by the FEA-PMO and the SAWG, then released to agencies for feedback on January 29, 2003. Agency comments on the TRM were received and compiled through March 31, 2003. This feedback was analyzed by the FEA-PMO to further advance/evolve the model. The FEA-PMO's response to Agency comments will be published in a Comments Response Document, and will be available via Agency Chief Information Officers (CIOs).

A first pass was performed at aligning the TRM to the Agencies' major IT initiatives, as well as the 24 Presidential Priority E-Gov initiatives to the TRM. The alignment will be validated by agencies through the Federal Enterprise Architecture Management System (FEAMS), discussed further in Chapter 4 of this document.

VENDOR-SPECIFIC PRODUCTS

The TRM is not intended to provide or endorse particular vendor products. Where specific products are listed, they are products sanctioned by the Federal CIO Council, and are those that specifically pertain to developing web solutions, as are all of the technologies, standards and specifications contained within the TRM. For example you *will* see a product such as Microsoft

.NET within the TRM because it's a product contained within the CIO Council list, and it's used for developing web pages and web service/component-based solutions, a component of CBA. You *will not* see technologies such as FORTRAN or COBOL as these programming languages are primarily for developing computational and client/server systems, and not web-based e-Government solutions.



TECHNICAL REFERENCE MODEL (TRM) VERSION 1.1

OVERVIEW

The TRM provides a foundation to describe the standards, specifications, and technologies supporting the secure delivery, exchange, and construction of business (or Service) components and e-Gov solutions. The TRM unifies existing Agency TRMs and electronic Government (e-Gov) guidance by providing a foundation to advance the re-use of technology and component services from a Government-wide perspective.

The TRM outlines the standards, specifications, and technologies that collectively support the secure delivery, exchange, and construction of business and application components (Service Components) that may be used and leveraged in a Component-Based or Service Orientated Architecture. As illustrated in Figure 5, The TRM identifies the core technologies that support the Federal Government information technology (IT) transition towards interoperable e-Government solutions.

Figure 5 – FEA Technical Reference Model (TRM)

The TRM is comprised of four (4) core Service Areas. Service Areas represent a technical tier supporting the secure construction, exchange, and delivery of Service Components.

Each Service Area aggregates and groups the standards, specifications, and technologies into lower-level functional areas. There are four (4) Service Areas within the TRM which are described as follows:

- ***Service Access and Delivery*** **-** refers to the collection of standards and specifications to support external access, exchange, and delivery of Service Components or capabilities. This area also includes the Legislative and Regulatory requirements governing the access and usage of the specific Service Component.

- ***Service Platform & Infrastructure*** **-** refers to the collection of delivery and support platforms, infrastructure capabilities and hardware requirements to support the construction, maintenance, and availability of a Service Component or capabilities.

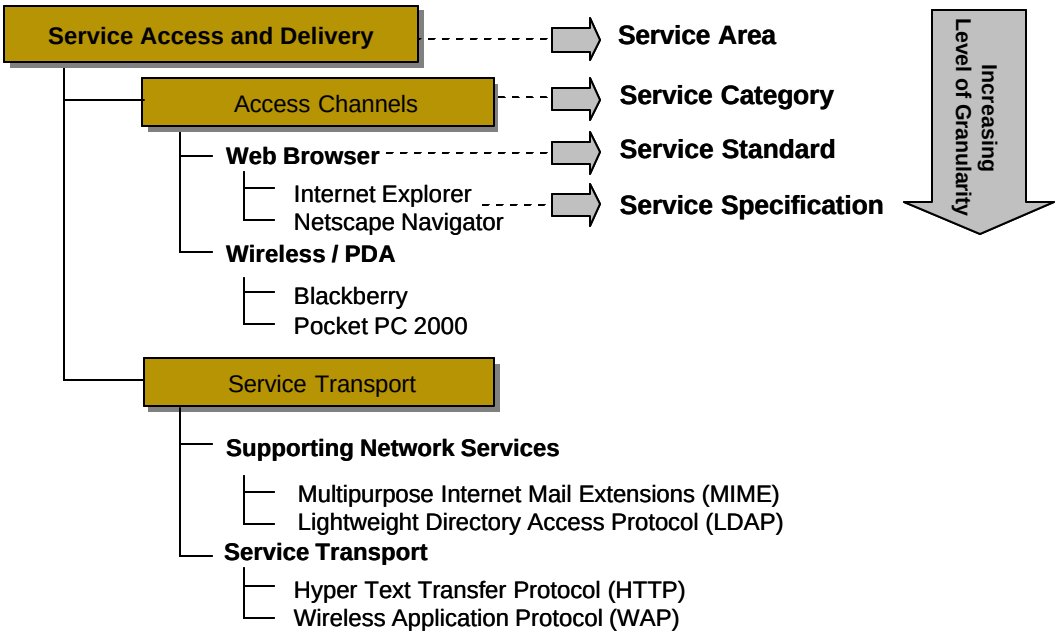
- ***Component Framework*** - refers to the underlying foundation, technologies, standards, and specifications by which Service Components are built, exchanged, and deployed across Component-Based, Distributed, or Service-Orientated Architectures.

- ***Service Interface and Integration*** **-** refers to the collection of technologies, methodologies, standards, and specifications that govern how agencies will interface (both internally and externally) with a Service Component. This area also defines the methods by which components will interface and integrate with back office / legacy assets.

Supporting each Service Area is a collection of Service Categories. Service Categories are used to classify lower levels of technologies, standards, and specifications in respect to the business or technology function they serve. Each Service Category is supported by one or more Service Standards.

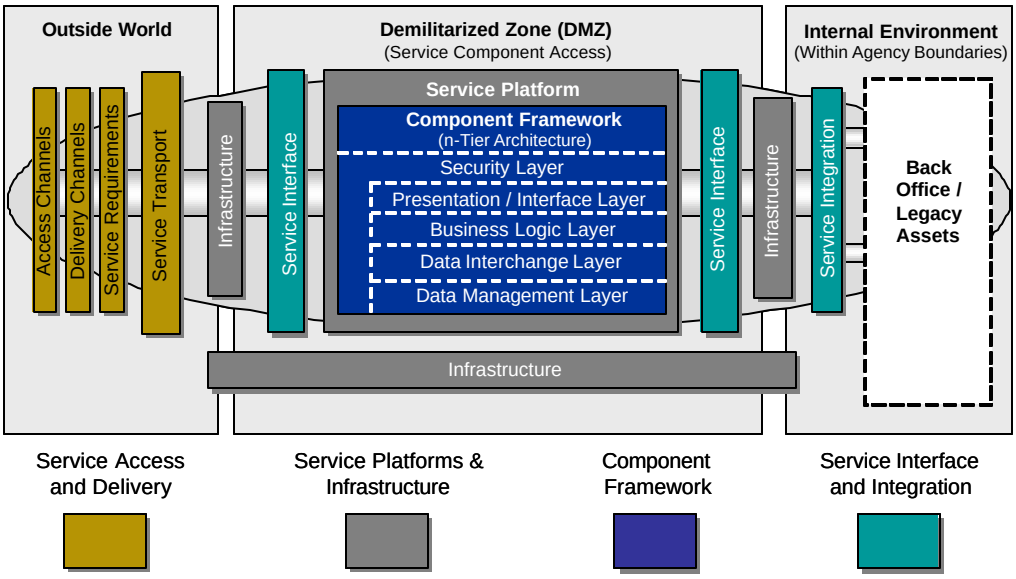
Service Standards are used to define the standards and technologies that support the Service Category. The final level of the TRM is the Service Specification layer that details the specification and / or provider of the Service Standard specification. See Figure 6.0 for a visual representation.

Figure 6 – Service Area, Category, Standard, and Specification



As depicted in Figure 7, each Service Area, and supporting Service Categories, can be structured across typical network topologies that provide clear distinctions between External Environments, Demilitarized Zones (DMZ) or Internal Environments housing back-office and legacy assets.

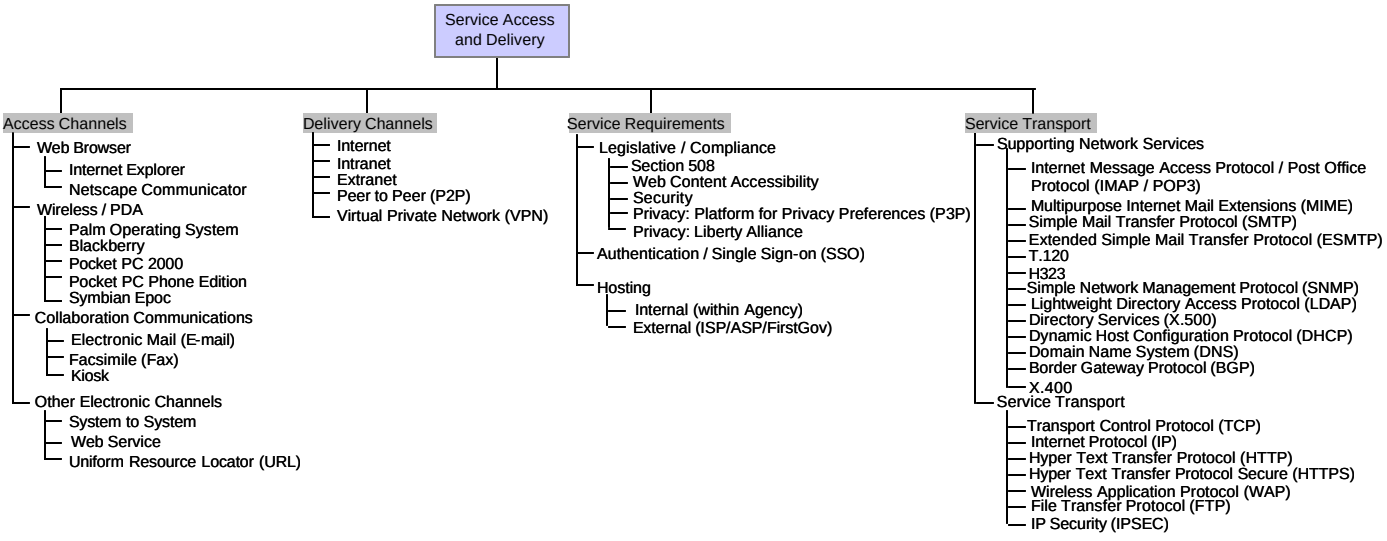
Figure 7 – TRM within a Typical Network Topology



SERVICE ACCESS AND DELIVERY

The Service Access and Delivery Service Area, as illustrated in Figure 8, defines the collection of Access and Delivery Channels that will be used to leverage the service component, and the legislative requirements that govern it's use and interaction.

Figure 8 – Service Access and Delivery Service Area



The Service Access and Delivery Service Categories, Standards, and Specifications are defined below:

Access Channels

Access Channels define the interface between an application and its users, whether it is a browser, personal digital assistant or other medium.

Web Browser – Define the program that serves as your front end to the World Wide Web on the Internet. In order to view a site, you type its address (URL) into the browser's location field.

Internet Explorer – Microsoft Internet Explorer (MSIE) is the most widely used World Wide Web browser.

http://www.microsoft.com/windows/ie/default.asp

Netscape Communicator – Netscape is the second most widely used World Wide Web browser.

http://channels.netscape.com/ns/browsers/

Wireless / PDA - Define the technologies that use transmission via the airwaves. Personal Digital Assistant (PDA) is a handheld computer that serves as an organizer for personal information. It generally includes at least a name and address database, to-do list and note taker.

Palm Operating System - Palm is the leading Personal Digital Assistant (PDA). Version 5 of Palm OS provides multitasking and other capabilities that will provide an improved platform for E-Gov solutions.

http://www.palmos.com/dev/

Blackberry - The leading email enabled wireless device with wide use in several Agencies.

http://www.blackberry.com/developers/na/index.shtml

Pocket PC Phone Edition - Microsoft's environment for internet capable cellular phones.

http://www.microsoft.com/mobile/pocketpc/phoneedition/default.asp

Pocket PC 2000 - Microsoft's environment for PDA level devices.

http://www.microsoft.com/mobile/pocketpc/learnmore.asp

Symbian Epoc - A leading environment for web capable cellular phones.

http://www.symbian.com/developer/index.html

Collaboration Communications – Define the forms of electronic exchange of messages, documents, or other information. Electronic communication provides efficiency through expedited time-of-delivery.

Electronic Mail (E-mail) – E-mail (Electronic mail) is the exchange of computer-generated and stored messages by telecommunication. An E-mail can be created manually via messaging applications or dynamically, programmatically such as automated response systems.

Facsimile (Fax) – A fax is the digitized image of text and/or pictures, represented as a series of dots (bit map). Faxes are sent and received through telecommunication channels such as telephone or internet.

Kiosk - A kiosk is a small physical structure (often including a computer and a display screen) that displays information for people walking by. Kiosks are common in public buildings. Kiosks are also used at trade shows and professional conferences.

Other Electronic Channels – Define the other various mediums of information exchange and interface between a user and an application.

System to System - System to System involves at least two computers that exchange data or interact with each other independent of human intervention or participation.

Web Service - Web services (sometimes called application services) are services (usually including some combination of programming and data, but possibly including human resources as well) that are made available from a business's web server for Web users or other Web-connected programs.

Uniform Resource Locator (URL) – URL is the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use (i.e. "http://"), and the second part specifies the IP address or the domain name where the resource is located (i.e. "www.firstgov.gov").

Delivery Channels

Delivery Channels define the level of access to applications and systems based upon the type of network used to deliver them.

Internet - The Internet is a worldwide system of computer networks in which users at any one computer can, if they have permission, get information from any other computer.

Intranet - An Intranet is a private network that is contained within an enterprise. It may consist of many inter-linked local area networks and is used to share company information and resources among employees.

Extranet - An Extranet is a private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company.

Peer to Peer (P2P) - Peer to Peer is a class of applications, that operate outside the DNS system and have significant or total autonomy from central servers, that take advantage of resources available on the Internet.

Virtual Private Network (VPN) - A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Service Requirements

Service Requirements define the necessary aspects of an application, system or service to include legislative, performance and hosting.

Legislative / Compliance - Defines the pre-requisites that an application, system or service must have mandated by congress or governing bodies.

Section 508 – Section 508 requires that Federal agencies' electronic and information technology is accessible to people with disabilities, including employees and members of the public.

Web Content Accessibility - Refers to hardware and software that helps people who are physically or visually impaired.

Security - Policy and procedures that protect data against unauthorized access, use, disclosure, disruption, modification or destruction.

Privacy: Platform for Privacy Preferences (P3P) – A specification that will allow users' Web browsers to automatically understand Web sites' privacy practices. Privacy policies will be embedded in the code of a Web site. Browsers will read the policy, and then, automatically provide certain information to specific sites based on the preferences set by the users. For instance, if the site is an e-commerce site, the browser will automatically provide shipping info. If the site is requesting demographic info, then the browser will know to provide it anonymously. The P3P specification was developed by the W3C P3P Syntax, Harmonization, and Protocol Working Groups, including W3C Member organizations and experts in the field of Web privacy. P3P is based on W3C specifications that have already been established, including HTTP, XML and Resource Description Framework (RDF). *Privacy* is policy that deals with the degree to which an individual can determine which personal information is to be shared with whom and for what purpose.

http://www.w3.org/P3P/

Privacy: Liberty Alliance – The Liberty Alliance Project is an alliance formed to deliver and support a federated network identity solution for the Internet that enables single sign-on for consumers as well as business users in an open, federated way. A federated network identity model will enable every business or user to manage their own data, and ensure that the use of critical personal information is managed and distributed by the appropriate parties, rather than a central authority. *Privacy* is policy that deals with the degree to which an individual can

determine which personal information is to be shared with whom and for what purpose.

http://www.projectliberty.org/

Authentication / Single Sign-on (SSO) – Refers a method that provides users with the ability to log-in one time, getting authenticated access to all their applications and resources.

Hosting – Refers to the service provider who manages and provides availability to a web site or application, often bound to a Service Level Agreement (SLA). The Hosting entity generally maintains a server farm with network support, power backup, fault tolerance, load-balancing, and storage backup.

Internal (within Agency) – The hosting of a web site or application within an Agency. The Agency is responsible for the maintenance, support and availability of the web site or application.

External (ISP/ASP/FirstGov) – The outsourcing of a web site or application with a managed service provider. An Internet Service Provider (ISP) provides telecommunications circuits, server co-location, and web site and application hosting. An Application Service Provider (ASP) offers software-based services for high-end business applications and specific-needs applications such as payroll, sales force automation, and human resources. FirstGov is the official managed service provider for the Federal Government.

Service Transport

Service Transport defines the end-to-end management of the communications session to include the access and delivery protocols.

Supporting Network Services - These consist of the protocols that define the format and structure of data and information that is either accessed from a directory or exchanged through communications.

Internet Message Access Protocol / Post Office Protocol (IMAP / POP3) – IMAP allows a client to access and manipulate electronic mail messages on a server. IMAP permits manipulation of remote message folders, called "mailboxes", in a way that is functionally equivalent to local mailboxes. IMAP also provides the capability for an offline client to resynchronize with the server. POP3 is the most commonly used protocol for retrieving e-mail from a mail host. (Refers to *RFC2060)*

http://www.imap.org/papers/docs/rfc2060.html

Multipurpose Internet Mail Extensions (MIME) – 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

email clients and servers to accurately communicate embedded information to internal and external users. (Refers to *RFC 2045)*

http://www.mhonarc.org/~ehood/MIME/2045/rfc2045.html

Simple Mail Transfer Protocol (SMTP) – 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. (Refers to *RFC821)*

http://rfc.net/rfc821.html

Extended Simple Mail Transfer Protocol (ESMTP) - ESMTP allows new service extensions to SMTP to be defined and registered with Internet Assigned Numbers Authority (IANA). (Refers to *RFC1869)*

http://ietfreport.isoc.org/rfc/rfc1869.txt

T.120 – T.120, an International Telecommunications Union (ITU) standard, contains a series of communication and application protocols and services that provide support for real-time, multipoint data communications. These multipoint facilities are important building blocks for collaborative applications, including desktop data conferencing, and multi-user applications.

http://www.imtc.org/t120body.htm

H.323 – H.323, an International Telecommunications Union (ITU) standard, addresses Video (Audiovisual) communication on Local Area Networks, including Corporate Intranets and packet-switched networks generally.

http://www.imtc.org/h323.htm

Simple Network Management Protocol (SNMP) - SNMP eliminates several of the security vulnerabilities in earlier version.

http://www.ietf.org/rfc/rfc2570.txt?number=2570

Lightweight Directory Access Protocol (LDAP) - LDAP is a subset of X.500 designed to run directly over the TCP/IP stack. LDAP is, like X.500, both an information model and a protocol for querying and manipulating it. LDAPv3 is an update developed in the IETF (Internet Engineering Task Force), which address the limitations found during deployment of the previous version of LDAP. (Refers to *LDAP V3, RFC 1779)*

http://www.opengroup.org/directory/branding/ldap2000/x99di.htm

Directory Services (X.500) – This is a network service that discovers and identifies resources on a network and makes them accessible to users and applications. The resources include users, e-mail addresses, computers, mapped drives, shared folders, and peripherals such as printers and PDA docking stations. Users and computers access these resources without the needing to know how or where the resources are connected.

http://www.faqs.org/rfc/rfc2116.txt

Dynamic Host Configuration Protocol (DHCP) – A protocol for assigning dynamic IP addresses to devices on a network. A device can receive a different IP address for every connection. Dynamic addressing provides reduced network administration over deploying and connecting user and peripheral devices.

http://ietfreport.isoc.org/rfc/rfc2300.txt

Domain Name System (DNS) – A protocol used for translating domain names (i.e. www.feapmo.gov) to their respective IP addresses. DNS is collectively a network of devices which store query results. As one DNS server or device cannot provide the translated IP address, it queries other DNS devices. This process is invisible to the user.

http://www.icann.org/icp/icp-1.htm

Border Gateway Protocol (BGP) – Refers to a routing protocol used to exchange routing information between routers on a network, enabling more efficient routing of data. BGP is part of RFC 1771.

http://www.arin.net/library/rfc/rfc1771.txt

X.400 – An ISO and ITU standard for e-mail message addressing and transporting. X.400 supports Ethernet, X.25, TCP/IP and dial-up transport methods.

http://www.faqs.org/rfcs/rfc1327.html

Service Transport - These consist of the protocols that define the format and structure of data and information that is either accessed from a directory or exchanged through communications.

Transport Control Protocol (TCP) - TCP provides transport functions, which ensures that the total amount of bytes sent is received correctly at the destination.

http://www.ietf.org/rfc/rfc0793.txt

Internet Protocol (IP) - This is the protocol of the Internet and has become the global standard for communications. IP accepts packets from TCP, adds its own header and delivers a "datagram" to the data link layer protocol. It may also break the packet into fragments to support the maximum transmission unit (MTU) of the network.

http://www.faqs.org/rfcs/rfc1349.html

Hyper Text Transfer Protocol (HTTP) - The communications protocol used to connect to servers on the World Wide Web. It's primary function is to establish a connection with a web server and transmit HTML pages to the client browser.

http://www.w3.org/Protocols/

Hyper Text Transfer Protocol Secure (HTTPS) - The protocol for accessing a secure Web server. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80. The session is then managed by a security protocol.

http://www.w3.org/Protocols/Specs.html

Wireless Application Protocol (WAP) - The Wireless Application Protocol (WAP) is an open, global specification that empowers users of digital mobile phones, pagers, personal digital assistants and other wireless devices to securely access and interact with Internet/intranet/extranet content, applications, and services.

http://www.wapforum.org/

File Transfer Protocol (FTP) - A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a Web site on a local machine, they are typically uploaded to the Web server using FTP.

http://www.w3.org/Protocols/rfc959/Overview.html

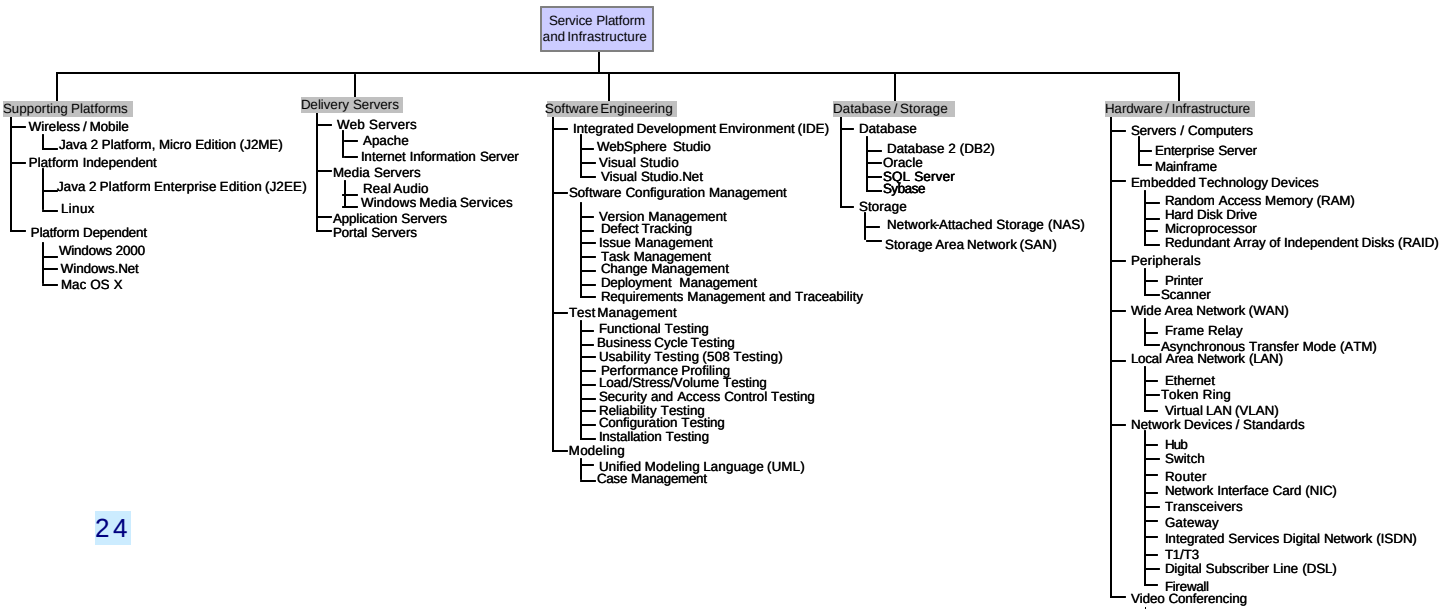
IP Security (IPSEC) – A set of protocols used to secure IP packet exchange. Tunnel and Transport are the two (2) modes supported by IPSEC. IPSEC uses certificates and Public Keys to authenticate and validate the sender and receiver.

http://www.ietf.org/html.charters/ipsec-charter.html

SERVICE PLATFORM AND INFRASTRUCTURE

The Service Platform and Infrastructure Area, as illustrated in Figure 9, defines the collection of platforms, hardware and infrastructure specifications that enable Component-Based Architectures and Service Component re-use.

Figure 9 – Service Platform and Infrastructure Service Area



The Service Platform and Infrastructure Service Categories, Standards, and Specifications are defined below:

Supporting Platforms

Supporting platforms are hardware or software architectures. The term originally dealt with only hardware, and it is still used to refer to a CPU model or computer family.

Wireless / Mobile - Radio transmission via the airwaves. Various communications techniques are used to provide wireless transmission including infrared line of sight, cellular, microwave, satellite, packet radio and spread spectrum.

Java 2 Platform, Micro Edition (J2ME) - Sun's Java environment for devices. It promises a relatively portable environment for those using Java for other tiers of the architecture.

http://java.sun.com/j2me/docs/

Platform Independent - Defines the operating systems and programming languages that are able to execute and run on any platform or operating system. A platform is the underlying hardware and software comprising a system.

Java 2 Platform Enterprise Edition (J2EE) - Sun's J2EE and Microsoft's .Net are the two dominant distributed computing architecture frameworks. J2EE provides portability of a single language (Java) over multiple operating systems and hardware platforms.

http://java.sun.com/j2ee/download.html#platformspec

Linux - Linux is an open source operating system that runs on multiple hardware platforms. With the ability to run on many platforms, including the PC and Macintosh, Linux has become an alternative to proprietary systems.

http://www.linux.org/

Platform Dependent - Defines the operating systems and programming languages that are able to execute and run on a specific platform or operating system. A platform is the underlying hardware and software comprising a system.

Windows 2000 - Also known as "Win2K" and "W2K," it is a major upgrade to Windows NT 4. Launched in February 2000, Windows 2000 comes in one client and three server versions. Windows 2000 looks like Windows 95/98, but adds considerably more features, dialogs and options.

http://www.microsoft.com/windows/default.mspx

Windows.Net - Microsoft's .Net and Sun's J2EE are the two dominant distributed computing architecture frameworks. .Net supports a wide range of languages but is primarily tied to the Microsoft Windows operating system and Intel hardware.

http://www.microsoft.com/net/products/default.asp

Mac OS X – Mac OS X is Apple's UNIX based operating system based on industry standards. Launched in March 2001, OS X has advanced built-in security functions and complete interoperability with both internet standards and Microsoft products.

http://www.apple.com/macosx

Delivery Servers

Delivery Servers are front-end platforms that provide information to a requesting application. It includes the hardware, operating system, server software, and networking protocols.

Web Servers – A computer that provides World Wide Web services on the Internet. It includes the hardware, operating system, Web server software, TCP/IP protocols and the Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an "intranet server."

Apache – A widely-used public domain, UNIX-based Web server from the Apache Group (www.apache.org). It is based on, and is a plug-in replacement for, NCSA's HTTPd server Version 1.3. The name came from a body of existing code and many "patch files."

http://www.apache.org/

Internet Information Server – Web server software from Microsoft that runs under Windows NT, Windows 2000, and Microsoft.Net. It supports Netscape's SSL security protocol and turns an NT-based PC into a Web site. Microsoft's Web browser, Internet Explorer, is also included.

http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/iis.mspx

Media Servers – Provide optimized management of media-based files such as audio and video streams and digital images.

Real Audio – streaming media server solution designed to supply desktop and mobile content.

http://www.realnetworks.com/solutions/enterprise/index.html

Windows Media Services – Part of Windows Server (2000 and .Net) optimized to deliver streaming media and dynamic digital content over intranet and internet delivery channels.

http://www.microsoft.com/windowsserver2003/technologies/winmedia/default.mspx

Application Servers – In a three-tier environment, a separate computer (application server) performs the business logic, although some part may still be handled by the user's

machine. After the Web exploded in the mid 1990s, application servers became Web based.

Portal Servers – Portals represent focus points for interaction, providing integration and single-source corporate information.

Software Engineering

Software engineering covers not only the technical aspects of building software systems, but also management issues, such as testing, modeling and versioning.

Integrated Development Environment (IDE) – This consists of the hardware, software and supporting services that facilitate the development of software applications and systems.

WebSphere Studio – Integrated Java (J2EE) environment for programmers building Java, web, and web services applications. Successor to IBM Visual Age.

http://www-3.ibm.com/software/awdtools/studiositedev/

Visual Studio – A complete development system providing the tools for analyzing and modeling all aspects of an application before a single component is built so that developers can design efficient architectures and reduce time to market. Developers can choose the programming language they know best and the language that is best suited to the solution, including Microsoft Visual Basic, Visual C++, Visual J++, and Visual FoxPro. Visual Studio is used to build scalable, data-driven Web sites and applications.

http://msdn.microsoft.com/vstudio/productinfo/previous/vs6/new.asp

Visual Studio.Net – A comprehensive tool set for rapidly building and integrating XML Web services, Microsoft Windows–based applications, and Web solutions. This is the successor to Visual Studio.

http://msdn.microsoft.com/vstudio/productinfo/default.asp

Software Configuration Management – Applicable to all aspects of software development from design to delivery specifically focused on the control of all work products and artifacts generated during the development process. Several solutions on the market provide the integration of the software configuration management functions.

Version Management – Refers to tracking and controlling versions of files. Version Management includes capabilities such as labeling, branching, merging, version content comparisons, and security and permission management across version-controlled projects.

Defect Tracking – Refers to the identification, assignment, and management of discovered defects within an application, product or solution. Defect tracking tools provide searchable defect data to identify urgent and related defects or

bugs. The architecture should be built to facilitate the pushing of software patches across the enterprise.

Issue Management – Refers to the management of business, technical, and infrastructure issues throughout the entire lifecycle of a project.

Task Management – Requirements, testing, and issues assignments are transformed into prioritized tasks. Task Management tools provide automation features for managing, delivering, assigning, reminding, and collaborating task management and execution.

Change Management – Refers to the management of application code and content changes across the software development lifecycles.

Deployment Management – Refers to the capability of software delivery to remote networked desktops, servers, and mobile devices across an enterprise. Deployment automation tools provide centralized and accelerated delivery of applications to users via push technologies, eliminating the need for manual installation and configuration.

Requirements Management and Traceability – Consists of information discovery, capture, storage and dissemination. Requirements management reduces software development costs and associated risks through documenting, measuring, and analyzing deviations to project requirements. Traceability refers to tracking requirements artifacts to their source, and changes in requirements to include the impact analysis of the change. Requirements traceability is an integral component in quality software implementation and the management of document succession.

Test Management – The consolidation of all testing activities and results. Test Management activities include test planning, designing (test cases), execution, reporting, code coverage, and heuristic and harness development.

Functional Testing – This type of test focuses on any requirements that can be traced directly to use cases (or business functions), business rules, and design.

Business Cycle Testing – Refers to the emulation of activities performed over a period of time that is relevant to the application under test.

Usability Testing (508 Testing) – Refers to a test to ensure that the application navigation, functionality, and GUI allow a user to effectively and efficiently do their work in a way that they are satisfied with the application.

Performance Profiling – Refers to a performance test that measures and evaluates response times and transaction rates.

Load/Stress/Volume Testing – Refers to tests that measure and evaluate how a system performs and functions under varying workloads, large amounts of data and/or resource utilization.

Security and Access Control Testing – Focuses on the technical, administrative and physical security controls that have been designed into the system architecture in order to provide confidentiality, integrity and availability.

Reliability Testing – Refers to the verification that failover methods are invoked properly and the system recovers properly.

Configuration Testing – Refers to a test to ensure that the application or system can handle all hardware and software variables and requirements that have been defined.

Installation Testing – Refers to the verification that the software installation process works properly in different environments and among varying conditions.

Modeling – The process of representing entities, data, business logic, and capabilities for aiding in software engineering.

Unified Modeling Language (UML) – A general-purpose notational language for specifying and visualizing complex software, especially large, object-oriented projects.

http://www.omg.org/gettingstarted/what_is_uml.htm

Case Management - Computer Aided Software Engineering (CASE) software that provides a development environment for programming teams. CASE systems offer tools to automate, manage and simplify the development process.

http://www.sei.cmu.edu/legacy/case/case_whatis.html

Database / Storage

Database / Storage refers to a collection of programs that enables storage, modification, and extraction of information from a database, and various techniques and devices for storing large amounts of data.

Database – Refers to a collection of information organized in such a way that a computer program can quickly select desired pieces of data. A database management system (DBMS) is a software application providing management, administration, performance, and analysis tools for databases.

Database 2 (DB2) – DB2 is a family of relational database products offered by IBM. DB2 provides an open database environment that runs on a wide variety of computing platforms.

http://www-3.ibm.com/software/data/db2/

Oracle – Relational database product; the first to support the SQL language.

http://www.oracle.com/ip/deploy/database/oracle9i/

SQL Server – Data management server product developed by Microsoft.

http://www.microsoft.com/sql/

Sybase – Data management and synchronization server products developed by Sybase.
http://www.sybase.com/products/databaseservers

Storage – Storage devices are designed to provide shared storage access across a network. These devices provide extended storage capabilities to the network with reduced costs compared to traditional file servers.

Network-Attached Storage (*NAS*) – A NAS device is a server that is dedicated to nothing more than file sharing.

Storage Area Network (SAN) – A SAN is a high-speed sub-network of shared storage devices. A storage device is a machine that contains nothing but a disk or disks for storing data.

Hardware / Infrastructure

Defines the physical devices, facilities and standards that provide the computing and networking within and between enterprises.

Servers / Computers – This refers to the various types of programmable machines which are capable of responding to sets of instructions and executing programs.

Enterprise Server – A computer or device on a network that manages network resources and shared applications for multiple users.

Mainframe – A very large computer capable of supporting hundreds, or even thousands, of users simultaneously. Mainframes support simultaneous programs.

Embedded Technology Devices – This refers to the various devices and parts that make up a Server or Computer as well as devices that perform specific functionality outside of a Server or Computer.

Random Access Memory (RAM) – A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is the most common type of memory found in computers and other devices, such as printers.

Hard Disk Drive – Refers to the area of a computer that where data is stored.

Microprocessor - A silicon chip that contains a CPU. In the world of personal computers, the terms microprocessor and CPU are used interchangeably. At the heart of all personal computers and most workstations sits a microprocessor.

Redundant Array of Independent Disks (RAID) – An assembly of disk drives that employ two or more drives in combination for fault tolerance and performance.

RAID disk drives are used frequently on servers but aren't generally necessary for personal computers. RAID is generally configured as mirrored or striped. Mirrored RAID (Level 1) provides a fail-over drive. Striped RAID (Levels 0, 3, and 5) write data across multiple disk drives so that a single disk failure can be recovered from the data on the remaining drives. There are three (3) types of RAID systems: failure-resistant disk systems (that protect against data loss due to disk failure), failure-tolerant disk systems (that protect against loss of data access due to failure of any single component), and disaster-tolerant disk systems (that consist of two or more independent zones, either of which provides access to stored data).

Peripherals – Computer devices that are not part of the essential computer (i.e. the memory and microprocessor). Peripheral devices can be external and internal.

Printer - Devices that print text or illustrations on paper. There are many different types of printers.

Scanner - Devices that can read text or illustrations printed on paper and translate the information into a form the computer can use. A scanner works by digitizing an image -- dividing it into a grid of boxes and representing each box with either a zero or a one, depending on whether the box is filled in.

Wide Area Network (WAN) - A data network typically extending a LAN outside a building or beyond a campus. Typically created by using bridges or routers to connect geographically separated LANs. WANs include commercial or educational dial-up networks such as CompuServe, InterNet and BITNET.

Frame Relay - packet-switching protocol for connecting devices on a Wide Area Network (WAN). Frame Relay networks in the U.S. support data transfer rates at T-1 (1.544 Mbps) and T-3 (45 Mbps) speeds.

http://www.frforum.com/

Asynchronous Transfer Mode (ATM) - A high bandwidth, high speed, controlled-delay, fixed-size packet switching and transmission system integrating multiple data types (voice, video, and data). Uses fixed-size packets also known as "cells" (ATM is often referred to as "cell relay").

http://www.iec.org/online/tutorials/atm_fund/

Local Area Network (LAN) - A network that interconnects devices over a geographically small area, typically in one building or a part of a building. The most popular LAN type is Ethernet. LANs allow the sharing of resources and the exchange of both video and data.

Ethernet - local-area network (LAN) architecture that uses a bus or star topology and supports data transfer rates of 10 Mbps, 100 Mbps (Fast Ethernet) or 1 Gbps (gigabit Ethernet). The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards.

http://grouper.ieee.org/groups/802/3/

Token Ring - A type of computer network in which all the computers are arranged (schematically) in a circle. A token, which is a special bit pattern, travels around the circle. To send a message, a computer catches the token, attaches a message to it, and then lets it continue to travel around the network.

http://www.8025.org/

Virtual LAN (VLAN) - Short for virtual LAN, a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which make them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

http://www.ieee802.org/1/pages/802.1Q.html

Network Devices / Standards - A group of stations (computers, telephones, or other devices) connected by communications facilities for exchanging information. Connection can be permanent, via cable, or temporary, through telephone or other communications links. The transmission medium can be physical (i.e. fiber optic cable) or wireless (i.e. satellite).

Hub - A common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Switch - In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

Router - A device or setup that finds the best route between any two networks, even if there are several networks to traverse. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create WANs.

Network Interface Card (NIC) - Often abbreviated as NIC, an expansion board you insert into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, and media, although some can serve multiple networks.

Transceivers - Short for *transmitter-receiver,* a device that both transmits and receives analog or digital signals. The term is used most frequently to describe the component in local-area networks (LANs) that actually applies signals onto the network wire and detects signals passing through the wire. For many LANs, the transceiver is built into the network interface card (NIC). Some types of networks, however, require an external transceiver.

Gateway - Gateways are points of entrance to and exit from a communications network. Viewed as a physical entity, a gateway is that node that translates between two otherwise incompatible networks or network segments.

Integrated Services Digital Network (ISDN) – ISDN is a system of digital phone connections which has been available for over a decade. This system allows data to be transmitted simultaneously across the world using end-to-end digital connectivity.

http://www.eff.org/Infra/ISDN/

T1/T3 - T1 service delivers 1.544 Mbps. Typically channelized into 24 DS0s, each capable of carrying a single voice conversation or data stream. The European T1 or E1 transmission rate is 2.048 Mbps. A T3 circuit communicates at 45 Mbps, or 28 T1 lines.

http://www.t1.org/

Digital Subscriber Line (DSL) - Refers collectively to all types of digital subscriber lines, the two main categories being ADSL and SDSL. Two other types of xDSL technologies are High-data-rate DSL (HDSL) and Very high DSL (VDSL).

http://www.faqs.org/faqs/datacomm/xdsl-faq/

Firewall – This refers to the network device that is designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. There are several types of firewall techniques and firewalls may implement one or more simultaneously. Packet filtering inspects inbound and outbound packets, validating against defined business rules. Application gateways apply security rules against applications. Circuit-level gateways apply security rules against physical connection attempts to and from the network. Proxy servers mask the internal requestor by inspecting and augmenting the packet header. Four common architectures of firewalls include the packet filtering router, the screened host firewall system, the dual homed host firewall, and the screened subnet firewall (with a DMZ), which is one of the most secure implementations.

Video Conferencing - Communication across long distances with video and audio contact that may also include graphics and data exchange. Digital video transmission systems typically consist of camera, codec (coder-decoder), network access equipment, network, and audio system.

Bridge - a bridge connects three or more conference sites so that they can simultaneously pass data, voice, or video. Videoconferencing bridges are often called MCUs (multipoint conferencing units).

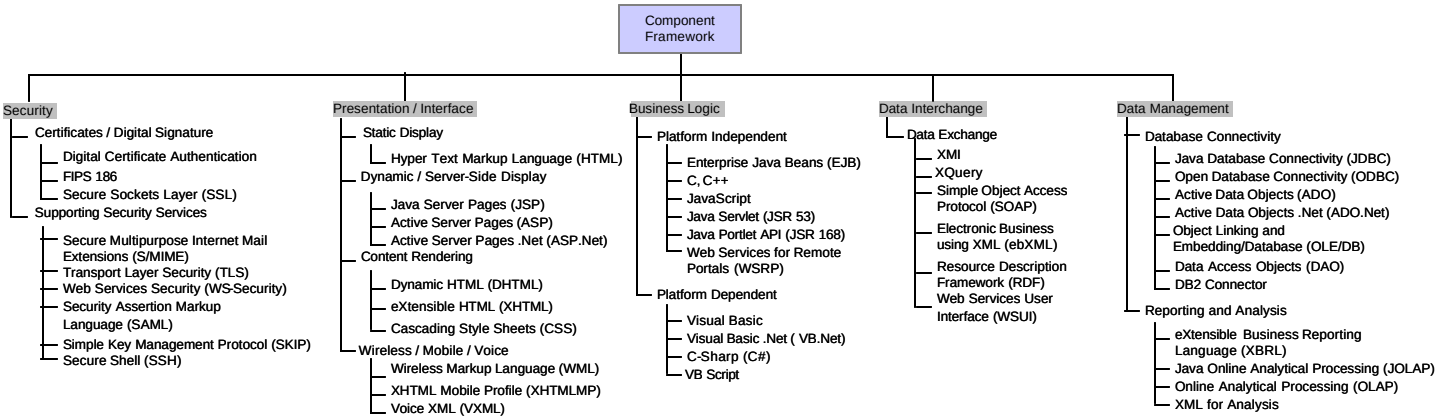
CODEC - a video codec converts analog video signals from a video camera to digital signals for transmission over digital circuits, and then converts the digital signals back to analog signals for display.

Receiver - An electronic device which enables a particular videoconference signal to be separated from all others being received by an earth station, and converts the signal format into a format for video, voice or data.

COMPONENT FRAMEWORK

The Component Framework Area, as illustrated in Figure 10, defines the underlying foundation and technical elements by which Service Components are built, integrated and deployed across Component-Based and Distributed Architectures. The Component Framework consists of the design of application or system software that incorporates interfaces for interacting with other programs and for future flexibility and expandability. This includes, but is not limited to, modules that are designed to interoperate with each other at runtime. Components can be large or small, written by different programmers using different development environments and may be platform independent. Components can be executed on stand-alone machines, a LAN, Intranet or on the Internet.

Figure 10 – Component Framework Service Area



The Component Framework Service Categories, Standards, and Specifications are defined below:

Security

Security defines the methods of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability. Biometrics, two-factor identification, encryption, and technologies based on the NIST FIPS-140 standards are evolving areas of focus.

http://csrc.nist.gov/cryptval/

Certificates / Digital Signature - Software used by a certification authority (CA) to issue digital certificates and secure access to information. The evolution of Public Key Infrastructure (PKI) is based on the verification and authentication of the parties involved in information exchange.

Digital Certificate Authentication – Authentication implementation for controlling access to network and internet resources through managing user identification. An electronic document, digital certificate, is issued and used to prove identity and public key ownership over the network or internet.

FIPS 186 - The Digital Signature Standard (DSS) specifies a digital signature algorithm (DSA) appropriate for applications requiring a digital, rather than written, signature. The DSA authenticates the integrity of the signed data and the identity of the signatory. The DSA may also be used to prove that data was actually signed by the generator of the signature. Additional references: *Draft ANSI X9.30-199x Part 1 and ISO/IEC JTC1/SC27/WG2, Project 1.27.08 Digital Signature with Appendix.*

http://www.dice.ucl.ac.be/crypto/standards.html

Secure Sockets Layer (SSL) - An open, non-proprietary protocol for securing data communications across computer networks. SSL is sandwiched between the application protocol (such as HTTP, Telnet, FTP, and NNTP) and the connection protocol (such as TCP/IP, UDP). SSL provides server authentication, message integrity, data encryption, and optional client authentication for TCP/IP connections.

http://www.webopedia.com/TERM/S/SSL.html

Supporting Security Services - These consist of the different protocols and components to be used in addition to certificates and digital signatures.

Secure Multipurpose Internet Mail Extensions (S/MIME) - Provides a consistent way to send and receive secure MIME data. Based on the Internet MIME standard, S/MIME provides cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and data confidentiality (using encryption). S/MIME is not restricted to mail; it can be used with any transport mechanism that transports MIME data, such as HTTP.

http://www.ietf.org/html.charters/smime-charter.html

Transport Layer Security (TLS) - Standard for the next generation SSL. TLS provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

http://www.ietf.org/html.charters/tls-charter.html

Web Services Security (WS-Security) - Describes enhancements to SOAP messaging to provide message integrity, message confidentiality, and single message au-

thentication. These mechanisms can be used to accommodate a wide variety of security models and encryption technologies including X.509, Kerberos, and SAML.

http://www.oasis-open.org/committees/wss/

http://www-106.ibm.com/developerworks/library/ws-secure/

Security Assertion Markup Language (SAML) - An XML-based framework for exchanging security information expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain. SAML is expected to play a key role in the Federal-wide E-Authentication initiative, and is supported by both the Liberty Alliance and WS-Security.

http://www.oasis-open.org/committees/security/

http://xml.coverpages.org/saml.html

Simple Key Management Protocol (SKIP) – A protocol developed by Sun Microsystems to handle key management across IP networks and VPNs.

http://www.networksorcery.com/enp/rfc/rfc2356.txt

Secure Shell (SSH) – A strong method of performing client authentication. Because it supports authentication, compression, confidentiality and integrity, SSH is used frequently on the Internet. SSH has two important components, RSA certificate exchange for authentication and Triple DES for session encryption.

http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-13.txt

http://www.ietf.org/internet-drafts/draft-ietf-secsh-auth-kbdinteract-05.txt

Presentation / Interface

This defines the connection between the user and the software, consisting of the presentation that is physically represented on the screen.

Static Display - Static Display consists of the software protocols that are used to create a pre-defined, unchanging graphical interface between the user and the software.

Hyper Text Markup Language (HTML) - The language used to create Web documents and a subset of Standard Generalized Markup Language (SGML)

http://www.w3.org/MarkUp/

Dynamic / Server-Side Display - This consists of the software that is used to create graphical user interfaces with the ability to change while the program is running.

Java Server Pages (JSP) - JSP is part of Sun's J2EE architecture and provide 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/

Active Server Pages (ASP) - A Web server technology from Microsoft that allows for the creation of dynamic, interactive sessions with the user.

http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28000522

Active Server Pages .Net (ASP.Net) - ASP.NET is a set of technologies in the Microsoft .NET Framework for building Web applications and XML Web Services. ASP.NET pages execute on the server and generate markup such as HTML, WML or XML that is sent to a desktop or mobile browser.

http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28000440

Content Rendering - This defines the software and protocols used for transforming data for presentation in a graphical user interface.

Dynamic HTML (DHTML) - A collective term for a combination of new Hypertext Markup Language (HTML) tags and options, style sheets, and programming that will allow Web pages that are more animated and more responsive to user interaction than previous versions of HTML.

http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28000522

eXtensible HTML (XHTML) - The W3C's recommendation for the next generation of HTML leveraging XML

http://www.w3.org/TR/2001/REC-xhtml11-20010531/

Cascading Style Sheets (CSS) - A style sheet format for HTML documents endorsed by the World Wide Web Consortium. CSS1 (Version 1.0) provides hundreds of layout settings that can be applied to all the subsequent HTML pages that are downloaded.

http://www.wdvl.com/Authoring/Style/Sheets/

Wireless / Mobile / Voice - Consists of the software and protocols used for wireless and voice-enabled presentation devices.

Wireless Markup Language (WML) - An XML-based protocol designed for Wireless devices.

http://www.oasis-open.org/cover/wap-wml.html

XHTML Mobile Profile (XHTMLMP) - XHTMLMP is designed for resource-constrained Web clients that do not support the full set of XHTML features, such as mobile phones, PDAs, pagers and set-top boxes. It extends XHTML Basic with modules, elements and attributes to provide a richer authoring language. XHTML replaces the Wireless Markup Language (WML).

http://www.wapforum.org/what/technical.htm

Voice XML (VXML) - VXML is an XML vocabulary for specifying IVR (Integrated Voice Response) Systems

http://www.w3c.org/Voice/

http://www.voicexml.org/

Business Logic

Defines the software, protocol or method in which business rules are enforced within applications.

Platform Independent - Consists of all software languages that are able to execute and run on any type of operating system or platform.

Enterprise Java Beans (EJB) - A software component in Sun's J2EE platform, which provides a pure Java environment for developing and running distributed applications.

http://java.sun.com/j2se/

C, C++ - C is a procedure programming language. C++ is an object-oriented version of C that has been widely used to develop enterprise and commercial applications.

http://www.accu.org/

JavaScript - A scripting language that runs within a web browser.

http://www.mozilla.org/js/

Java Servlet (JSR 53) - Java Servlets provide reusable web components that can be incorporated into portals.

http://www.jcp.org/aboutJava/communityprocess/final/jsr053/

Java Portlet API (JSR 168) - Java Portlet API enables interoperability between Portlets and Portals by defining APIs that address the areas of aggregation, personalization, presentation and security.

http://www.jcp.org/jsr/detail/168.jsp

Web Services for Remote Portals (WSRP) - WSRP defines an XML and Web services standard that will allow the plug-n-play of visual, user-facing Web services with portals or other intermediary Web applications.

http://www.oasis-open.org/commitees/wsrp

Platform Dependent - Consists of the programming languages and methods for developing software on a specific operating system or platform.

Visual Basic - A version of the BASIC programming language from Microsoft specialized for developing Windows applications.

http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28000520

Visual Basic .Net (VB.Net) - A version of the BASIC programming language from Microsoft specialized for developing Windows applications that is used within Microsoft's .NET environment.

http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28000520

C-Sharp (C#) - An object-oriented programming language from Microsoft that is based on C++ with elements from Visual Basic and Java.

http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28000520

VB Script - A scripting language from Microsoft. A subset of Visual Basic, VBScript is widely used on the Web for both client processing within a Web page and server-side processing in Active Server Pages (ASPs).

http://www.w3schools.com/vbscript/default.asp

Data Interchange

Define the methods in which data is transferred and represented in and between software applications.

Data Exchange – Data Exchange is concerned with the sending of data over a communications network and the definition of data communicated from one application to another. Data Exchange provides the communications common denominator between disparate systems.

XMI - Enables easy interchange of metadata between modeling tools (based on the OMG UML) and metadata repositories (OMG MOF based) in distributed heterogeneous environments. XMI integrates three key industry standards: XML, UML, and MOF. The integration of these three standards into XMI marries the best of

OMG and W3C metadata and modeling technologies, allowing developers of distributed systems to share object models and other metadata over the Internet.

http://www.omg.org/technology/documents/formal/xmi.htm

XQuery – A language used for processing and evaluating XML data. The XQuery language provides results of expressions allowing the use of evaluations to the implementation of XQuery.

http://www.w3.org/XML/Query

Simple Object Access Protocol (SOAP) – SOAP provides HTTP/XML based remote procedure call capabilities for XML Web Services.

http://www.w3.org/2000/xp/Group/

http://msdn.microsoft.com/msdnmag/issues/0300/soap/soap.asp

Electronic Business using XML (ebXML) - A modular suite of specifications that enables enterprises to conduct business over the Internet: exchanging business messages, conducting trading relationships, communicating data in common terms and defining and registering business processes.

http://www.ebxml.org/

Resource Description Framework (RDF) - RDF provides a lightweight ontology system to support the exchange of knowledge on the Web. It integrates a variety of web-based metadata activities including sitemaps, content ratings, stream channel definitions, search engine data collection (web crawling), digital library collections, and distributed authoring, using XML as interchange syntax. RDF is the foundation for the Semantic Web envisioned by Tim Berners-Lee - an extension of the current web in which information is given well-defined meaning, better enabling computers and people to work in cooperation.

http://www.w3.org/RDF/

http://www.w3.org/2001/sw/

Web Services User Interface (WSUI) - WSUI uses a simple schema for describing a WSUI "component" that can be used in a portal to call backend SOAP and XML services. WSUI uses XSLT stylesheets to construct user-facing views to enable users to interact with the services.

http://www.wsui.org/

Data Management

The management of all data/information in an organization. It includes data administration, the standards for defining data and the way in which people perceive and use it.

Database Connectivity - Defines the protocol or method in which an application connects to a data store or data base.

Java Database Connectivity (JDBC) - JDBC provides access to virtually any tabular data source from the Java programming language. It provides cross-DBMS connectivity to a wide range of SQL databases, and other tabular data sources, such as spreadsheets or flat files.

http://java.sun.com/products/jdbc/

Open Database Connectivity (ODBC) - A database programming interface from Microsoft that provides a common language for Windows applications to access databases on a network. ODBC is made up of the function calls programmers write into their applications and the ODBC drivers themselves.

http://www.webopedia.com/TERM/O/ODBC.html

Active Data Objects (ADO) - A programming interface from Microsoft that is designed as "the" Microsoft standard for data access. First used with Internet Information Server, ADO is a set of COM objects that provides an interface to OLE DB. The three primary objects are Connection, Command and Recordset.

http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28000520

Active Data Objects .Net (ADO.Net) - ADO.Net is the data-access component of the Microsoft's .NET Framework. It provides an extensive set of classes that facilitate efficient access to data from a large variety of sources, enable sophisticated manipulation and sorting of data.

http://support.microsoft.com/default.aspx?xmlid=fh%3BEN-US%3Badonet

Object Linking and Embedding/Database *(OLE/DB)* – A Microsoft low-level API designed to provide connections to different data sources. OLE/DB allowed connectivity to ODBC-based SQL providers/sources as well as other formats such as text and comma-delimited.

http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?Object+Linking+and+Embedding

Data Access Objects (DAO) – DAO is the Microsoft library for accessing Microsoft Jet engine data sources such as Microsoft Office-based applications. DAO is replaced by ADO and ADO.Net.

http://msdn.microsoft.com/library/default.asp?URL=/library/devprods/vs6/visualc/vctutor/_gs_a_brief_overview_of_dao.htm

DB2 Connector – An IBM connectivity API to access DB2 sources.

http://www.ibm.com

Reporting and Analysis - Consist of the tools, languages and protocols used to extract data from a data store and process it into useful information.

eXtensible Business Reporting Language (XBRL) - Extensible Business Reporting Language (XBRL is an open specification which uses XML-based data tags to describe financial statements for both public and private companies.

http://www.xbrl.org/

Java Online Analytical Processing (JOLAP) - 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

Online Analytical Processing (OLAP) - Decision support software that allows the user to quickly analyze information that has been summarized into multidimensional views and hierarchies.

http://www.olapcouncil.org/

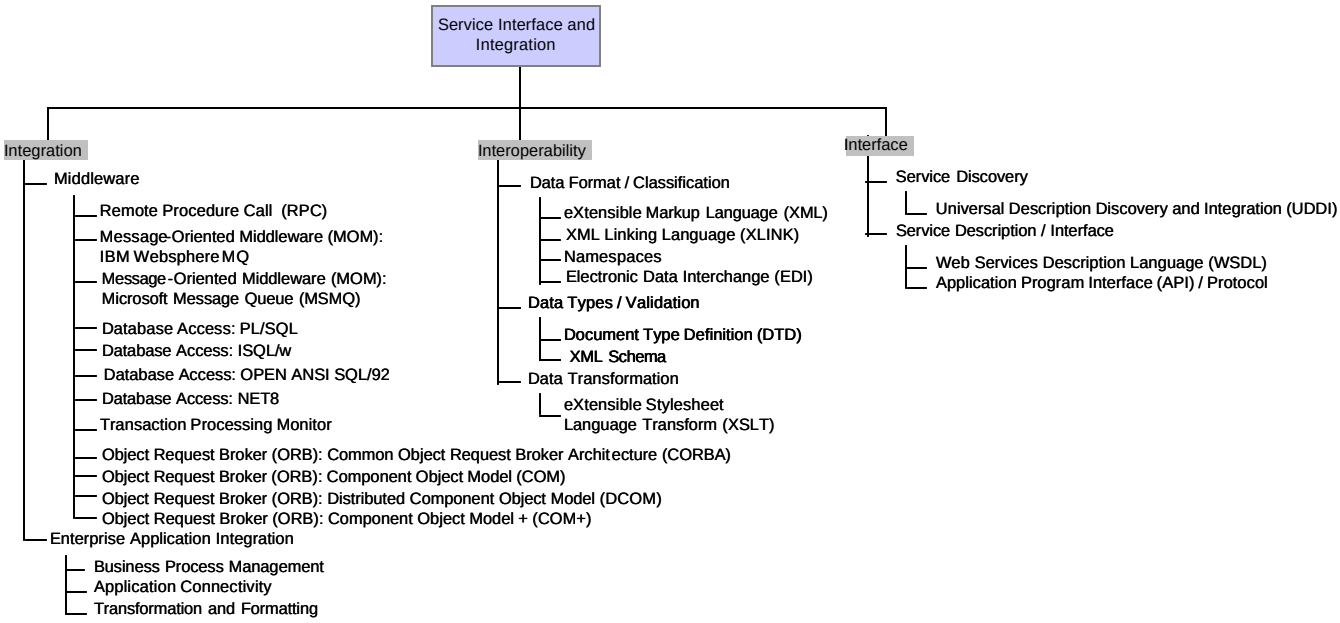
XML for Analysis - XML for Analysis uses the Simple Object Access Protocol (SOAP) to let Web browser-based programs access back-end data sources for data analysis. The specification allows companies to build online analytical processing (OLAP) and data mining applications that work over the Web.

http://www.microsoft.com/data/xml/XMLAnalysis.htm

SERVICE INTERFACE AND INTEGRATION

The Service Interface and Integration Area, as illustrated in Figure 11, defines the discovery, interaction and communication technologies joining disparate systems and information providers. Component-based architectures leverage and incorporate Service Interface and Integration specifications to provide interoperability and scalability.

Figure 11 – Service Interface and Integration Area



The Service Interface and Integration Categories, Standards, and Specifications are defined below:

Integration

Integration defines the software services enabling elements of distributed business applications to interoperate. These elements can share function, content, and communications across heterogeneous computing environments. In particular, service integration offers a set of architecture services such as platform and service location transparency, transaction management, basic messaging between two points, and guaranteed message delivery.

Middleware – Middleware increases the flexibility, interoperability, and portability of existing infrastructure by linking or "gluing" two otherwise separate applications.

Remote Procedure Call (RPC) – RPC is a protocol allowing a program on a client computer to invoke a program on a server computer.

http://www.faqs.org/rfcs/rfc1831.html

Message-Oriented Middleware (MOM): IBM Websphere MQ – Software solution providing APIs, queue management, message routing, automatic fail-over, and workload balancing. Message-Oriented Middleware (MOM) is software residing in both sides of the client/server architecture providing support for asynchronous calls, or messages, between applications. Message queues are used to track and store requests waiting for execution by the source application. Messaging allows otherwise complex programming and networking details to be abstracted from the developer.

http://www-3.ibm.com/software/ts/mqseries/

Message-Oriented Middleware (MOM): Microsoft Message Queue (MSMQ) – Software technology providing synchronous and asynchronous message queueing, routing, and security. Message-Oriented Middleware (MOM) is software residing in both sides of the client/server architecture providing support for asynchronous calls, or messages, between applications. Message queues are used to track and store requests waiting for execution by the source application. Messaging allows otherwise complex programming and networking details to be abstracted from the developer.

http://www.microsoft.com/msmq/

Database Access: PL/SQL – Oracle's procedural extension to industry-standard SQL. Database Access provides access to and across multiple database technologies in a distributed environment. Database Access is provided through the use of native database Application Programming Interfaces (APIs), client-side APIs, or server-side database gateways.

http://www.orafaq.org/faqplsql.htm

Database Access: ISQL/w – Microsoft's implementation of ANSI SQL. Database Access provides access to and across multiple database technologies in a distributed environment. Database Access is provided through the use of native database Application Programming Interfaces (APIs), client-side APIs, or server-side database gateways.

http://www.microsoft.com/sql/

Database Access: OPEN ANSI SQL/92) – SQL is the information processing industry standard language of relational database management systems (RDMS). ANSI X3.135-1992 (also referred to as SQL-92 and ANSI SQL) is the industry standard for Database Language SQL. This standard promotes the portability and interoperability of database application programs and facilitates maintenance of database systems across heterogeneous data processing environments. SQL-92 provides a standardized way for embedding SQL statements into application development languages. Database Access provides access to and across multiple database technologies in a distributed environment. Database Access is provided through the use of native database Application Programming Interfaces (APIs), client-side APIs, or server-side database gateways.

http://www.odbmsfacts.com/articles/sql-92.html

Database Access: NET8 – NET8 (called SQL*NET prior to Oracle8) is Oracle's client/server middleware product that offers transparent connection from client tools to the database, or from one database to another. SQL*Net/ Net8 works across multiple network protocols and operating systems. Previous versions referred to as SQL*Net. Database Access provides access to and across multiple database technologies in a distributed environment. Database Access is provided through the use of native database Application Programming Interfaces (APIs), client-side APIs, or server-side database gateways.

http://www.orafaq.org/faqnet.htm

Transaction Processing Monitor – Software providing synchronous messaging and queuing along with other transaction management services designed to support the efficient processing of high volumes of transactions. Core services include load balancing, rollback/commit, and recovery. Transaction Processing provides cost-effective scalability to applications and database systems by managing and throttling transactions on behalf of the database system.

Object Request Broker (ORB): Common Object Request Broker Architecture (CORBA) – An architecture that enables objects to communicate with one another regardless of what programming language they were written in or what operating system they're running on. Object Request Broker (ORB) is a technology enabling distributed objects to communicate and exchange data with remote objects. ORB encapsulates the locality and implementation of the objects, allowing users to develop applications that leverage components by accessing the components interface.

http://www.corba.org

Object Request Broker (ORB): Component Object Model (COM) – A software architecture created by Microsoft to design and build component-based applications. COM object capabilities are accessible from exposed interfaces. Object Request Broker (ORB) is a technology enabling distributed objects to communicate and exchange data with remote objects. ORB encapsulates the locality and implementation of the objects, allowing users to develop applications that leverage components by accessing the components interface.

http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28000520

Object Request Broker (ORB): Distributed Component Object Model (DCOM) – An extension of the Component Object Model (COM) that allows COM components to communicate across network boundaries. Traditional COM components can only perform interprocess communication across process boundaries on the same machine. Object Request Broker (ORB) is a technology enabling distributed objects to communicate and exchange data with remote objects. ORB encapsulates the locality and implementation of the objects, allowing users to develop applications that leverage components by accessing the components interface.

http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28000520

Object Request Broker (ORB): Component Object Model + (COM+) – COM+ is an extension of the COM that provides a runtime and services that are readily used from any programming language or tool, and enables extensive interoperability between components regardless of how they were implemented. Object Request Broker (ORB) is a technology enabling distributed objects to communicate and exchange data with remote objects. ORB encapsulates the locality and implementation of the objects, allowing users to develop applications that leverage components by accessing the components interface.

http://msdn.microsoft.com/library/default.asp?url=/nhp/Default.asp?contentid=28000520

Enterprise Application Integration – Refers to the processes and tools specializing in updating and consolidating applications and data within an enterprise. EAI focuses on leveraging existing legacy applications and data sources so that enterprises can add and migrate to current technologies.

Business Process Management – This process is responsible for the definition and management of cross-application business processes across the enterprise and/or between enterprises.

Application Connectivity – This process provides reusable, non-invasive connectivity with packaged software. This connectivity is provided by uni- or bi-directional adapters.

Transformation and Formatting – This process is responsible for the conversion of data, message content, information structure, and syntax to reconcile differences in data amongst multiple systems and data sources.

Interoperability

Interoperability defines the capabilities of discovering and sharing data and services across disparate systems and vendors.

Data Format / Classification – Defines the structure of a file. There are hundreds of formats, and every application has many different variations (database, word processing, graphics, executable program, etc.). Each format defines its own layout of the data. The file format for text is the simplest.

eXtensible Markup Language (XML) – XML has emerged as the standard format for web data, and is beginning to be used as a common data format at all levels of the architecture. Many specialized vocabularies of XML are being developed to support specific Government and Industry functions.

http://www.w3.org/XML/

XML Linking Language (XLINK) – A language used to modify XML documents to include links, similar to hyperlinks, between resources. XLINK provides richer XML content through advanced linking integration with information resources.

http://www.w3.org/TR/xlink/

Namespaces – Namespaces are qualified references to URI (Uniform Resource Identifier) resources within XML documents.

http://www.w3.org/TR/REC-xml-names/

Electronic Data Interchange (EDI) - Defines the structure for transferring data between enterprises. EDI is used mainly used for purchase-related information. ANSI X.12 refers to the approved EDI standards.

http://www.disa.org/

Data Types / Validation – Refers to specifications used in identifying and affirming common structures and processing rules. This technique is referenced and abstracted from the content document or source data.

Document Type Definition (DTD) – DTD is used to restrict and maintain the conformance of an XML, HTML, or SGML document. The DTD provides definitions for all tags and attributes within the document and the rules for their usage. Alterations to the document are validated with the referenced DTD.

http://www.w3.org/TR/REC-html40/sgml/dtd.html

XML Schema – XML Schemas define the structure, content, rules and vocabulary of an XML document. XML Schemas are useful in automation through embedding processing rules.

http://www.w3.org/XML/Schema

Data Transformation - Data Transformation consists of the protocols and languages that change the presentation of data within a graphical user interface or application.

eXtensible Stylesheet Language Transform (XSLT) - Transforms XML document from one schema into another. Used for data transformation between systems using different XML schema, or mapping XML to different output devices.

http://www.w3.org/Style/XSL/

Interface

Interface defines the capabilities of communicating, transporting and exchanging information through a common dialog or method. Delivery Channels provide the information to reach the intended destination, whereas Interfaces allow the interaction to occur based on a predetermined framework.

Service Discovery - Defines the method in which applications, systems or web services are registered and discovered.

Universal Description Discovery and Integration (UDDI) - UDDI provides a searchable registry of XML Web Services and their associated URLs and WSDL pages.

http://www.uddi.org/about.html

Service Description / Interface - Defines the method for publishing the way in which web services or applications can be used.

Web Services Description Language (WSDL) - WSDL is an XML based Interface Description Language for describing XML Web Services and how to use them.

http://www.w3.org/TR/wsdl

Application Program Interface (API) / Protocol - A language and message format used by an application program to communicate with the operating system or some other control program such as a database management system (DBMS) or communications protocol. APIs are implemented by writing function calls in the program, which provide the linkage to the required subroutine for execution. Thus, an API implies that some program module is available in the computer to perform the operation or that it must be linked into the existing program to perform the tasks.

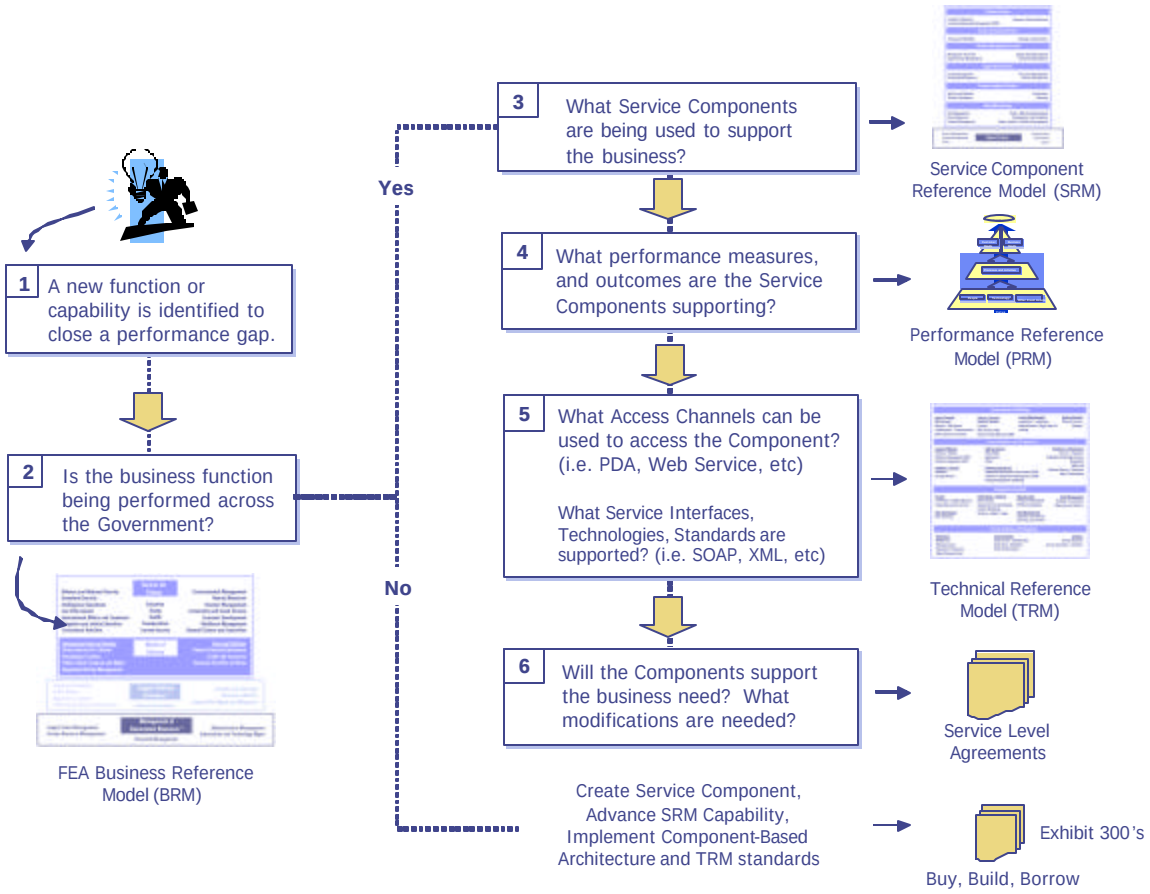
3. Use and Maintenance

FEAPMO

USE AND MAINTENANCE

The FEA and TRM are intended to assist Federal Agencies in optimizing re-use of IT capability and technology investments. The TRM provides the foundation for identifying target technical architectures and should be reflected where applicable in baseline architectures. Migration strategies should be developed to outline the approach to achieving the target architecture consisting of component-based architectures. Upon "publishing" this collection of information, and coupling with the SRM, agencies are offered the ability to discover workable capability and technology configurations. Realizing and leveraging existing investments is a key benefit and driver of the FEA. Figure 12 illustrates at a high level, an example of using the TRM in conjunction with the other reference models of the FEA.

Figure 12 – FEA / TRM Utility Example

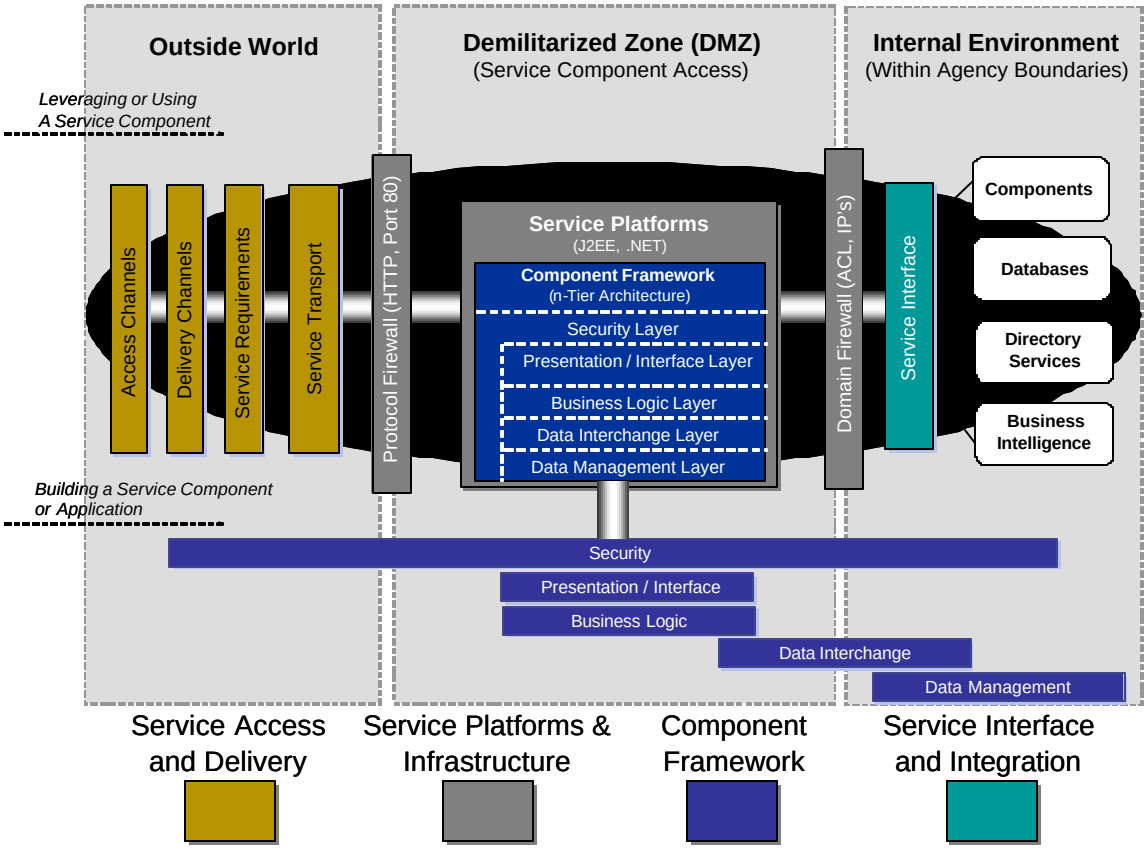


The alignment and relationship of the TRM to Agency enterprise architectures is one of the next steps towards implementing the model across the Federal Government. Aligning the layers of the TRM and the SRM to Agency technology, business (process or activity), and application architectures enables the categorization of an Agency's IT investments, assets and infrastructure by the common definition and purpose of the Service Specifications and Service Components in the TRM and SRM, respectively.

AGENCY IMPLEMENTATION OF THE TRM

As a foundation for Federal Agencies, the TRM is composed of technology components that encompass the Agency's entire infrastructure – internal, external and the connection in between. These components reside across the network and the application topology. Figure 13 expands the TRM model presented in earlier chapters to illustrate where an Agency might typically employ the TRM service category components.

Figure 13 – TRM in relation to an Agency's Infrastructure



While the above Figure identifies typical placement of various components within an Agency's environment, it is only an example, and should not be construed as prescriptive. Many technology standards can exist within more than one partition of the physical networks that make up an enterprise infrastructure. The Agency TRM should specifically identify the technologies and products used within their enterprise as well as their physical or logical placement.

To illustrate employment of the concepts above, the US Patent and Trademark Office (USPTO) is presented here as an example. They restructured their Agency TRM (USPTO TRM version 7) to better align their baseline and target architectures with the TRM. USPTO also conducts technology reviews in order to continue, contain, or retire technologies (a part of standards life cycle management) as necessary as they strive to achieve a components-based architecture.

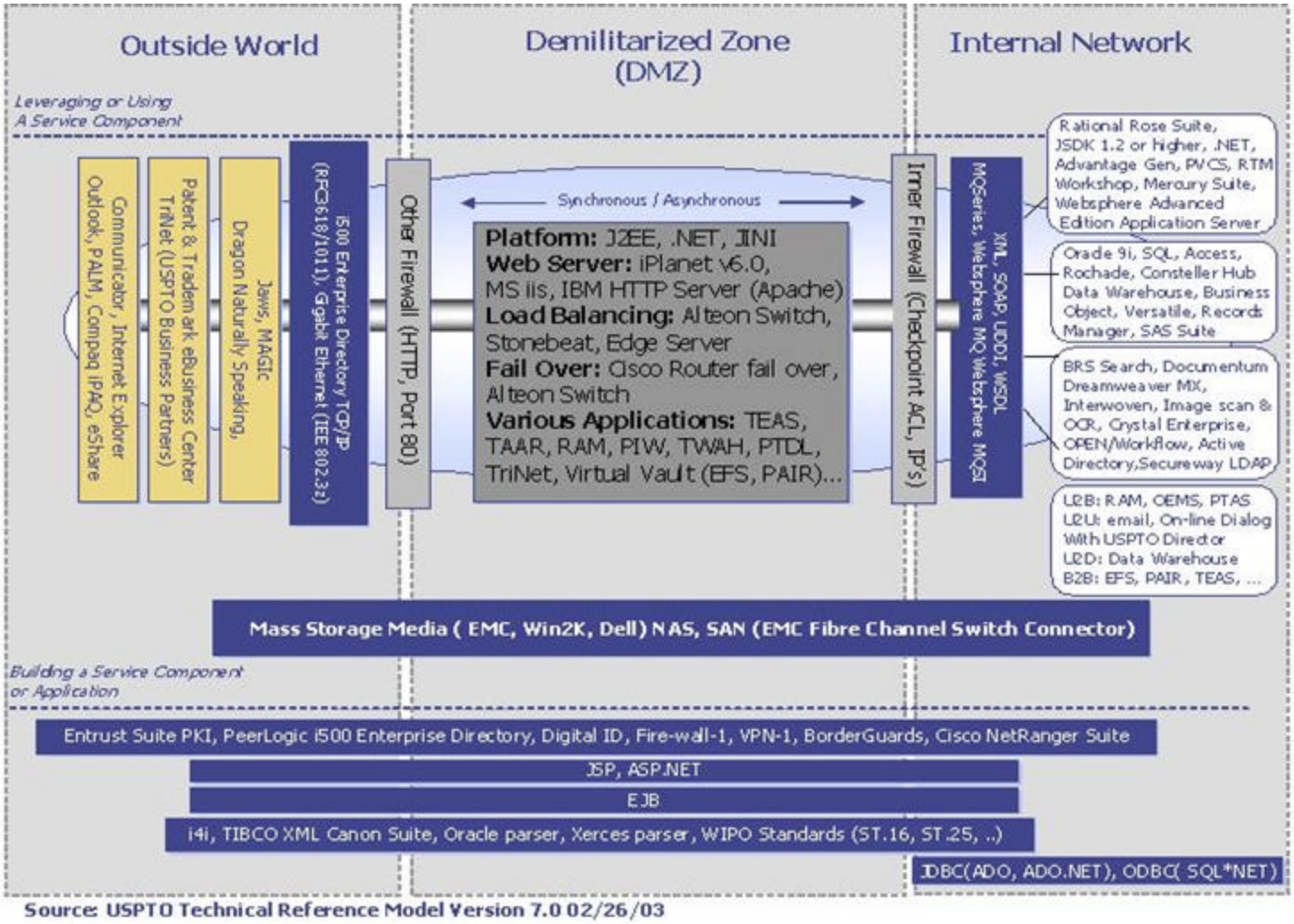
USPTO claims three significant advantages with the implementation of their TRM in alignment with the FEA:

- Reduced infrastructure complexity through identification of standards and products

- Improved leveraging of innovative technology
- Increased access to information

Figure 14 shows how USPTO has aligned their technology to the TRM.

Figure 14 – USPTO Implementation of / Alignment to the TRM

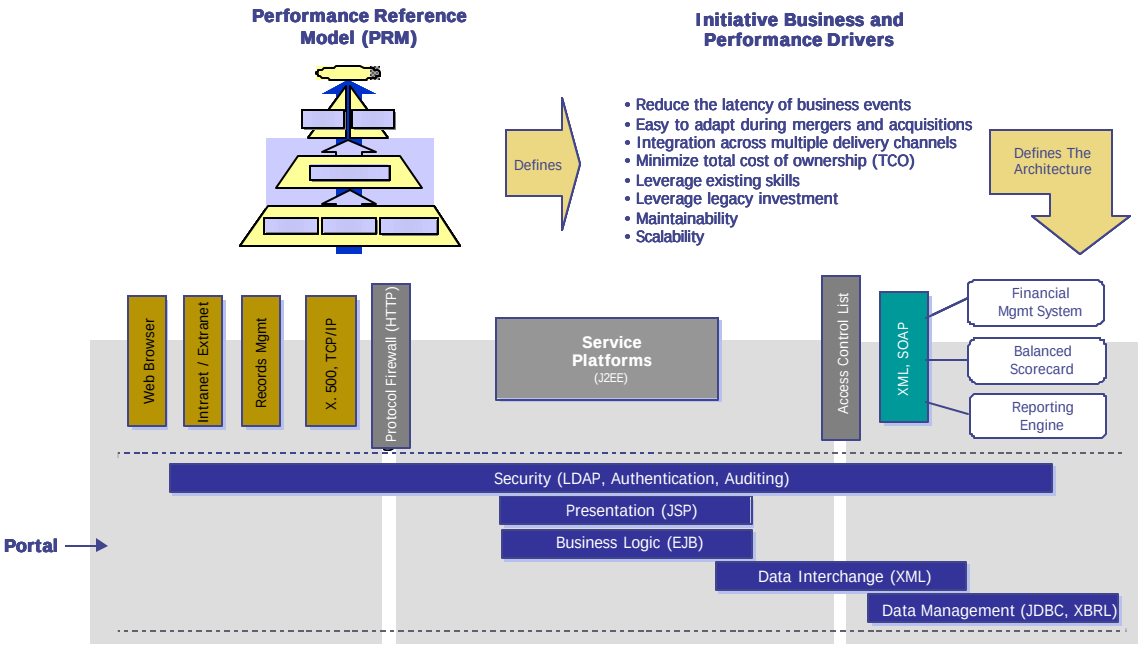


Source: USPTO Technical Reference Model Version 7.0 02/26/03

The Federal Government can benefit from the information gathered and efforts engaged by USPTO (and other Agencies) through the "patterns" they establish of workable capabilities and technologies in meeting business and performance requirements. As Agencies begin assembling technology components, and determining the appropriate configurations to overcome specific performance gaps, certain technology patterns begin to emerge. These patterns, mapped to the SRM service components employed and performance goals (from the PRM) achieved, will

also indicate specific environments where they succeed. Agencies can leverage the success of others in building their own architectures. Figure 15 illustrates a sample pattern.

Figure 15 – Sample FEA Pattern for Back Office Integration



Additionally, in the coming months and via separate documents, the FEA-PMO will look to provide some guidance on selection of various components and building secure infrastructures.

THE FEDERAL ENTERPRISE ARCHITECTURE MANAGEMENT SYSTEM (FEAMS)

FEA analysis and maintenance are greatly facilitated through the use of an Internet-based, automated EA repository and analysis tool – the Federal Enterprise Architecture Management System (FEAMS). Agencies will be given access to FEAMS and can use it in both capital planning and architecture development efforts.

In addition to storing the FEA reference models, FEAMS, as shown conceptually in Figure 17, will include general information on Agencies' IT initiatives. Initiatives will be aligned to the BRM Lines of Business that they support, to the Service Components and technology that these components leverage, and to the performance metrics that they use in achieving performance objectives. It is OMB's goal that the FEAMS will eventually include information on all of the capital assets in which Federal Agencies invest.

Figure 16 – FEAMS

The FEA, including the TRM, is being released to Federal Agencies through the FEA-PMO Website, http://www.feapmo.gov. The website provides Agencies with downloadable access to the TRM in multiple electronic formats – PDF, Word, and XML. FEAMS will advance these capabilities by providing Agency representatives the ability to search across FEA reference models to determine the availability of services and components they may be able to reuse as well as data and information that they may be able to share.

FEA RELATED ACTIVITIES

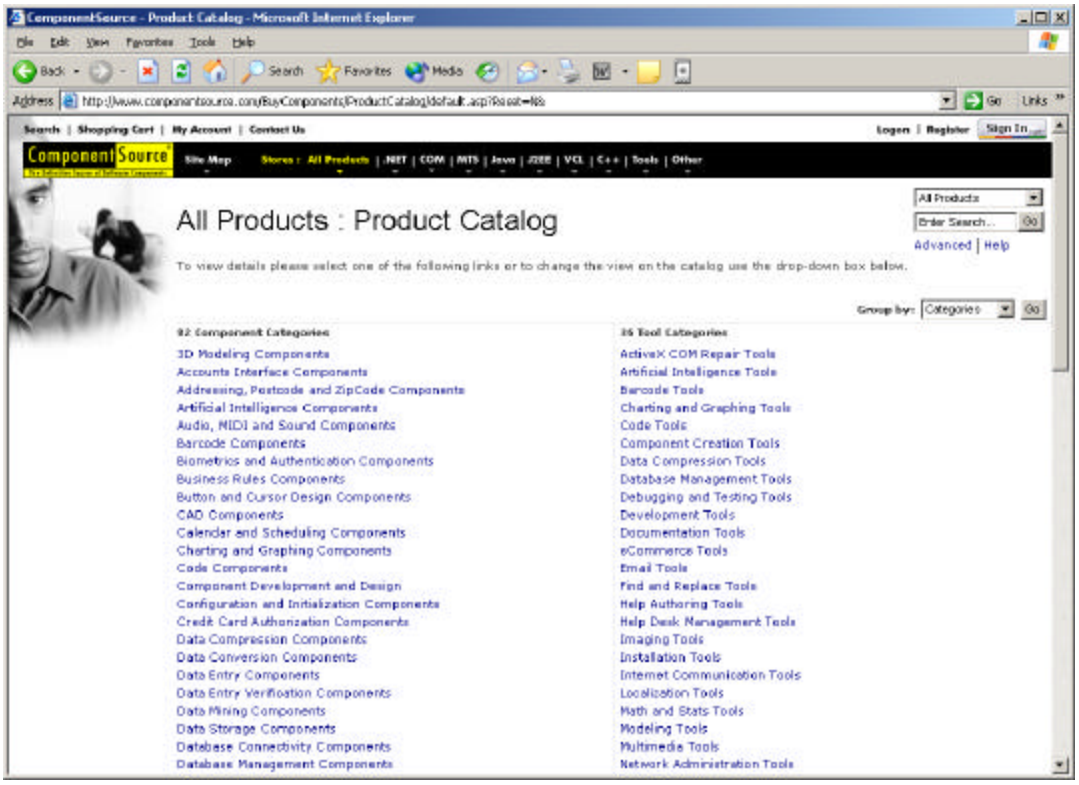
Component Registry /Repository

The creation of a component repository and registry for component directory services is envisioned to be one of the tangible, ongoing outcomes of the FEA analysis at the service, technology and data layers. As reusable components are identified and collaboration between

agencies begins to take place, there will be the need for a repository and mechanism for storing, maintaining and sharing these components.

The AIC Components Subcommittee (CS) will establish a component registry that will be accessible over a secure extranet to initiative owners and the managing partners of the 24 Presidential Priority E-Gov initiatives. For instance, this registry might provide an area in which users can find, evaluate, share, download, and rate software components, as shown in Figure 16, as well as a directory of business functions that the component supports. The component registry might provide the "latest" research and analysis surrounding the selection and recommendation of third-party / industry components that are supported by the Component-Based Architecture specifications.

Figure 17 - Sample Component Registry



The component repository will enable the rapid discovery and assembly of data, technology and service components for use in applications and systems that support the objectives of an agency initiative. Whenever possible, the sharing of these components will be accomplished through standards-based, reusable, secure, portable and interoperable technology. Service Level Agreements between the partnering agencies will help build the understanding for implementation and usage of these components.

The establishment of a component registry is widely accepted as a means in which organizations can leverage the knowledge and intellectual property across public, state and local indus-

tries. For instance, organizations such as the National Association of State CIO's (NASCIO) have partnered with ComponentSource to create the National Software Component Exchange (NSCE) for state and local governments. Other exchanges and component-service organizations offer similar services that should be leveraged when making the decision to partner and/or build a similar solution.

Component-Based Architecture (CBA)

The AIC CS is currently engaged in the creation of the FEA Component-Based Architecture (CBA) document to support the adoption of components and component-based architectures within and across an enterprise. This document will include, but will not be limited to:

- Scope and Objectives
- A high-level concept of the Government's federated component based architecture, and the strategy for evolution from today to the future.
- Why Component Based Architecture?
- What is it?
- What does it do for me?
- When to apply it?
- Where does it apply?
- Who applies it?
- High-level use case / concept of operations
- Impacts / Implications
- Constraints and Challenges
- Examples and lessons learned

Solution Development Life Cycle (SDLC)

The FEA-PMO, in close cooperation with the SAWG and the AIC CS is championing the creation of a new Solution Development Life Cycle (SDLC) that focuses on the rapid assembly and deployment of solutions using a Component-Based approach. The SDLC consists of parallel strategic, business, and implementation phases that continually measure and evolve the initiative performance, objectives, and outcomes – in respect to how the initiative supports the customer. The SDLC will compliment existing SDLC methodologies and provide a common framework to support the architecting, development, and implementation of cross-agency e-Gov initiatives.

EFFECT OF THE TRM ON CAPITAL PLANNING AND BUDGET PROCESSES

Under OMB Circular A-130, Management of Federal Information Resources, all agencies are required to document and provide their EAs to OMB as significant changes are incorporated. In addition, under the President's FY 2004 Budget Preparation process outlined in the revised OMB Circular A-11, agencies must align their budget justifications with the President's Management Agenda, Federal E-Government initiatives, and the Federal Enterprise Architecture. Specifically relating to architecture, agencies must map their major IT capital investments to the Components and Technologies identified in the SRM and TRM and describe how their initiatives support the Service Components and TRM Service Specifications.

The FEA, SRM, and TRM are intended for use in analyzing investments in IT and other capital assets. As Agencies plan for their capital assets, they will be able to access the FEA to identify:

- Agencies that are building or have already built similar Service Components and capabilities,
- Agencies that are already collecting or plan to collect similar data,
- Suitable technologies, standards, and specifications already being used elsewhere, in support of Service Components, in the Federal government.

In this manner, the FEA will provide agencies with a powerful tool to investigate alternatives to costly (and potentially duplicative) IT investments *up front* and before a significant expenditure of resources. Reciprocally, OMB will also be using the FEA to ensure that proposed Agency IT investments are not duplicative and to analyze the architecture throughout the year to identify opportunities for cross-agency collaboration. As such, the FEA will help ensure that the Federal Government eliminates duplicative and redundant investments, and that Agencies save time and money by leveraging re-usable business processes, data, IT components, and innovative technologies.

UPDATES AND MODIFICATIONS TO THE TRM

As the FEA – and the TRM – become institutionalized, the maintenance and upkeep will be the responsibility of both agencies and OMB. Agencies will provide the high-level information – often through the annual budget preparation process – required to maintain (and mature) the FEA. However, comments on the TRM may be made throughout the year through the FEAPMO website as new issues arise.

OMB and the FEAPMO look forward to a process of consistent improvement to all aspects of the FEA, and certainly, Federal Agencies must play a primary role in the process. OMB will receive, compile, normalize, and validate comments on the TRM throughout the year. A process is being established to integrate the TRM revision process with Agencies' capital planning efforts and OMB's budget review and allocation processes to ensure that updated versions of the model are issued before agencies initiate their annual planning processes.

In summary, OMB envisions a collaborative and mutually beneficial management plan for the FEA that will result in positive outcomes for all stakeholders. OMB will work during the coming

months to develop and publish a formalized FEA Management and Maintenance Plan that will provide explicit instructions to Agencies on the roles, responsibilities, standards, and expectations for the management and upkeep of the FEA. The high-level information contained herein is intended to provide the general concepts of current thinking in this area, and is subject to modification. OMB commits to obtaining Agency comments and feedback on the FEA Management and Maintenance Plan.

A. The Federal Enterprise Architecture

FEAPMO

THE FEDERAL ENTERPRISE ARCHITECTURE

The FEA is a business and performance-based framework for cross-agency, government-wide improvement. It provides OMB and the Federal agencies with a new way of describing, analyzing, and improving the federal government and its ability to serve the citizen. The lack of an FEA to support cross-agency collaboration was cited by the 2001 Quicksilver E-Government Task Force as a key barrier to the success of the 24 Presidential Priority E-Government initiatives approved by the President's Management Council in October 2001.

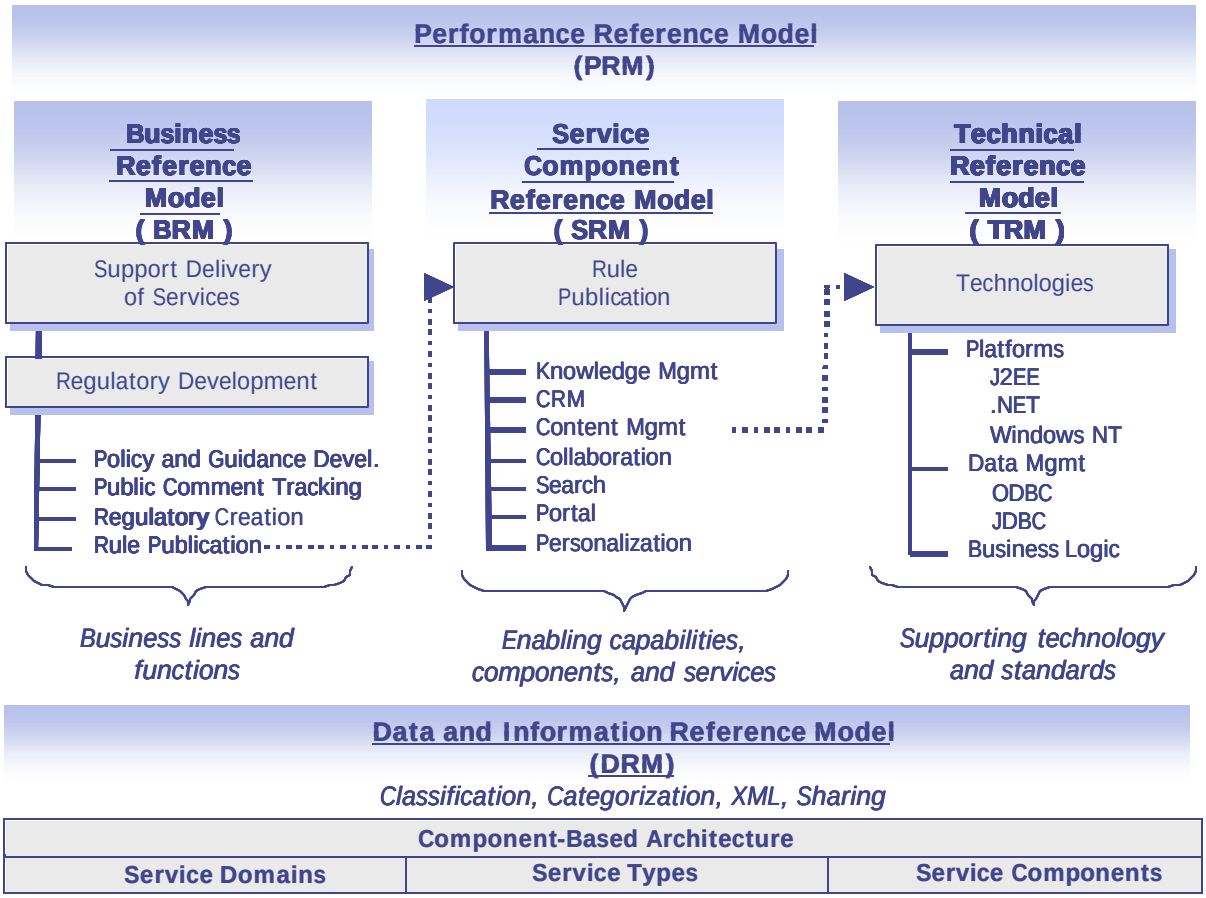
Led by OMB, the purpose of the FEA is to identify opportunities to simplify processes, re-use Federal IT investments and unify work across the agencies and within the lines of business of the Federal Government. The outcome of this effort will be a more citizen-centered, customer-focused government that maximizes technology investments to better achieve mission outcomes.

FEA REFERENCE MODELS

The FEA, as illustrated in Figure 18, is comprised of five (5) reference models. Collectively, they will provide universal definitions and constructs of the business, performance and technology of the Federal Government. The reference models will serve as a foundation to leverage existing proc-

esses, capabilities, components and technologies as Government Agencies build target enterprise architectures. They are designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across Federal Agencies.

Figure 18 – FEA Reference Model Integration



Performance Reference Model (PRM) – Version 1.0 in Draft

The PRM is a framework for performance measurement that provides common outcome and output measures throughout the Federal government. It allows agencies to better manage the business of Government at a strategic level while providing a means for gauging progress towards the target FEA. The PRM accomplishes these goals by establishing a common set of general performance outputs and measures that agencies use to achieve program and business goals and objectives. The model articulates the linkage between internal business components and the achievement of business and customer-centric outcomes. Most importantly, it facilitates resource allocation decisions based on comparative determinations of which programs/ organizations are more efficient and effective.

The PRM will be designed to integrate with and complement OMB's development of the Program Assessment Rating Tool (PART) and Common Measures Initiative. By defining outcome and output for TRM Service Areas, Representations and Categories, the PRM will provide the tools necessary to measure the effectiveness of technology across agency initiatives at the federal enterprise level. Additional guidance on both the PRM and PART will be provided as the linkages between these two initiatives are clearly established.

Business Reference Model (BRM) – Version 2.0 Released

The Business Reference Model is a framework for describing the business of the Federal Government independent of the agencies that perform it, and serves as the foundation for the FEA. The model describes the Federal Government's Lines of Business, including its internal operations and its services for the citizen, independent of the Agencies, bureaus and offices that perform them. By describing the Federal Government around common business areas instead of the stove-piped, agency-by-agency view, the BRM promotes agency collaboration.

The new version of the BRM (Version 2.0) will be used in support the FY 2005 budget formulation process. Version 2.0 differs from its predecessor as a result of agency comments, the addition of a new "Mode of Delivery" layer, and closer alignment with the Budget Function Classifications.

Service Component Reference Model (SRM) – Version 1.0 Released

The SRM is a business-driven, functional framework that classifies Service Components with respect to how they support business and/or performance objectives. The SRM is structured across horizontal service areas that, independent of the business functions, can provide a leverageable foundation for reuse of applications, application capabilities, components, and business services.

Technical Reference Model (TRM) – Version 1.0 Released

The TRM is a framework to describe how technology supports the secure delivery, exchange, and construction of Service Components. The TRM outlines the technology elements that collectively support the adoption and implementation of component-based architectures, as well as the identification of proven products and toolsets that are embraced by government-wide initiatives such as FirstGov.Gov, Pay.Gov, and the 24 Presidential Priority E-Government Initiatives.

Data and Information Reference Model (DRM)

The Data and Information Reference Model (DRM), still being developed, will describe, at an aggregate level, the data and information that support program and business line operations. The model will aid in describing the types of interactions and information exchanges that occur between the Federal Government and its various customers, constituencies, and business partners. It will categorize the government's information along general content areas specific to BRM sub-functions and decompose those content areas into greater levels of detail, ultimately to data elements that are common to many business processes or activities. The DRM will establish a commonly understood classification for Federal data and lead to the identification of duplicative data resources as well as enable information sharing between agencies. A common data classification model will streamline the processes associated with information exchange

both within the Federal government and between the government and its external stakeholders.

The DRM will be produced on a business line by business line basis, as opposed to a single cumulative effort. This allows for the identification of and concentration on key improvement areas, producing clearly identified and measurable results. The FEA-PMO will oversee the focused DRM efforts to ensure all appropriate points of integration are identified. Additionally, they will also help identify reusable data components that support a Lines of Business and/or Sub-functions. Attributes of these data components would be based upon specifications as identified in the FEA Technical Reference Model, and accessed by a specific Service Component.

BENEFITS OF THE FEA

Federal Agency Benefits

The FEA is a high-level architecture for the Federal government as a whole. The FEA provides vision into the federal-wide architecture giving each agency a collection of new capabilities from which to choose for defining and implementing their target EA environments. Agencies will now be able to:

- Save time and money by leveraging reusable business processes, data, and IT-components in other agencies
- Leverage FEA work products as a catalyst for agency-specific EA efforts
- Ensure proposed investments are not duplicative with those of other agencies – prior to developing business cases and submitting them to OMB
- Suggest modifications to the SRM to ensure future versions accurately portray the Capabilities and Service Components of industry and government, including the role specific agencies play
- Improve interoperability and security through common infrastructure components and services.

Agencies have played a key role in the definition of Version 1.0 of the TRM and they will continue to play a role in its advancement and evolution.

Citizen Benefits

The true driver behind the FEA effort is the need to improve the government's delivery of services both to and for the public. The agency-centric systems and processes that have previously characterized government must be replaced with integrated, citizen-centric applications and processes. The FEA, through its support of the 24 Presidential Priority e-Government Initiatives, as well as other cross-agency, citizen-focused e-Government efforts, is a key component of the citizen-focused transformation in government.

OMB Benefits

The FEA provides both the policy and budget sides of OMB with a greatly enhanced cross-agency analytical capability. Through the analysis of the FEA, OMB will be able to see opportunities for collaboration of processes, data, services and technology across the federal agencies. Examples of the benefits to OMB include:

- Elimination or consolidation of redundant investments in IT capabilities, business processes, or other capital assets
- Identification of common business functions across agencies
- Integration of performance measurement with the budget process along the key business lines of the government

Congressional Benefits

Application of the Federal Enterprise Architecture will yield a wealth of information on Federal business lines, programs and capital investments; and the performance of those business lines, programs and capital investments. This information will be made available to Congress as it considers the authorization of and appropriation of funding for Federal programs, and as it fulfills its oversight responsibilities on behalf of the citizen.

THE FEA PROGRAM MANAGEMENT OFFICE

The Federal Enterprise Architecture Program Management Office (FEA-PMO) was established to provide the definition and development of the FEA. The FEA-PMO manages and coordinates activities surrounding:

- Definition of the FEA through a set of Government-wide reference models focusing on business, performance, service components and capabilities, technologies and standards, and data and information.
- Development of a core set of standardized Component-Based Architecture models to facilitate technology solutions and the development of a complete architecture (baseline, target, and transition) for each of the 24 Presidential Priority E-Government initiatives.
- Assessment and identification – through high-level architecture, critical success factors, and Line of Business performance information – of new opportunities for business process and system consolidation to improve government efficiency and effectiveness.
- Development of a web-based FEA repository, called the Federal Enterprise Architecture Management System (FEAMS), to provide agencies with a view of cross-agency information and the alignment of IT investments to areas of the Federal Enterprise Architecture.

FEA-PMO Governance Structure

OMB's Chief Technology Officer (CTO) and the FEA Program Manager provide leadership for the FEA-PMO and SAWG (discussed in the following section). The CTO is responsible for ensuring the overall success of the Program, overseeing the completion of program tasks, and securing the approval of program deliverables by senior OMB officials and the Program's external stakeholders (e.g., CIO Council, CFO Council, Procurement Executives Council, and senior federal IT, planning, budget, and procurement staff). The Program Manager provides day-to-day guidance on specific tasks, approves all work products and deliverables, and secures sufficient resources to carry the Program forward. Both the CTO and Program Manager communicate with the Program's stakeholders, both formally and informally, on a regular basis.

The Solution Architects' Working Group (SAWG)

To support the development and implementation of various reference models and IT investments, including the Presidential Priority E-Gov initiatives, the FEA-PMO has the SAWG. The primary goal of the SAWG is to help define and evolve several of the federal reference models, and to assist Federal Agencies with activities surrounding the technical design of solutions to their initiatives and to promote and communicate the principles of Component-Based Architecture and component reuse. Specifically, the SAWG is responsible for:

- Providing E-Government initiative teams with a suite of templates to assist in the development, implementation and rollout of an e-Gov initiative.
- Providing E-Government initiative teams with solution architects who will assist in defining initiative blueprints, and validate system architectures to support the planning and implementation of the Presidential Priority E-Government initiatives.
- Establishing linkages between relevant Government-wide entities to ensure that standards, best practices, and lessons learned are leveraged across the entire government.
- Selecting, recommending, and assisting in the deployment of technologies that are proven, stable, interoperable, portable, secure, and scalable.
- Facilitating the migration and transition of E-Government initiatives from legacy and "inward-driven" architectures (i.e. agency-centric), to architectures that embrace component-driven methodologies and technology reuse.
- Identifying and capitalizing on opportunities to leverage, share, and reuse technologies to support common business requirements, activities, and operations across the Federal Government.
- Championing the creation and propagation of intellectual capital that can assist in E-Government transformation.

The FEA Program Manager serves as the Chief Architect for the SAWG. In this capacity, the Program Manager is responsible for determining the appropriate technical architecture to be used

by the Presidential Priority E-Government initiatives, and providing the necessary technical oversight of the project to ensure that the technical architecture is designed, developed, tested, and deployed properly and according to plan. The Chief Architect works closely with the Solutions Architect(s) assigned to each E-Government initiative to ensure that all technical architecture requirements are adequately addressed.

OMB's IT/E-Gov Working Group

OMB's IT/E-Gov Working Group provides overall guidance to the work of the FEA-PMO. It is comprised of the IT leads within the Resource Management Offices and officials within the Information Policy and Technology Branch. The ultimate goal of the Working Group is to leverage Agency management, investments, and processes to achieve effectiveness and efficiency goals for programs and business lines. The Working Group played a key role in developing and implementing IT policy in preparation for the Fiscal year 2004 budget process, and is playing a key role in the development of the Federal Reference Models.

FEA-PMO Support Team

The FEA-PMO Support Team was established to execute program tasks in accordance with the FEA-PMO Work Plan. The Support Team is responsible for delivering draft work products – for example, the FEA reference models – to Federal agencies for review and comment; and analyzing and incorporating comments, as appropriate, to produce a final product. The FEA-PMO has created and maintains a website, http://www.feapmo.gov, to help ensure that Program information is shared with as wide an audience as possible.

Architecture and Infrastructure Committee (AIC) – Components Subcommittee

The AIC Components Subcommittee (CS) was established to foster the identification, maturation, use and reuse of Component-Based Architectures and Architectural Components in the federal government. The underlying objectives are to foster the basic principles of interoperability, reusability and portability of processes, services and infrastructure components by Federal agencies and related partners and stakeholders as they modernize their business processes through data sharing, e-government automation and improved information systems.

The efforts of the CS will be directed toward achieving these outcomes:

- Identification of business processes, service components, and technologies for re-use through analysis of the FEA Service Component and Technical Reference Models.
- Reduction of IT costs for federal agencies achieved through the re-use of business processes, service components, and technologies.
- Rapid solution development through the re-use of components.
- Rapid integration of disparate business services.
- Development and implementation of e-Gov solutions based on component-based architectures.