U.S. Environmental Protection Agency

Technical Reference Model

Information Technology and Security Architecture Program

Version 2.0

November 30, 2006

EPA

OFFICE OF ENVIRONMENTAL INFORMATION

Attachment 1-C

This page intentionally left blank.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

The United States Environmental Protection Agency (EPA) Enterprise Architecture (EA) program aligns the Agency's Information Technology (IT) resources with the Agency's mission, goals, and business processes. One component of the EA program is the development of an Enterprise Technology Architecture (ETA) that serves as the blueprint for how IT supports the Agency's mission. The ETA provides explicit descriptions of the current and desired state of IT as a resource to facilitate and enhance the business processes and management of the Agency.

The EPA's ETA contains five elements:

- Technical Reference Model (TRM)

  The TRM is a classification model useful when discussing technologies relevant to the EPA. All technologies in use at the Agency should fit into a classification identified in the TRM.

- Baseline Enterprise Technology Architecture

  The Baseline ETA is a point-in-time description of the then-current state of technology usage within the Agency.

- Target Enterprise Technology Architecture

  The Target ETA describes the desired future state of technology usage in the Agency. This is what the Agency wants the IT infrastructure to become.

- Enterprise Technology Architecture Sequencing Plan

  The ETA Sequencing Plan outlines a plan by which the Agency can transition from the Baseline state to the Target state.

- Standards Profile

  The Standards Profile provides an up-to-date list of the technologies that are in use at the agency at any given time, along with an indication of their current use status (e.g. proposed target, current standard, legacy technology). It is used by the Program Offices and system owners to identify what technologies may be used in systems development to ensure compliance with the ETA.

The purpose of this document is to describe the TRM. This is done first generically to explain the concept of the TRM (Section Two), and then specifically to describe the building blocks of EPA's ETA (Sections Three and Four). The Appendices provide References, a mapping to the Federal Enterprise Architecture TRM, and a Technology Glossary.

The remainder of the section explains the purpose, intended use, and scope of the TRM.

1.1 Abstract

The Clinger-Cohen Act of 1996 assigns the Chief Information Officer (CIO) the responsibility to develop an Enterprise Architecture including Information Technology (IT) architectures to manage information resources. The Office of Management and Budget (OMB) Memo M-97-02,

Funding Information Systems Investments, October 1996, requires that Agency investments in major information systems be consistent with the information technology architecture.1 The objective of a Technical Reference Model (TRM) is to define the building blocks for developing the information technology architecture.2

The Office of Management and Budget (OMB) Memorandum of June 1997, concerning IT architectures, calls for all federal agencies to develop a TRM and a Standards Profile:

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

EPA's TRM establishes a framework for the Enterprise Technology Architecture in terms of information technologies. The Standards Profile is maintained in the IT Roadmap web site, which contains a database of products and technologies the Agency identifies as standard, target, interim, and legacy.

The EPA TRM consists of seven major technology areas with associated subcategories by which the Agency's IT standards are expressed. The seven major areas are: 1) User Environment, 2) Application Technologies, 3) Data Technologies, 4) Hosting Platforms, 5) Networks/Telecom, 6) Technology Management, and 7) Security.

EPA's first TRM document was finalized and published in November 2002. This TRM Version 2.0 document is a revision of the 2002 document that reflects the maturity of the Agency's EA and the industry advances and trends of the last three years. It also reflects changes in the way the technology architecture layer treats Application Technologies within the context of the EA, and a redefinition of the Security section to use a three-layered model3. Further refinements include some name changes for technology categories and adjusting the major category interfaces along the lines of a technology "stack."

1.2 Purpose and Intended Use

A Technical Reference Model is a framework that:

- Defines the building blocks for developing an ETA.
- Provides a common conceptual view of IT.
- Establishes a common vocabulary to better describe, compare, and contrast systems and components.

---

[1] Preface, Federal Enterprise Architecture Framework, V1.1, CIO Council, September 1999

[2] Department of Commerce Technical Reference Model and Standards Profile Framework, pg 1, February 6, 2001

[3] EPA has adopted a security architecture based on the Burton Group Security Model. See Section 4 of this document.

- Provides a consistent set of technology areas, definitions, interfaces, and relationships used to address interoperability and open system issues.
- Serves as a basis (or aid) for the identification, comparison, and selection of existing and emerging standards.

In a more colloquial generic sense, a TRM is the way in which one views an organization's IT resources. It is the "lens" through which the IT resources come into focus.

The EPA TRM provides guidance to enterprise architects, technology managers, developers, and individuals that plan, acquire, develop, or use information systems. The TRM promotes open source design by identifying the relationship between IT components and services. Program Office system developers or system owners can use the TRM to identify types of technologies they will need to enable their systems. By focusing on these technology categories, they can articulate their IT needs at a higher level of abstraction, which avoids linking solutions to specific products or vendors too early in the system development life cycle (SDLC). Once the major technology categories for system design are identified, the developer or owner can use the IT Roadmap to trace each specific TRM section to the products and technologies the Agency supports for each function.

The TRM also provides the foundation for the organization and structure of the baseline and target technology and security architectures. The TRM establishes a common technology vocabulary and identifies a set of services and interfaces common to EPA IT systems.

The EPA TRM also establishes consensus on how to describe, discuss and relate the many technologies that support the IT infrastructure and enables a common framework for mapping IT investments in the Capital Planning and Investment Control (CPIC) process. This includes tracing investments to the Standards Profile and to the Federal Enterprise Architecture model as required by the Office of Management and Budget (OMB). The OMB EA Assessment Framework 2.0 calls for mapping technology and investment according to a Technical Reference Model. Using the EPA TRM for these purposes facilitates strategic alignment of IT investments while ensuring a high level of program maturity under the OMB Assessment Framework capabilities model.

1.3 Scope

The EPA TRM is to be considered as the foundation model describing services, interfaces, and their interrelationships that can be applied to all systems, including multi-platform, networked, and distributed applications. All EPA organizations are encouraged to apply the model to their information technology systems to support interoperability, portability, open systems, and standards.

The TRM is intended to provide developers, IT managers, system owners, and other interested parties with a complete vocabulary to enable technology planning and decision making within EPA. It is not a stand-alone document, but is meant to be used in conjunction with other architecture and systems design documentation. In specific, the TRM should be used in conjunction with the Architecture Development Methodology, the EPA EA Meta-model framework, and the 2006 Standards and Guidance documents in order to understand IT management at EPA. Specific systems developers should use the TRM in conjunction with the Standards Profile to determine appropriate technology solutions available for use at EPA.

The TRM is not meant to specify specific vendor products that are used within the Agency; that is the goal of the Standards Profile. The TRM simply provides a classification scheme by which to

discuss technology and to plan for systems development at a high level. If a program office wishes to know what specific products can be used for the development of a system, they should consult the standards profile for more information. If an office has concerns that a particular technology solution is not reflected in the standards profile, they should follow the processes explained on the IT Roadmap site4 or contact the Technology Architect for guidance. Typically, if a technology is not represented in the standards profile, it will undergo a review with the Technology Architecture Working Group (TAWG) and be proposed as a standard to the Quality Technology Subcommittee (QTS) for approval before addition to the Standards Profile.

1.4 Applicability

The EPA TRM applies to EPA information systems and information technology application enablers at all EPA organization levels and environments. The EPA TRM guides the selection of interfaces and services that form technology architecture. The model provides a basis for categorizing the Agency's Standards Profile, for structuring the baseline and target technology and security architectures, and for categorizing the research projects in the Technology Architecture Change Management (TACM) process.

Different stakeholder groups will use the TRM in different ways. For instance, IT managers should map their technology solutions to the TRM for CPIC purposes and to ensure alignment with the Agency's technology architecture. Architects should do the same and use it to facilitate redundancy or gap analysis. If TRM subcategories are not available to support a new design component, then this provides an opportunity for managers and solution architects to requisition new IT subcategories. Developers may need the TRM for a common vernacular, and more importantly use the Standards Profile to complete solution architectures and obtain guidance on product and security standards.

1.5 Relationship with the Enterprise Architecture

The following diagram in Figure 1.1 depicts the relationship between the EA, the ETA, and the Security Architecture (SA). The Federal Enterprise Architecture Framework (FEAF) is comprised of five layers, from top to bottom: Goals, Business, Data, Applications, and Technology. Each layer provides a foundation for the layers above it and guidance to the layers below it. For example, the Business Layer identifies the business processes used within the Agency. These processes are mapped directly to the goals above to show the necessity of each process in meeting the Agency's mission. The processes are also mapped to the data in the layer below to show what data holdings support the business process.

Figure 1.1 depicts the business segments that EPA has defined for the purpose of collecting, integrating, and maintaining architecture information across the Agency. The segments include horizontal business functions as defined by the FEAF Business Reference Model as well as EPA vertical business programs consistent with the environmental media that EPA protects.

The TRM is a product of the cross-cutting IT Management segment that organizes the ETA to facilitate communication, analysis, and effective management of information technology. As such, it is applicable to the technology layer of all other segment architectures as well as the Enterprise Architecture. The TRM is represented by the box diagram in the middle of the figure.

[4] http://intranet.epa.gov/ITRoadmap

Within the TRM, IT Security is further broken down into a separate model based on the Burton IT Security Architecture Model. This model facilitates the communication, analysis, and effective management of the rules, processes, and technologies employed to ensure the proper safeguarding of Agency IT assets and data. More information on the Burton IT Security Architecture Model is described later in this document in Section 4.

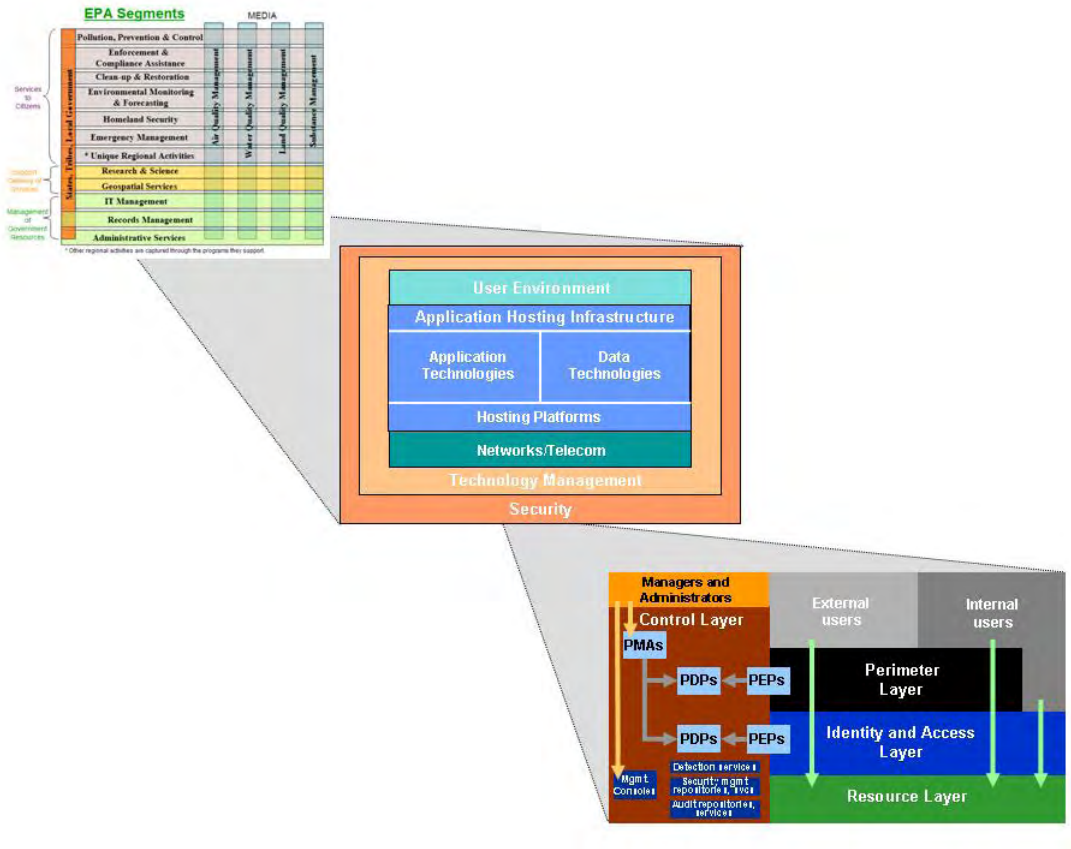

Figure 1-1. Relationship of Enterprise Architecture, Technical Reference Model, and Information Security Technology Model

1.6 Document Lifecycle

The EPA TRM is not a point-in-time snapshot, but rather a living document. As the IT environment changes, new categories of technologies will become available and older categories will reach obsolescence. As such, the TRM will need to adapt over time to maintain relevance in supporting IT decision processes at the Agency. Revisions of the TRM will happen at regular timeframes as dictated by the Technology Architect. These revisions will consist of a review and vetting with the Technical Architecture Working Group (TAWG), including Program Office representatives, to ensure that the broadest possible needs will be met with each revision of the model. Should a system owner or other reader identify a category that is not properly identified within the TRM, they should bring this omission to the attention of the Technology Architect.

Attachment 1-C

This page intentionally left blank.

2. CONCEPT OF A TECHNICAL REFERENCE MODEL

The following subsections describe the concepts behind a Technical Reference Model.5

2.1 Background

When two or more systems or components are required to interoperate or exchange information, a set of common and consistent service and interface definitions is needed to ensure the integrity of the information to be passed or exchanged. The set of definitions, integrated into a framework or abstract, is known as a reference model. Rapid changes in technology and the need to provide extensive user coordination and effect cross-service operations have underscored the need for such a set of definitions associated around a model. The need for a foundation model that provides greater definition and clarity of technologies and interfaces is essential for an open-systems approach conducive to achieving interoperability.

The intent of the TRM is to support standards and interoperability across organizational domains, in joint development, and across a wide range of applications.

2.2 Structure

Diverse and demanding IT requirements often result in the need for a structured TRM. Proper attention to, and application of, a TRM will assist organizations in achieving more effective levels of portability and interoperability in the following ways:

- Consistent and common description of interoperability requirements.
- Consistent specification of system architecture.
- Support for commonality across systems.
- Consistent use of standards.
- Comprehensive identification of interfaces.

Any such model must also be evolutionary and flexible enough to support current as well as future needs across a broad range of requirements and platform configurations. The model must be tailored to enable users to extract only those elements required to support their domain needs and to leverage technology. The set of technologies and interfaces must also be robust enough and malleable enough to enable system architects and developers to develop their domain-specific views. The higher-level abstraction of a TRM is intended to fill that role.

2.2.1 Consistent and Common Description of Interoperability Requirements

Information exchange and interoperability requirements between systems can be described in terms of the model's vocabulary and the particular layer of the model affected by the requirement. The use of the TRM may influence the description of requirements in such a way that standards may emerge for describing interoperability requirements. Using the TRM, systems can be

[5] Based on Department of Defense Technical Reference Model, Ver. 2.0, Section 2, April 9, 2001, web site at: http://www-trm.itsi.disa.mil

defined in terms of consistent definitions and common functionality (i.e., via the technologies and interfaces). The functionality is needed to provide interoperability, portability, and scalability of computerized applications across networks of heterogeneous hardware/software platforms. The model may even be used to develop guides for describing interoperability requirements.

2.2.2 Consistent Specification of System Architecture

The TRM facilitates developing system architectures that specify the characteristics of key system interface requirements and ensures that these requirements and the system and technical "responses" are clearly related to each other across all views of a technological architecture. The application layer, for example, should be defined primarily in support of application interoperability and portability. The data layer should define the standardization and registration of individual data element types to meet the requirements for data sharing and interoperability among information systems throughout the enterprise.

2.2.3 Support for Commonality Across Systems

The TRM facilitates the development of a common infrastructure to support interoperability and portability of applications. The TRM guides the implementation of a communications and computing infrastructure based on standards and common interoperability and including, but not limited to, operating systems, database management, data interchange, network services, network management, and user interfaces. The basis for a common infrastructure is to identify core capabilities that are applicable across multiple technology areas. This, in the near term, enables the migration from static applications to a more open environment enabling data and data format transparency across different platforms.

2.2.4 Consistent Use of Standards

Use of the TRM facilitates the profiling and grouping of technology so that standards can be set for use and acquisition. A Standards Profile defines the specific set of technologies and products that support the categories and interoperability in the TRM.

The Standards Profile establishes the minimum criteria needed to specify technology that achieves standardization across the enterprise. It also identifies a number of mandatory standards while providing a published set of recommendations for others.6

2.2.5 Comprehensive Identification of Interfaces

The TRM, via its combination of technology and interface views, facilitates the identification and definition of interface services and specifications. The TRM interface identification can be expressed graphically in a TRM diagram or defined more explicitly, but in both cases, the interface identification is logical rather than physical and is a high-level description. This is needed to support the development of complex and enterprise-wide systems that require technology components from many different areas.

[6] EPA's Standards Profile is provided in the IT Roadmap web site http://intranet.epa.gov/ITRoadMap.nsf

3. VOCABULARY

One of the goals of this document is to establish a common vocabulary to describe, discuss, compare, and contrast information technology components at EPA. This vocabulary is specific to EPA, but by no means exclusive to the Agency, as other agencies may use a similar vocabulary. This section introduces the principal common technology vocabulary that is used to describe the technology areas in Section Four.

3.1 Enterprise Technology Architecture (ETA)

The ETA is a comprehensive blueprint of an organization's information technology that includes five components: 1) TRM, 2) Standards Profile, 3) Baseline Architecture, 4) Target Architecture, and 5) Sequencing Plan. The ETA provides explicit descriptions of the current and desired state of the information technology resources of an organization.

3.2 Technical Reference Model (TRM)

A conceptual framework that defines a common vocabulary and a set of technology categories and relationships, in order to define the building blocks of the ETA of an organization, in this case, the EPA. The use of a TRM allows an organization to better control and coordinate development, acquisition, interoperability, and support of its IT systems.

3.3 Technology Categories and Subcategories

This TRM describes the main elements of a complete IT resource as a set of discrete technologies. A technology category is a high-level abstraction that consists of a collection of components organized to accomplish a specific function or set of functions. Technologies support requirements via their functions and capabilities. This document discusses an extensive set of technology areas and subcategories that support EPA's business and mission as set forth in the Agency's Enterprise Architecture.

3.4 User Environment

The User Environment section of the TRM consists of the sum of all hardware and software components needed to interface with EPA's information technology for all levels and types of users. The User Environment section defines the technologies that allow users to interact with the rest of EPA's IT resources or to perform productive work using IT resources at the user's immediate disposal. User Environment technologies are often dependent upon, or work in conjunction with, technologies belonging to the other sections of the TRM. The User Environment is categorized into ten subcategories.

3.5 Application Hosting Infrastructure

The Applications Hosting Infrastructure refers to a grouping of three major TRM sections that work together to enable the development, deployment, and hosting of applications. This infrastructure supports application development from design to deployment and then manages and delivers the application functionality and the data storage and maintenance required in using an application. The major TRM sections that make up the Applications Hosting Infrastructure are Application Technologies, Data Technologies, and Hosting Platform sections, described below.

3.5.1 Application Technologies

The Application Technologies provide the environment for developing and deploying applications for the Agency. These technologies include application platforms, web platforms, portal software, middleware, web services, application languages, and the development environment. Custom applications that perform Agency functions are not included, as these are part of the Applications Layer of the Enterprise Architecture pyramid and not a part of the IT infrastructure. The Application Technologies section is categorized into five subcategories.

3.5.2 Data Technologies

The Data Technologies provide the handling, management and storage of data that can be defined independently of the processes that create or use it. This section provides the "Store for Use" function or the "activities necessary to ensure (that) data are readily available and ready for analysis."7 This section includes maintaining a set of coordinated databases, providing for metadata, data integration, interchange, replication, transformation, analysis, reporting, search, and migration. The technologies of this section make data available to the Application and User Environment technologies. The Data Technologies section is categorized into eleven subcategories.

3.5.3 Hosting Platforms

The Hosting Platform technologies provide a comprehensive processing environment consisting of the computer platforms, file systems, storage systems, and delivery systems that support the IT infrastructure and the Agency's applications. Hosting Platform technologies may be centrally located or may be distributed geographically but centrally coordinated. The TRM divides the Hosting Platforms section into seven subcategories.

3.6 Networks/Telecom

The Networks and Telecom Technologies support the transfer, translation, and transport of data and multimedia packets across the distributed enterprise so that all the services can interoperate and connect with the User Environment; and these technologies also support the provisioning of telecommunication systems. The technologies within this section include handling different packet types and protocols, routing of packets, and maintenance of the networks and telecommunication services that connect the enterprise. This section is categorized into fifteen subcategories.

3.7 Technology Management

The Technology Management technologies provide the comprehensive system administration, control, and management of information systems, resources, and support services. This section interacts with and helps to facilitate the smooth functioning of all the other TRM areas. Since this section is intertwined with the other categories of technology, it is sometimes difficult to isolate from the other categories. For instance, this area does not include the maintenance of hosting systems, but does include the planning and forecasting of systems' capacity to meet usage and performance goals. The Technology Management section is categorized into four subcategories.

[7] Model for Information Integration, EPA Information Integration Program, Draft, February 19,2002, pages vi and 37-50

3.8 Security

The Security Technologies are employed by EPA to ensure appropriate levels of integrity, confidentiality, and availability of information processing systems and mission critical information. Information security is necessary to protect the information and IT resources from malicious or unintentional loss, misuse, and destruction. This section of the TRM is concerned with qualifying access to enterprise information and the information technology infrastructure, preventing and detecting unauthorized activities, maintaining integrity and confidentiality of information and IT resources and those mechanisms which manage the security of the resource. It includes a perimeter layer, an identity and access layer, and a control layer8. This set of technologies cuts across all domains and services of the EA and TRM respectively. The Security section is categorized into nineteen subcategories.

[8] "Information Security Technology Model," Burton Group, Midvale UT, Jan. 17, 2005

Attachment 1-C

This page intentionally left blank.

4. EPA TECHNICAL REFERENCE MODEL

The TRM describes the agency's information technology (IT) as belonging to one of seven major categories:

- User Environment
- Application Technologies
- Data Technologies
- Hosting Platforms
- Networks/Telecom
- Technology Management
- Security

The TRM also diagrams the relationship between these seven major technology areas by arranging to show how they logically relate. The usefulness of this model is to compartmentalize the wide array of IT into manageable areas and to guide the development of the ETA. Diverse groups at EPA applying IT to their business needs can reference a common model for technology and a common vocabulary. Doing so also helps to improve the representation of these groups in the process of developing the technology architecture through the use of this common vocabulary. EPA's TRM also provides a way to categorize the Agency's IT Research Agenda which brings new technology to the ETA.

4.1 EPA TRM Design

The seven major sections of the TRM and the interfaces that collectively model EPA's Enterprise Technology Architecture are illustrated in Figure 4.1 below.

The User Environment contains the technologies that interface directly with the user. This area is shaded in light blue.

The Application Hosting Infrastructure contains the technologies that enable applications and information and is the core of the ETA. This area is shaded in blue.

The Networks/Telecom technologies connect the IT resources of the Agency and provide the Agency's connections to the "outside world". This area is shaded in teal.

The Technology Management and Security areas impact all other categories and so are shown as layers that surround the other categories. These services are colored in shades of orange.

The TRM diagram layers the technology areas in a meaningful fashion. Each distinct layer is separated by a dark line. The top layer consists of end-user technology and its position serves to emphasize that the other layers exist to support the end-user. The next three layers are grouped together into the Application Hosting Infrastructure because together they provide the common services used to develop and support EPA's software applications. The interface lines in this grouping are white instead of black, indicating that the three areas are interdependent and grouped. The Networks/Telecom layer is separated by a black line from the Application Hosting Infrastructure indicating that it operates mostly independently. The Technology Management and

Security layers are also separated with black lines as they operate independently but affect the technology areas they surround. Figure 4.1 illustrates the interfaces of the various sections.

Each of the major technology areas is associated with more specific types of technology (i.e., subcategories). The subcategories are more granular and provide a more specific indication of what technologies are in use. A few subcategories are broken down into an even finer level of detail to accommodate additional specificity. For example, the Systems Management subcategory is made up of a number of more granular subcategories and the Security Service is divided into three layers with more granular subcategories.

Each of the seven major technology areas and their associated subcategories are defined and described in the rest of this section so that Agency stakeholders (IT architects, managers, developers) and other users of the TRM have a good understanding of the major technology area concept and the technologies being used in each subcategory. Stakeholders can and should contribute to the validation of the subcategory definitions and/or the modification of the definitions to accurately reflect how technology is used at EPA. As new technologies are implemented in the Agency, new subcategory designations may be required. Similarly, some subcategories may no longer be used at EPA and these are deleted or replaced.

EPA TECHNICAL REFERENCE MODEL – With Subcategory Detail

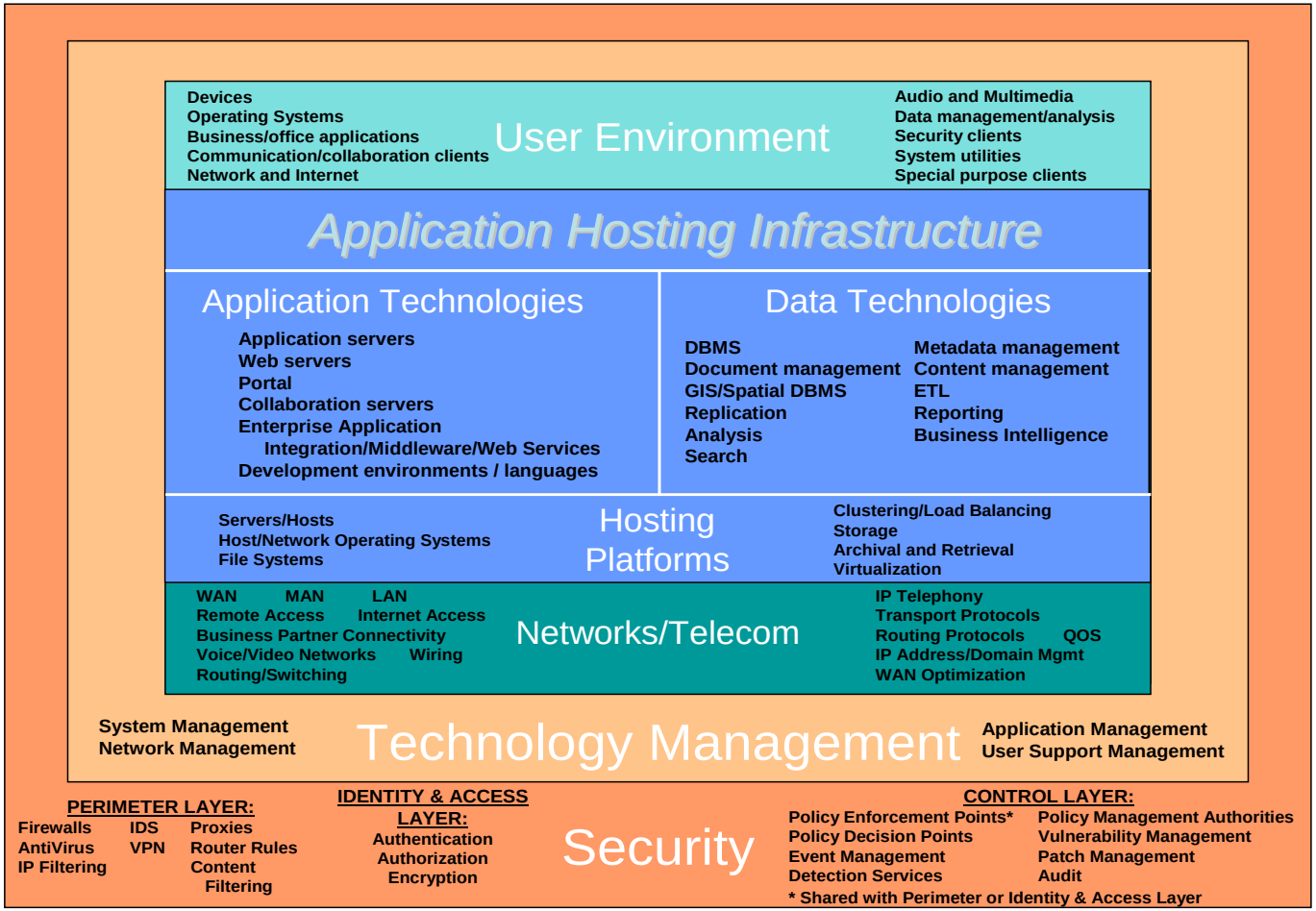

Figure 4-1. EPA Technical Reference Model

4.2 Descriptions of TRM Major Technology Areas and Subcategories

The initial delineation of the seven major technology areas, identified in Figure 4.1, provides a framework that enables a basic viewpoint and understanding of EPA technology architecture. The EPA TRM major technology areas are each associated with more specific technologies (i.e., subcategories). Some of these subcategories are also associated with a finer level of detail (e.g., Systems Management). The purpose of the following discussion is to define these subcategories so that Agency IT stakeholders (architects, managers, developers) and other users of the TRM have a good understanding of the concept and can contribute to the validation of the definition and/or the modification of the definition to accurately reflect the particular use of technology at EPA. As new technologies are implemented, a new piece of technology may require a new subcategory designation and definition. The TRM is a living document that will be modified to reflect the needs of EPA and the rapid changes occurring in information technology.

User Environment (UE) Technologies

The User Environment is defined as the sum of all hardware and software components needed to provide computerized access to EPA information for all levels and types of users. This set of technologies provides the devices and their support software and file systems that makes it possible for users to receive, view, store, transfer, and process digital information. In certain instances, User Environment technologies are tightly integrated with, and are sometimes difficult to distinguish from, corresponding technologies within the Application Hosting Infrastructure.

Devices

Provide the end-user with the physical hardware necessary to interface with the rest of EPA's IT resources. They allow an end-user to connect with other IT resources, and to communicate, process, and store information locally and through the rest of the infrastructure. Devices include any end-user equipment that is connected to the EPA network or used to process environmental data. As such it includes traditional computer workstations, laptops, mainframes, etc., as well as personal digital assistants (PDAs), web-enabled phones, GPS devices, and field and laboratory equipment capable of transferring data via electronic means.

Operating Systems

Provide the services needed to make the devices intelligent and capable of storing and retrieving information. Operating Systems provide the interface between the user, the application software, and the hardware devices.

Business/Office Applications

Provide the end-user with software to automate office productivity functions such as filing, documentation, calculation, presentation, and management tasks.

Communication/Collaboration Clients

Allows end-users to communicate and collaborate, whether in real-time or not, with peers inside and outside the EPA.

Network and Internet

Includes software used to establish connectivity and access to information resources over a network, typically the Internet; includes network operating system clients, web browsers, and other, often protocol-specific, software clients.

Audio and Multimedia

Provides software utilities that allow users to open and play audio and video information stored in a variety of formats, including software to process and play streaming audio and video to the user.

Data Management/Analysis

Provides software to analyze, condense, map, graph, and visualize data to make data reliable, manageable, useful, and understandable. It enables the representation of data in a geographical context and can include personal database software, statistical software, and GIS client software.

Security Clients

Provide the user with software to secure user environment devices against threats from connecting the devices to the network or to other devices, and allow users to obtain secure access to remote systems. Also includes software for enabling client side remote access through a Virtual Private Network (VPN) and access management authentication on user devices.

System Utilities

Provides software that makes the end-user's computational environment more secure, productive, manageable, and available—sometimes referred to as “desktop tools.”

Special Purpose Clients

Provides the user with software not included in the other subcategories of the User Environment which performs a specific purpose, often intended for a specific job function. Examples might be software technologies that provide specific services and functions to scientists, attorneys, engineers, or information technology professionals. Single-purpose “commercial off-the-shelf” software often falls into this “catch-all” category.

Application Technologies

Provides the software components that facilitate the development, integration, management, deployment, and delivery of Agency applications. This area provides the support environment for the applications, but does not include the applications themselves.

Application Servers

Provides the software that enables a proper technical platform in which to build complex multi-tiered programmatic applications. Enables the reuse of code, integration of backend systems, and rapid implementation of graphical user interfaces as well as business integration and intelligence suites, gateways for grid computing, support for Service-Oriented Architecture (SOA) development, and features for scalability, availability, manageability, and security.

Web Servers

Provides the software that accepts Hypertext Transfer Protocol (HTTP) requests from clients, typically web browsers, and serves them content as web pages. Keeps logs of page requests and where requests come from, which can be used for audit, security, performance monitoring, and capacity forecasting.

Portal

Provides for integration of functions and data from multiple systems and secure access to those functions and data, with single sign-on, through a custom, personalized user interface.

Enterprise Application Integration (EAI) / Middleware / Web Services

Provides the technologies that facilitate sharing and re-use of logic and data associated with disparate applications, thus allowing integration of business processes. Middleware provides software that acts as an intermediary or interface between applications and application components. Web Services are platform-independent software systems that support application-to-application or machine-to-machine interaction over a network, typically the Internet; these "services" are developed, advertised, and managed in adherence with a set of standard protocols and represent a major component of a "Service Oriented Architecture."

Development Environments / Languages

Provides the development tools and languages used to write, test, and deploy enterprise applications or standalone programs, including software to manage the development environment, code management, code libraries, object libraries, language compilers, software emulation tools, Computer Aided Software Engineering (CASE) tools, object-oriented designer tools, and quality assurance development and software testing.

Collaboration Servers

Provide a framework of services to facilitate the communication and sharing of information, either in real-time or not, with peers both inside and outside of the EPA. Typical services of a Collaboration Server include file sharing, discussion forums, shared calendars and task lists, virtual team workspaces, web conferencing, and instant messaging. Some of these services require use of Collaboration/Communications Clients as well as Collaboration Servers (e.g. web conferencing often has a client and a server component).

Data Technologies

Data Technologies provide the software infrastructure to collect, store, move, copy, transform, analyze, relate, and manage the data of the Agency.

Database Management Systems (DBMS)

Provides the capability to store, retrieve, organize, and manipulate data (typically "structured" data) in a database management system (DBMS) and includes the operation, maintenance, upgrades, partitioning, user accounting, and documentation of the DBMS and individual databases.

Document Management

Provides for archival, retention, and retrieval of Agency documents, as well as the software to manage EPA's records collection to promote adherence to the National Archives and Records Administration (NARA) record retention policy.

Geographical Information Systems/Spatial DBMS

Includes Geographical Information Systems (GIS) and a specialized DBMS that relates data to geographical locations or other spatial content. GIS blends mapping with data acquisition, classification, analysis, and display of geographic data. A Spatial DBMS relates data with geographical parameters, such as rivers, factories, or roadways and facilitates the use of satellite imaging in producing maps and in displaying environmental data.

Replication

Provides for redundancy of data in order to make it fault-tolerant and thus more available to users and to other systems.

Analysis

Provides the tools used to analyze data and make data useful, as well as the tools to validate, reduce, qualify, and normalize data such that it becomes useful and accurate; and, provides statistical tools to derive information from data to enhance its value.

Search

Provides the tools needed to find data in an efficient manner; uses software to index data, generate topical collections, and provide access points to the data for quick identification and retrieval.

Metadata Management

Facilitates the generation, storage, retrieval, and management of metadata, or "data about data." This subcategory is also one of the tools being used to enable the integration of data. Metadata are maintained primarily in database systems provided by the DBMS subcategory.

Extract Transform and Load (ETL)

Provides for the interchange and migration of data through extraction from source systems, transformation to meet business needs, and loading into repositories such as data warehouses. Since many organizations at EPA collect data separately that ultimately should be combined to make it more useful and accessible, there is a need for ETL tools to build normalized datasets.

Content Management

Manages the life cycle of "unstructured" digital content in the form of text, documents, images, and multimedia (audio or video) files, including the Agency's large and increasingly complex body of web content. This subcategory includes technologies used to catalogue and allocate content and keep it current.

Reporting

Simplifies access to information relevant to the environment for the Agency, external stakeholders, and the general public; it primarily summarizes data for output to an end-user or system such that the presentation of the data is more useable than the format of the source dataset.

Business Intelligence

Provides tools for the development of new knowledge by correlating and combining existing data into new constructs. This subcategory provides a suite of query, analysis, and performance management tools, and applies data integration to make information available for all levels of users across an organization.

Hosting Platforms

Provides the hardware systems and infrastructure to run the applications and to store and archive the data of the Agency. The Hosting Platforms area is divided by the TRM into seven subcategories.

Servers/Hosts Hardware

Provides a variety of hardware platforms, whether centralized at EPA's National Computer Center (NCC) or distributed across Agency locations, as servers for running EPA's enterprise-wide applications. Provides for hosting "departmental" applications that process data for a particular user project or localized user community, as well as "enterprise" applications that serve many Agency users, Agency business partners, and the public.

Host/Network Operating Systems

Provides support for the installation, maintenance, and updates of the operating systems that run on the various servers supported centrally at the NCC and distributed in the Agency's laboratories and regions. These operating systems support the Servers/Hosts Hardware to manage devices, transactions, user accounts, network connections.

Host/Network File Systems

Provides a method for organizing, referencing, and accessing computer files stored on physical media. File systems are often dependent upon or closely associated with the underlying host or network operating system.

Clustering/Load Balancing

Provides for the integration and management of server/hosts to enable physical and logical redundancy for load balancing, failover, and increased performance (i.e., better quality of service). Clustering allows servers to service requests as a group and load balancing distributes the resources of clustered servers so that the central processor unit (CPU) utilization of each server is kept below 100% and so that transaction queue bottlenecks are avoided.

Storage Systems

Includes the support for centrally storing and managing data for transparent retrieval and high-availability in central and distributed server environments. Provides for centralized and discrete storage facilities such as a Storage Area Network (SAN) that has a high-speed sub-network of shared storage devices. Provides functions for assessing storage requirements, protecting and preventing damage to stored data, and ensuring that the infrastructure and processes are in place to backup and recover stored data in the event of equipment failures and/or power outages.

Virtualization

Technologies that present the user a logical grouping or subset of computing resources so that they can be accessed in ways that give benefits over the original configuration. This "virtual" view of the resources is not restricted by the implementation, geographic location, or the physical configuration of underlying resources. Examples are application virtualization through terminal services and server virtualization through establishment of "guest" operating systems in "virtual machines."

Archival and Retrieval

Provides for maintaining a retention copy of Agency data and allowing future online retrieval of the stored data, as well as recovery of damaged, lost data, or archival data.

Networks/Telecom

Provides the hardware infrastructure and systems to connect the other technologies in order that they can connect with each other and with systems outside EPA's IT infrastructure. The EPA Networks/Telecom area is categorized into fifteen subcategories, which are described below.

Wide Area Networks (WAN)

Provides the communication facility between the Agency's Local and Metropolitan Area Networks and between the Agency and the outside world. This facility includes high-speed backbone channels to interconnect geographically distant EPA resources in a seamless fashion.

Metropolitan Area Networks (MAN)

Provides the communication facility that allows EPA buildings collocated in a campus or metropolitan area to be interconnected without having to traverse EPA's Wide Area Network. This subcategory typically provides high-bandwidth fiber optic channels for high-speed communication between Server/Hosts in different buildings and between Server/Hosts and data storage networks.

Local Area Networks (LAN)

Provides the communication facility between departmental Server/Hosts and User Environment (UE) devices that are geographically located in close proximity, typically within a single building. This subcategory typically provides connections to other UE devices and to shared storage, printing, and faxing and includes wired or wireless connections between the UE devices and the local access point.

Internet Access

Provides the communication facility between the EPA Wide Area Network and an Internet Service Provider (ISP), or between EPA facilities or personnel not connected to the EPA WAN and an ISP.

Routing/Switching

Provides the hardware and software for connecting networks and network segments. Routing occurs at Layer 3 (the "Network Layer") of the Open Systems Interconnection (OSI) Reference Model, whereas switching occurs at Layer 2 (the "Data Link Layer"). These devices manage the transfer of data packets from source to destination.

Transport/Network Protocols

Communication protocols that define the formats and operational rules for the transfer of data over a backbone network at Layer 4 (the "Transport Layer") and Layer 3 (the "Network Layer") of the OSI Model. The Layer 3/4 protocols of the Internet Protocol (IP) suite, commonly referred to as TCP/IP, are ubiquitous in today's network and are used exclusively in some; legacy transport/network protocols include IBM's SNA, Novell's IPX/SPX, Digital's DECnet, and Apple's AppleTalk.

Routing Protocols

Protocols used by routers to make decisions about which path is most optimal for reaching remote networks, typically based on metrics such as the number of hops (routers or networks) between source and destination, the path's bandwidth, and delay across a link to the destination. Interior Gateway Protocols are used to communicate reach-ability information internally within an autonomous system, and Exterior Gateway Protocols do so to reach other autonomous systems.

Wiring

The physical cabling infrastructure required for data communication within a building or campus. Wiring includes fiber optic and copper cabling, Ethernet coaxial cable segments, twisted pair copper wiring, network switches, network bridges, and network gateways. This subcategory includes owned and leased resources.

Remote Access

The means by which an organization provides enterprise network connectivity for individuals who are not physically located at enterprise network sites. This remote connectivity supports access to a variety of applications and network-based services (e.g., file services, electronic mail, and intranet resources) as if the user were directly connected to an enterprise LAN (although with perhaps degraded performance). Connectivity for specific single-purpose applications (e.g., using RIM Blackberry devices to access electronic mail messages) is also included.

Business Partner Connectivity

The means by which connectivity is established between an enterprise and its external business partners for mutually beneficial exchange of data. In EPA's case, this connectivity is typically between the Agency and other government agencies which submit environmental data.

Voice/Video Networks

Provides telephone and video communications through a Public Switched Network (PSN) provider, cellular network provider, or satellite network provider, and internal communications through analog or Integrated Services Digital Network (ISDN). This subcategory includes telephone carriers' dial tone support, local message units for voice messaging, and selected calling features like call forwarding. Also provides for local and long distance access, comprehensive telephone directories, directory assistance, automated directory assistance, and the management of portable telephone devices.

IP Telephony

Includes the software and specialized hardware to enable telephone capabilities using the Internet Protocol (IP). This subcategory provides users with voice communication via the EPA data network.

Quality of Service (QOS)

The technologies and practices used to ensure that a network delivers acceptable levels of service to network applications and users in support of the enterprise's business policies. Delay-sensitive traffic such as voice and video typically require a guaranteed amount of throughput or limits on jitter and delay. Enterprises also may prioritize traffic in order to offer premium quality network service.

IP Address/Domain Management

Consists of the hardware and software used to maintain and manage EPA's IP directory and network domain structure, as well as the means to manage the identities and relationships that make up the logical structure of network environments.

WAN Optimization/Performance Enhancement

Technologies that improve the performance of applications by optimizing wide area network utilization through compression, caching, or protocol modification.

Technology Management

Provides the resources and methods to administer and manage the IT resources of the Agency. Information systems are composed of a wide variety of diverse resources that must be managed effectively to achieve the goals of a standards-based environment.

Systems Management

Systems management functionality is divided into the following elements: Usage Monitoring, Capacity Planning and Forecasting, Change Management, Configuration Management, and Asset/Inventory Management.

Usage Monitoring

Measures system resource utilization on the various hosting platforms provided by the Agency. Also measures usage of the Agency's web servers, which include the large Internet and Intranet web sites, and the specialized web application servers.

Capacity Planning and Forecasting

Collects information on system resource utilization and applies statistical trending techniques to provide short-term (planning) and long-term (forecasting) estimates of Hosting platform resource requirements; applied primarily to the Enterprise (mainframe) Server and the large UNIX systems, but may also be applied to the smaller application servers and the High Performance Computing platform.

Change Management

Provides for the orderly and planned execution of changes to computer system hardware and software, including processing capacity, storage capacity, peripheral changes, version upgrades, and operating system migrations. Tracks if and when changes can and should occur, and notifies the user community of upcoming changes to minimize disruption of service.

Configuration Management

Provides for selecting system and system resource parameters to make them more efficient and effective and to ensure that they meet the needs of the user community. Provides the testing and documentation of hardware and operating systems to define the proper operating parameters within the Agency's IT infrastructure to address inter-system conflicts and security concerns. Includes managed distribution of computer resources and publication of configuration and installation documents.

Asset Management

Provides for the inventory, accounting, and allocation of the Agency's computers and peripherals. Helps to manage software upgrades, security, and licensing; useful for depreciating resources and planning capital improvements, as well as tracking the movement of equipment and peripherals.

Network Management

Network Management handles the complex task of ensuring the proper functioning of EPA's network systems and the management of network resources. It monitors network nodes for traffic density, re-routes network traffic in the event of a network component failure, monitors the type of data being transported, and plans for the availability and bandwidth of the Agency's Wide Area, Metropolitan Area, and Local Area Networks.

Application Management

Application Management provides the tools and resources needed to monitor the proper functioning of applications and the distribution and licensing of applications at EPA. Applications include Commercial Off-The-Shelf (COTS) software and internally developed systems; this subcategory includes managing development and deployment of applications.

User Support Management

User Support Management functionality is divided into the following subcategories: Help Desk Support, Software Distribution, and Problem Management.

Help Desk Support

Assists the user community to resolve IT problems and track the cause and solution of IT problems. This subcategory is provided by EPA's Technical Support Center (TSC).

Software Distribution

Provides for the efficient and effective delivery of software to the distributed computing resources of the Agency, including approximately 24,000 personal and mobile computers. Preferably transparent to the user; at the very least, must provide a cost-effective approach to updating software in the distributed computer environment.

Problem Management

Available as part of Help Desk Support to track and manage problems with the Agency's IT resources; supports a problem-tracking database to prioritize, escalate, and close problems and provide historical data on the handling of problems and their resolution.

Security

EPA's TRM Security area is defined as the set of controls designed into all IT components that balance accessibility, availability, and ease of use with the protection, integrity, and confidentiality of EPA's data and IT systems. Security is an omnipresent service encircling all the other TRM sections and cross-cutting the Enterprise Architecture model. It affects the other TRM technology areas but also depends on most of them to be implemented and managed.

The Security section of EPA's TRM is modeled after the Burton Group Information Security Technology Model (ISTM)[9]. This model (see Figure 4.2) divides information technology security into four components or layers: 1) Perimeter, 2) Identity & Access, 3) Control, and 4) Resource. Since the Resource Layer consists of the technologies in the User Environment and the Application Hosting Infrastructure sections, or in the application or data layers of the Enterprise Architecture, it is not a part of the TRM's Security area. The Security area is categorized into three layers containing eighteen subcategories.

[9] ISSN 1048-4620, Copyright 2005 Burton Group.

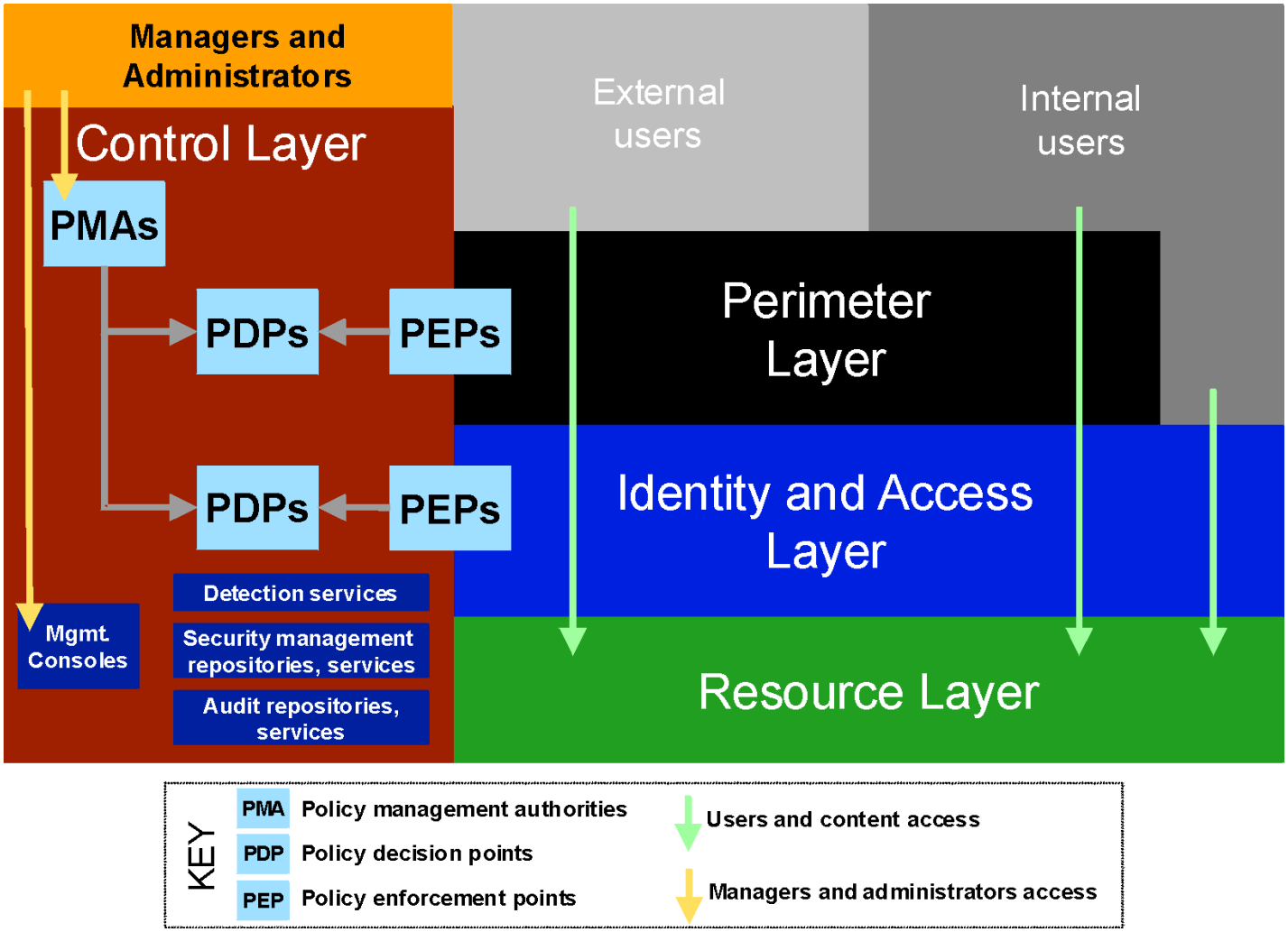

Figure 4-2. Burton Group Information Security Technology Model

Perimeter Layer

Perimeter layer technologies provide identity-independent protection, typically based on location, form, or content of information flows in context, and policy enforcement points.

Firewalls

Provides for packet inspection, location filtering, and traffic filtering. This includes products and solutions such as a planned network Demilitarized Zone (DMZ), firewall hardware, and personal firewalls and other software based solutions.

Intrusion Detection & Prevention

Provides for detection and prevention of attempted intrusions into EPA's network and systems; includes network-based, host-based, and end-user technologies.

Anti-virus

Primarily provides products to detect and neutralize computer viruses at the Email gateway, on email servers, on file servers, and on end-user devices; includes real-time file system protection and regularly scheduled full system scans for personal computers.

Virtual Private Network (VPN)

Provides the hardware and software to communicate securely over a shared, typically public, network. VPNs typically establish an encrypted "tunnel" between source and destination, using one of several available protocols. A VPN "tunnel" may terminate at an endpoint device or elsewhere within an enterprise's infrastructure.

Proxies

Provides hardware and software to allow clients to make indirect connections to network resources, typically by connecting to the requested resource on the client's behalf. Proxies can prevent unauthorized content from entering a system, prevent external systems from seeing internal systems and resources, and restrict the types of traffic that arrive at internal systems.

Router Rules

Provides configuration of Agency routers to perform filtering and packet detention and physical network configuration/segmentation.

IP Filtering

Provides for router-based filtering using Access Control Lists (ACLs) that explicitly permit or deny particular types of IP traffic between particular sources and particular destinations. Also includes host-based IP filtering through TCP wrappers.

Content Filtering

This subcategory provides for filtering of URLs and XML gateway packets.

Identity & Access Layer

The Identity & Access Layer controls access based on identity or other considerations such as transaction state or application context, and policy enforcement points.

Authentication

Technologies used to confirm the identity of users (people, computer systems, applications, or web services) who request access to EPA information. Includes detecting and processing the requirements for identification such as user ID and password.

Authorization

Provides the necessary measures to protect IT resources by ensuring that resource consumers (users, platforms, applications, web services) have been granted authority to use them. Each resource layer component is authorized using policies from the Control Layer of the security model.

Encryption

Includes encryption of data, encryption of communication, and processes to provide proof of the integrity of data (i.e., that data are not altered or destroyed in an unauthorized manner). Provides for cryptographic algorithms and encryption key management, email encryption, session encryption, secure web traffic (HTTPS/SSL), proxy encryption, data encryption, file encryption, and database encryption.

Control Layer

The Control Layer handles security administration and policy management, including configuration, command, control, auditing, and detection. The control layer includes technologies used to distribute, carry out, or otherwise manage policy and includes the registration of authorized users and the serving of identity information through the different control facilities.

Detection

Technologies that help assess the security state of the network by taking data from sensors and security management repositories and generating alerts or notifications to security administrators.

Vulnerability management

Evaluates robustness of the security mechanisms protecting the Agency's IT infrastructure. May include monitoring system management and change control, asset identification, vulnerability identification, vulnerability and asset classification, prioritization of vulnerabilities, reporting, and remediation.

Patch management

Provides the software systems to manage and deploy security updates to the Agency's IT resources.

Policy Management Authority (PMA)

A person, application, or technology that composes or creates electronic representation of policy (based on high-level enterprise security policy). Provides the interface between technical security policy decision-makers and the enterprise protection control system. The output of a PMA is stored within a Policy Decision Point (PDP).

Policy Decision Point (PDP)

Stores policy and makes policy decisions at runtime, at the request of the Policy Enforcement Point (PEP), about what to do in a specific circumstance. PDPs are sometimes collocated within a single device with PEPs, or they may be separated.

Policy Enforcement Point (PEP)

Enforces policy at runtime, referring to the Policy Decision Point (PDP). PEPs are shared between the Control Layer and the Perimeter and Identity and Access Layers.

Event Management

Handles security-related data produced by network and system components and applies rule-based processing to find attacks, threats, and vulnerabilities. May include technologies that can store long-term event data, perform real-time analysis of events to detect problems, and respond to policy violations or attack sequences.

Audit

Ensures compliance with the Agency's security program by reviewing records of prior network traffic and activity in order to reconstruct previous attempted and/or successful intrusions or compromises. Includes forensics analysis of logs, intrusion analysis, and incident reporting.

Resource Layer

A collection of systems, applications, repositories, and content to be protected by information security measures. The resource layer contains all other technology categories in the TRM. These resources are protected at Policy Enforcement Points by “actuators” (mechanisms that conduct policy and security management) and “sensors” (components or functions within the resource that provide feedback to security management systems, audit systems and policy decision points and are typically invoked by actuators).

This page intentionally left blank.

Appendix A. References

Dan Blum, *Information Security Technology Model, Version: 1.0*, Jan 17, 2005, © 2005 Burton Group, www.burtongroup.com

Department of Commerce Technical Reference Model and Standards Profile Framework. February 6, 2001. trm_draft_rev7.wpd.

Department of Defense Technical Reference Model. Section 2. April 9, 2001

Eric Maiwald, *Vulnerability Management: Toward Technical Security Policy Management Products* v1.0, 20 May 2005, © 2005 Burton Group, www.burtongroup.com

FEA Consolidated Reference Model Document, May 2005. *http://www.whitehouse.gov/omb/egov/documents/CRM.PDF*

FEA Reference Model Mapping Quick Guide, August 2005. http://www.whitehouse.gov/omb/egov/documents/FY07_Ref_Model_Mapping_QuickGuide.pdf

Grossman, Ira and James Sargent. *An IT Enterprise Architecture Process Model*. https://secure.cio.noaa.gov/hpcc/docita/files/ita_process_paper.htm

Grossman, Ira. *Case Study: Establishing Federated Information Technology (IT) Architectures*. Department of Commerce and National Oceanic and Atmospheric Administration. July 26, 2001.

Health and Human Services Department-Wide Standards (Draft). April 26, 2000.

Karen S. Evans, *Expanding E-Government: Partnering for a Results-Oriented Government* , December 2004

Model for Information Integration (Draft), EPA Information Integration Program, February 19, 2002

The Software Productivity Consortium, *Define the Technical Architecture*. http://www.software.org/sysmigweb/framework/framework-3.asp

Technical Reference Model, Centers for Disease Control and Prevention. November 16, 2002 http://www.cdc.gov/irmo/ea/trm.htm

Attachment 1-C

This page intentionally left blank.

Appendix B. Mapping to FEA TRM

The Federal Enterprise Architecture Technical Reference Model (FEA-TRM) is a component-driven, technical framework used to categorize the standards, specifications, and technologies that support and enable the delivery of service components and capabilities.

The FEA-TRM provides a foundation to categorize the standards, specifications, and technologies to support the construction, delivery, and exchange of business and application components (Service Components) that may be used and leveraged in a Component-Based or Service-Orientated Architecture. The FEA-TRM unifies existing Agency TRMs and E-Gov guidance by providing a foundation to advance the re-use of technology and component services from a government-wide perspective.

Mapping Agency technology to the FEA-TRM is desirable since it provides a cross-agency framework for measuring investments and for inter-agency technology collaboration. The table below is an initial reference to map the FEA-TRM services to the EPA TRM major technology areas.

It is important to realize that the mapping between the FEA-TRM and the EPA TRM is not a one-to-one correlation. Rather, there are several services and sub services in the FEA-TRM that map to a single EPA TRM subcategory. Similarly, there are several EPA TRM subcategories that map to a single FEA-TRM service. The determination of what maps to what is based on the definition of the FEA service and the EPA TRM descriptions contained in this document. In cases where the definitions allowed for multiple relationships, all the relationships were mapped. In a few cases where a definitive relationship was not available based on the definition alone, the skill and experience of the Technology Architecture team and industry subject matter experts was used to propose a proper mapping.

Table B-1. Services Mapped to EPA TRM Major Technology Areas

FEDERAL EA TECHNICAL REFERENCE MODEL	EPA TRM
Service Access & Delivery	
Refers to the collection standard 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.	
Access Channels	
Access Channels define the interface between an application and its users, whether it is a browser, personal digital assistant or other medium.	
Collaboration Communications	
Define the forms of electronic exchange of messages, documents, or other information. Electronic communication provides efficiency through expedited time-of-delivery.	User Environment

FEDERAL EA TECHNICAL REFERENCE MODEL	EPA TRM
Other Electronic Channels Define the other various mediums of information exchange and interface between a user and an application.	User Environment
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.	User Environment
Wireless / PDA Technology that uses transmission via the airwaves. A 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.	User Environment
Delivery Channels Delivery channels define the level of access to applications and systems based upon the type of network used to deliver them.	
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.	Networks/Telecom Security – Identity and Access Management
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.	Networks/Telecom Security - Perimeter
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.	Security – Identity & Access Management Networks/Telecom
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.	Security - Perimeter User Environment

FEDERAL EA TECHNICAL REFERENCE MODEL	EPA TRM
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	Security - Perimeter User Environment
Service Requirements Service Requirements define the necessary aspects of an application, system or service to include legislative, performance and hosting.	
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.	Security – Identity & Access Management
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.	Hosting Platforms Security - Resource
Legislative / Compliance Defines the pre-requisites that an application, system or service must have mandated by congress or governing bodies.	-
Service Transport Service Transport defines the end-to-end management of the communications session to include the access and delivery protocols.	
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.	Networks/Telecom
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.	Networks/Telecom
Service Platform and Infrastructure The Service Platform and Infrastructure Category define the collection of platforms, hardware and infrastructure specifications that enable Component-Based Architectures and Service Component re-use.	

FEDERAL EA TECHNICAL REFERENCE MODEL	EPA TRM
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.	Data Technologies
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.	Data Technologies
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.	Hosting Platforms
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.	
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.	Application Technologies, Hosting Platforms
Media Servers Provide optimized management of media-based files such as audio and video streams and digital images.	Data Technologies, Hosting Platforms
Portal Servers Portals represent focus points for interaction, providing integration and single-source corporate information.	Application Technologies, Hosting Platforms
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.”	Application Technologies, Hosting Platforms

FEDERAL EA TECHNICAL REFERENCE MODEL	EPA TRM
Hardware / Infrastructure Defines the physical devices, facilities and standards that provide the computing and networking within and between enterprises.	
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.	User Environment
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.	Networks/Telecom
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).	Networks/Telecom
Peripherals Computer devices that are not part of the essential computer (i.e. the memory and microprocessor). Peripheral devices can be external and internal.	User Environment
Servers / Computers This refers to the various types of programmable machines which are capable of responding to sets of instructions and executing programs.	Hosting Platforms
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.	User Environment
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.	Networks/Telecom

FEDERAL EA TECHNICAL REFERENCE MODEL	EPA TRM
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.	Application Technologies
Modeling The process of representing entities, data, business logic, and capabilities for aiding in software engineering.	Application Technologies
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.	Technology Management
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.	Technology Management Security - Resource
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.	
Platform Dependent Consists of the programming languages and methods for developing software on a specific operating system or platform.	Application Technologies
Platform Independent Defines the programming languages that are able to execute and run on any platform or operating system.	Application Technologies
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.	Networks/Telecom

FEDERAL EA TECHNICAL REFERENCE MODEL	EPA TRM
Component Framework	
The Component Framework Area 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	
Business Logic	
Defines the software, protocol or method in which business rules are enforced within applications.	
Platform Dependent	
Consists of the programming languages and methods for developing software on a specific operating system or platform.	Application Technologies
Platform Independent	
Consists of all software languages that are able to execute and run on any type of operating system or platform.	Application Technologies
Data Interchange	
Data Interchange defines 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.	Data Technologies
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.	Data Technologies

FEDERAL EA TECHNICAL REFERENCE MODEL	EPA TRM
Reporting and Analysis Consist of the tools, languages and protocols used to extract data from a data store and process it into useful information.	Data Technologies
Presentation / Interface This defines the connection between the user and the software, consisting of the presentation that is physically represented on the screen.	
Content Rendering This defines the software and protocols used for transforming data for presentation in a graphical user interface.	User Environment
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.	User Environment
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.	User Environment
Wireless / Mobile / Voice Consists of the software and protocols used for wireless and voice-enabled presentation devices.	User Environment, Networks/Telecom
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.	
Certificates / Digital Signature Software used by a certification authority (CA) to issue digital certificates and secure access to information.	Security – Identity & Access Management
Supporting Security Services These consist of the different protocols and components to be used in addition to certificates and digital signatures.	Security – Identity & Access Management Security - Control

FEDERAL EA TECHNICAL REFERENCE MODEL	EPA TRM
Service Interface & Integration	
The Service Interface and Integration Area define 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.	
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.	
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.	Application Technologies
Middleware	
Middleware increases the flexibility, interoperability, and portability of existing infrastructure by linking or “gluing” two otherwise separate applications	Application Technologies
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 Description / Interface	
Defines the method for publishing the way in which web services or applications can be used.	Application Technologies
Service Discovery	
Defines the method in which applications, systems or web services are registered and discovered.	Application Technologies
Interoperability	
Interoperability defines the capabilities of discovering and sharing data and services across disparate systems and vendors.	

FEDERAL EA TECHNICAL REFERENCE MODEL	EPA TRM
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.	Data Technologies
Data Transformation Data Transformation consists of the protocols and languages that change the presentation of data within a graphical user interface or application.	Data Technologies
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.	Data Technologies

Table B-2 below groups the FEA TRM components into the seven major technology areas of the EPA TRM. Each major technology area is highlighted to show which components from the FEA TRM map to that area.

Following the table are four diagrams that respectively map the four major service areas of the FEA TRM into the EPA TRM. The components of each major FEA TRM service are shown in their relationship to the seven major technology areas of EPA's TRM.

Table B-2. EPA TRM Technology Areas Mapped to FEA TRM Services

EPA TRM - USER ENVIRONMENT			
	Service Access and Delivery	Access Channels	Collaboration Communications
			Web Browser
			PDA
			Other Electronic Channels
		Delivery Channels	VPN
			Peer to Peer
	Service Platform and Infrastructure	Hardware/Infrastructure	Embedded Technology Devices

			Peripherals
			Video Conferencing
			Servers/computers
	Component Framework	Presentation/Interface	Content rendering
			Dynamic/server-side display
			Static display
			Wireless/mobile/voice
EPA TRM - APPLICATION TECHNOLOGIES			
	Service Platform and Infrastructure	Delivery Servers	Application Servers
			Portal Servers
			Web Servers
		Supporting Platforms	Platform dependent
			Platform independent
		Software Engineering	Integrated Development Environment
			Modeling
	Component Framework	Business Logic	Platform dependent
			Platform independent
	Service Interface and Integration	Integration	Enterprise Application Integration
			Middleware
		Interface	Service description/interface
			Service discovery

EPA TRM - DATA TECHNOLOGIES			
	Service Platform and Infrastructure	Database/Storage	Database
		Delivery Servers	Media servers
	Component Framework	Data Interchange	Data exchange
		Data Management	Data connectivity
			Reporting and Analysis
	Service Interface and Integration	Interoperability	Data format/classification
			Data transformation
			Data types/validation
EPA TRM - HOSTING PLATFORMS			
	Service Access and Delivery	Service Requirements	Hosting
	Service Platform and Infrastructure	Database/Storage	Storage
		Hardware/Infrastructure	Servers/computers
		Delivery Servers	Application Servers
			Media servers
			Portal Servers
			Web Servers
EPA TRM - NETWORKS/TELECOM			
	Service Access and Delivery	Delivery Channels	Internet
			Intranet
		Service Transport	Service Transport
			Supporting Network Services

	Service Platform and Infrastructure	Hardware/Infrastructure	Wide Area Network
			Local Area Network
			Network devices/standards
		Supporting Platforms	Wireless/mobile
	Component Framework	Presentation/Interface	Wireless/mobile/voice
EPA TRM - TECHNOLOGY MANAGEMENT			
	Service Platform and Infrastructure	Software Engineering	Software configuration management
			Test management
EPA TRM - SECURITY			
	Service Access and Delivery	Delivery Channels	Extranet
			Intranet
			VPN
			Peer to Peer
		Service Requirements	Authentication/Single Sign-on
	Component Framework	Security	Certificates/digital signature
			Supporting security services
(NOT MAPPED)			
	Service Access and Delivery	Service Requirements	Legislative/Compliance

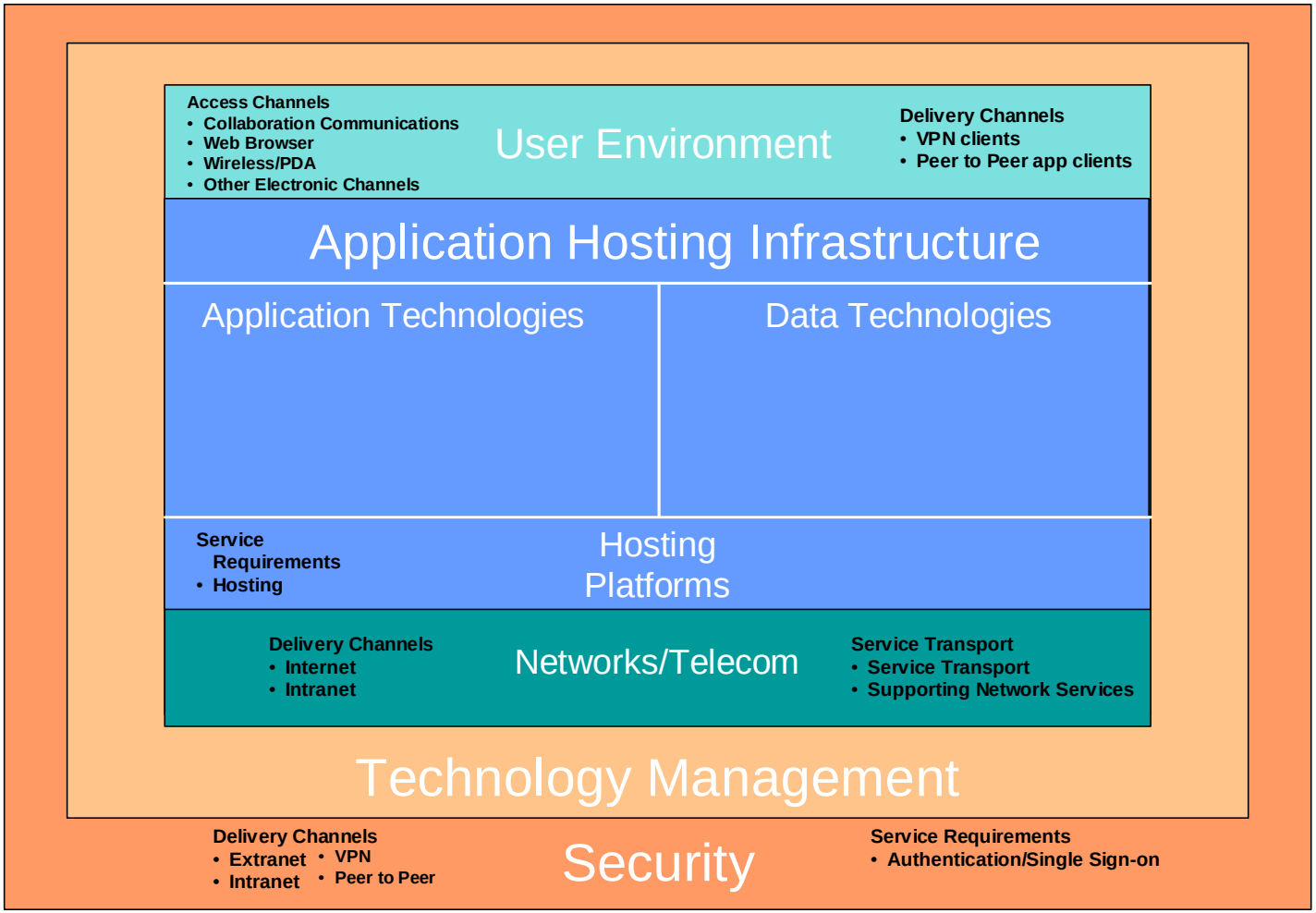

Figure B.1 EPA TRM with FEA TRM Service Access and Delivery Components

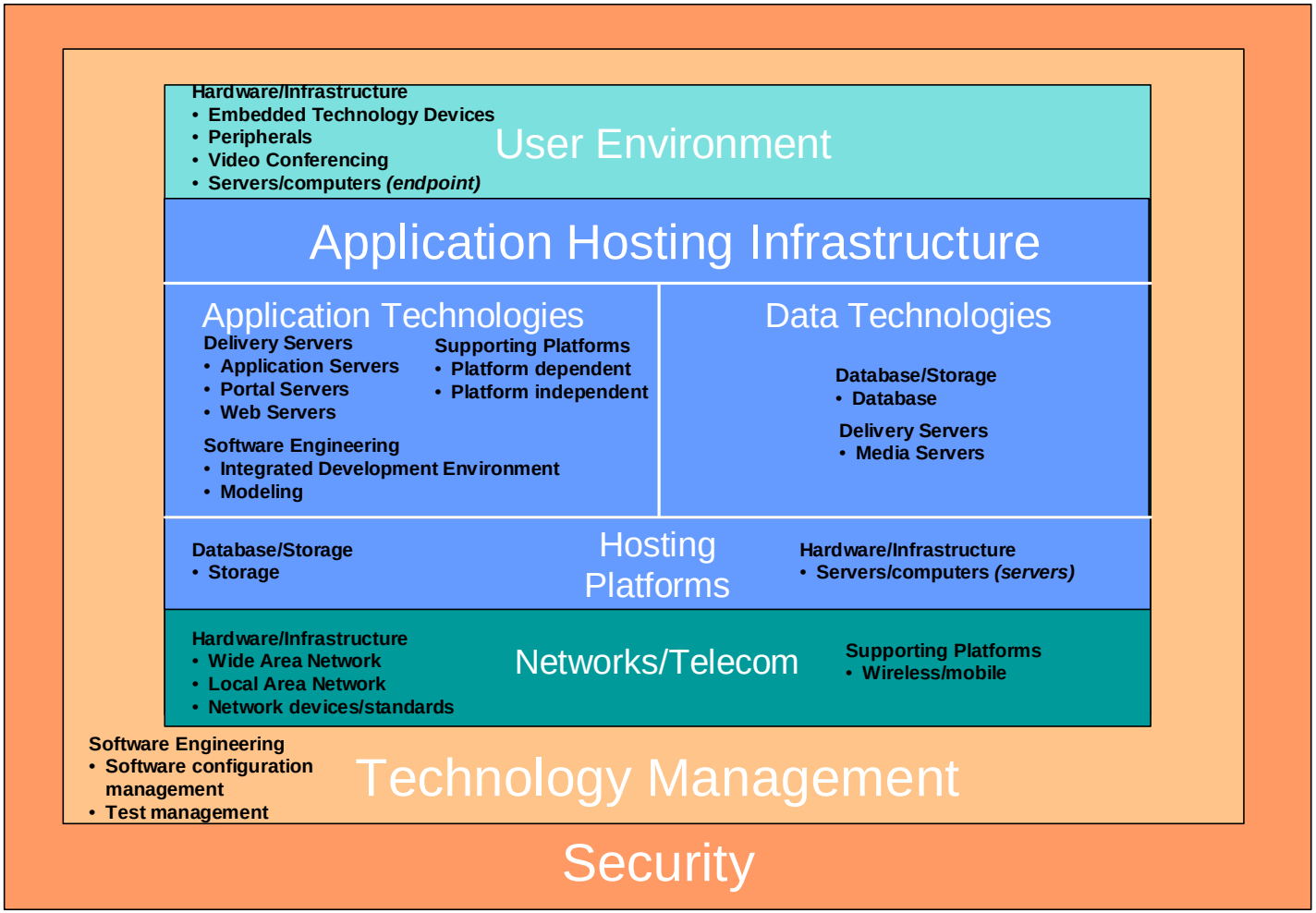

Figure B.2 EPA TRM with FEA TRM Service Platform and Infrastructure Components

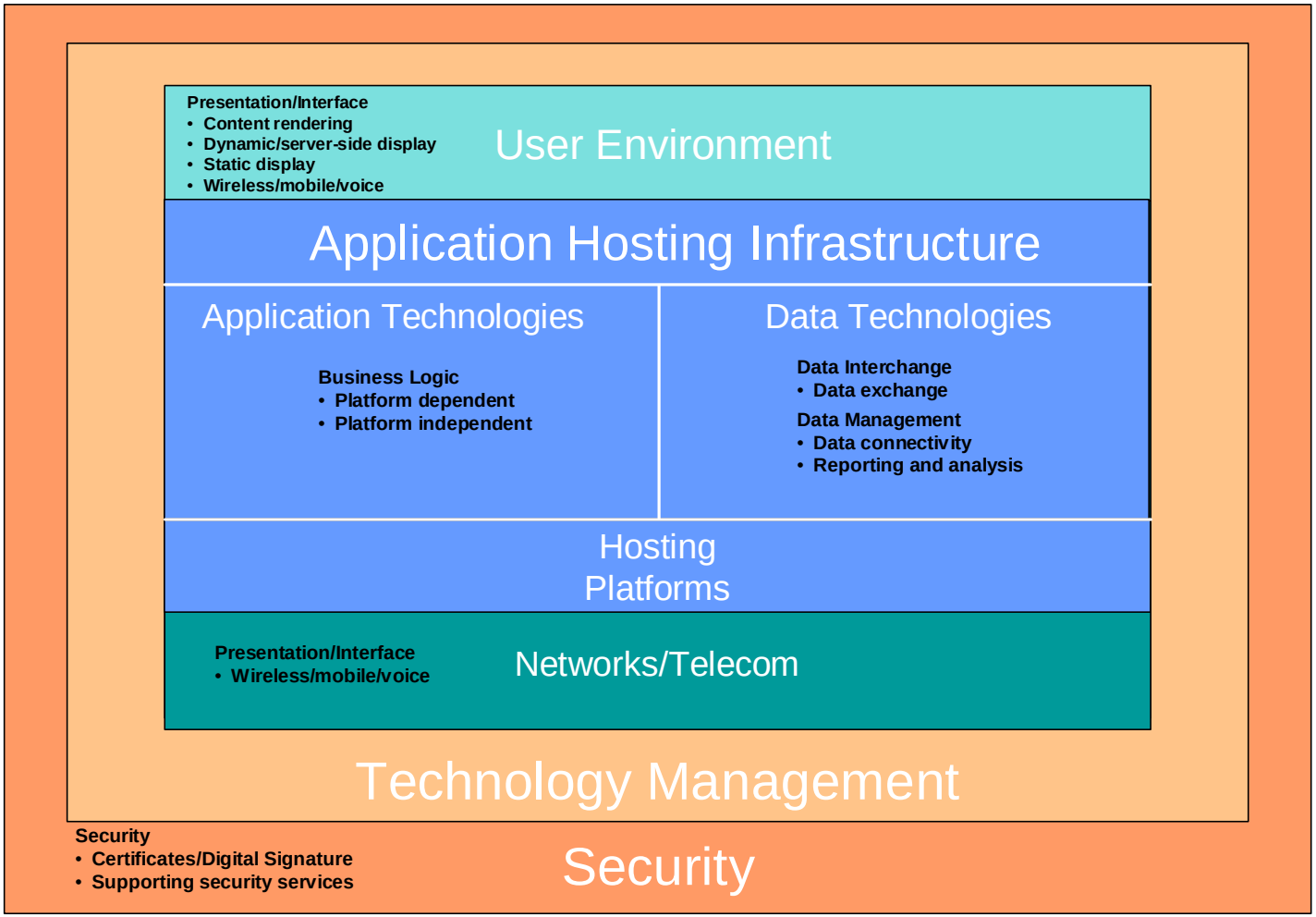

Figure B.3 EPA TRM with FEA TRM Component Framework

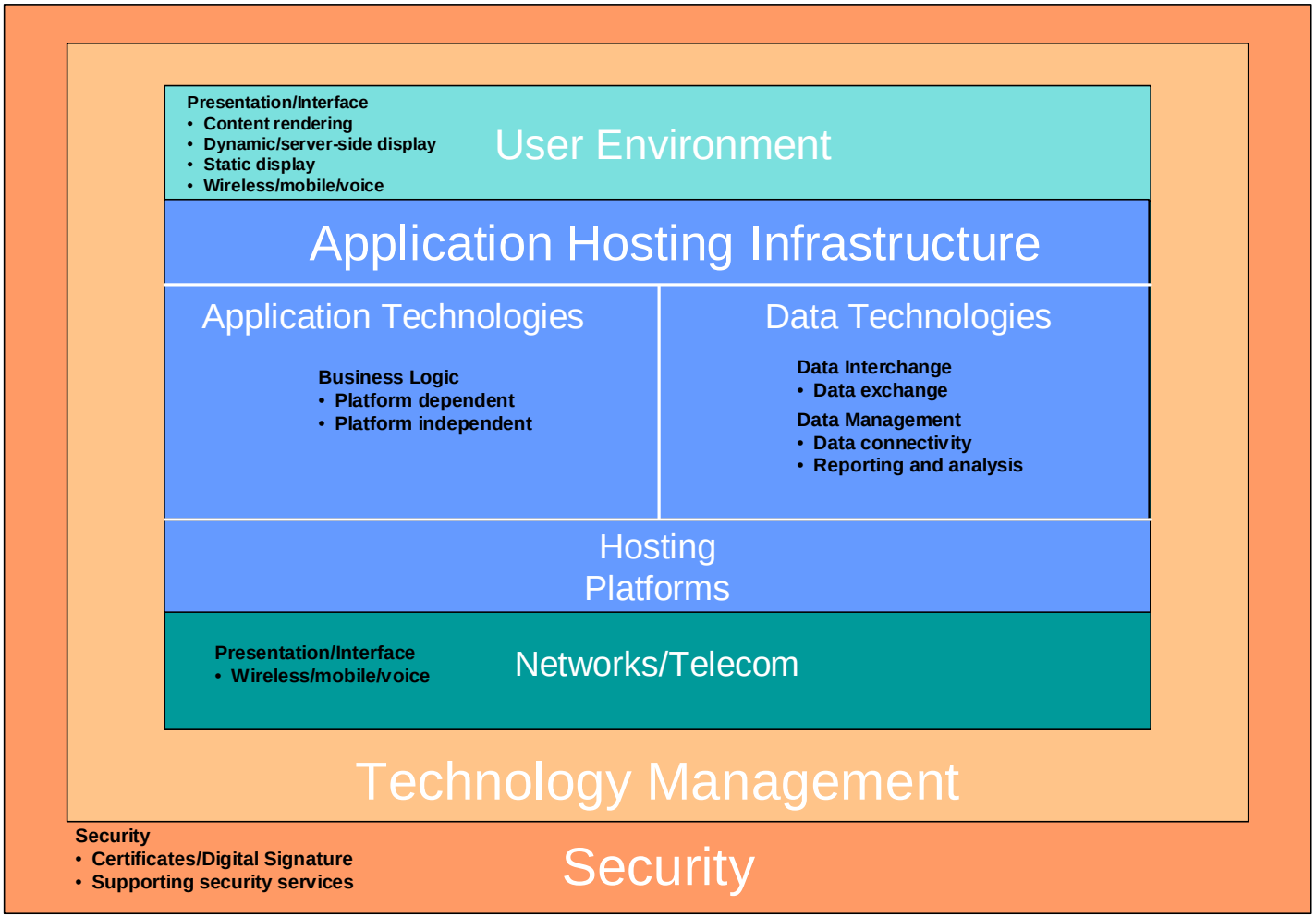

Figure B.4 EPA TRM with FEA TRM Service Inferface and Integration Components

This page intentionally left blank.

Appendix C. Standards Profile

The Standards Profile defines a set of specific technologies and products that are categorized generally in the TRM. The Standards Profile establishes the technology that achieves standardization across the enterprise and insures interoperability and secure computing. Adherence to technology standards is the first step in assuring that computers systems comply with standard configurations and security controls.

EPA's Standards Profile has been maintained since 1998 as a web-enabled database accessible through the IT Roadmap web site (http://basin.rtpnc.epa.gov/ntsd/ITRoadmap.nsf). The IT Roadmap documents EPA's information technology standards and the process for selecting and approving these standards. These technology standards allow the Agency to maintain an infrastructure with a high level of interoperability, stability, and security.

The IT Roadmap database divides EPA's product and technology standards into computer system platforms and technology categories established before the development of the Agency's TRM. Since the present TRM facilitates the profiling and grouping of technology in a new framework, a current effort underway is aligning the platforms and categories of the database with the major and minor technology categories of the TRM. Once this is completed and published, this Appendix will be updated to reflect the new framework.

The IT Roadmap kernel is the Product/Technology Matrix (PTM) database, which categorizes all major IT components considered by the Agency in seven platforms and 12 functional categories. Where specific products or technologies have not evolved sufficiently, the entry may contain a reference to a specification, rather than a product or technology. This matrix allows users to search for supported technologies by platform or technology type, and to query the database for the status of specific products or for all the products in a particular status, category, or platform.

Each product or technology in the PTM is listed with one of four status classifications used to describe the implementation level of the product/technology within the Agency. The four classifications are:

- Target: Product/technology is a future direction for the Agency in the next five years.
- Standard: Product/technology has been officially endorsed as a standard for EPA. The product has been tested for stability and integration in the Agency's computing environment. Standard products must be followed, adopted, and used to comply with Agency guidelines.
- Interim: Endorsed as a necessary Agency product/technology being considered for a standard or being used during the migration process toward a standard.
- Legacy: Product/technology previously endorsed as a Standard but has been replaced or outdated and is no longer considered for use when planning and developing new IT systems.

This page intentionally left blank.

Appendix D. Glossary of Terms

API (Application Program Interface) – A set of software components that allows a programmer to issue commands and receive results to and from an operating system or other software system, such as a Data Base Management System.

Backbone – A network segment that connects other network segments and carries high concentrations of traffic.

Bandwidth – The measurement of the capacity of a transmission medium. The terms for measurement vary from analog (hertz – cycles per second) and digital (bits per second). Common measurements include: Kbps (kilobits per second), Mbps (megabits per second), and Gbps (gigabits per second).

Bit/byte – A bit is the smallest unit of data in a computer. Computers usually store data and execute instructions in multiples of bits, called bytes. In most computer systems, there are eight bits in a byte (which generally represents a single letter or character, or four bytes to a word). A byte is abbreviated with a capital "B" and a bit is abbreviated with a small "b".

CPIC (**Capital Planning and Investment Control)** – A process to structure budget formulation and execution and to ensure that investments consistently support the strategic goals of the Agency.

CASE (Computer Aided Software Engineering) – Software tools used by programmers to assist with the task of programming, typically by translating pseudo code into a computer language, providing structure to the programming process, and providing for re-use of code.

Client/server – The relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request. Although the client/server concept can be used by programs within a single computer, it is a more often deployed in a networked environment. In a network, the client/server model provides a convenient way to service many different end users with a single program and database system. Computer transactions using the client/server model are very common.

Typically, multiple client programs share the services of a common server program. Both client programs and server programs are often part of a larger program or application. Relative to the Internet, your Web browser is a client program that requests services (the sending of Web pages or files) from a Web server (which technically is called a Hypertext Transport Protocol or HTTP server) in another computer somewhere on the Internet. Similarly, your computer with TCP/IP installed allows you to make client requests for files from File Transfer Protocol (FTP) servers in other computers on the Internet. Lotus Notes is another example of a client/server application that uses a specific TCP/IP port. Lotus Development Corporation registered the port they wished to use with the InterNIC so only they could use that port for their applications on the Internet. Many client/server vendors have followed suit and registered their ports.

Other client/server models included master/slave, with one program being in charge of all other programs, and peer-to-peer, with either of two programs able to initiate a transaction.

DBMS (Data Base Management System) – A complex set of programs that control the organization, storage, and retrieval of data for many users; extensively used in business environments. Data is organized in fields, records, and files. A database management system

must also control the access to the database. Examples of database management systems are Oracle, Sybase, and Datacom.

Desktop Computer – A personal computer that is designed to fit conveniently on top of a typical office desk. A desktop computer typically comes in several units that are connected together during installation: (1) the processor box which is designed to fit under the desk or in a unit that goes on top of the desk, (2) the display monitor, and (3) input/output devices - usually tactile such as keyboard and a mouse (pointing device). Today, almost all desktop computers include a built-in modem or Ethernet Network Interface Card (NIC), a CD-ROM drive, a multi-gigabyte magnetic storage drive, and speakers. At home, most desktop computer users also purchase a printer. In businesses and increasingly at home, desktop computers are interconnected and can share resources such as printers by being connected to a local area network (LAN).

Domain Naming Service (DNS) – A lookup service needed for most networks that translate a computer name into an IP address.

Enterprise Application Integration (EAI) – A process to link stove-piped applications so that they provide enterprise-wide processing.

Enterprise Technology Architecture (ETA) – A comprehensive blueprint of an organization's information technology that includes five components: 1) TRM, 2) Standards Profile, 3) Baseline Architecture, 4) Target Architecture, 5) Sequencing Plan. The ETA provides explicit descriptions of the current and desired state of the information technology resource of an organization.

Extranet – A private network that uses the Internet protocols 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 the part of a company's Intranet that is extended to users outside the company.

An Extranet requires security and privacy controls such as firewall server management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages, and the use of virtual private networks (VPN) that tunnel (encapsulate data) through the public network.

Companies can use an Extranet to:

- Exchange large volumes of data electronically
- Share product catalogs exclusively with wholesalers or those "in the trade"
- Collaborate with other companies on joint development efforts
- Jointly develop and use training programs with other companies
- Provide or access services provided by one company to a group of other companies, such as an online banking application managed by one company on behalf of affiliated banks
- Share news of common interest exclusively with partner companies

Oracle and Sun Microsystems have announced an alliance to ensure that their Extranet products can work together by standardizing on JavaScript and the Common Object Request Broker Architecture (CORBA). Microsoft supports the Point-to-Point Tunneling Protocol (PPTP) as a VPN. The IBM Lotus Corporation is promoting its groupware product, Notes, as well-suited for Extranet use.

Firewall – A set of related programs, located at a network gateway server or switch, which protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an Intranet connection that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users may access.

Basically, a firewall, working closely with a router program, filters all network packets to determine whether to forward them toward their destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain names and IP addresses. For mobile users, firewalls allow remote access in to the private network by the use of secure login procedures and authentication certificates.

FTP (File Transfer Protocol) – A protocol used for transferring files from one computer to another over a TCP/IP network (including the Internet).

Gateway – Electronic repeater devices that intercept and steer electrical signals from one network to another. A gateway is an entrance into, and exit out of, a communications network.

High Performance Computer (HPC) – see Supercomputer.

HTTP (Hypertext Transfer Protocol) – The protocol most often used to transfer information from World Wide Web servers to browsers, which is why Web addresses begin with http://.

HTTPS (Hypertext Transfer Protocol-Secure) – HyperText Transmission Protocol, Secure. HTTP for secure transactions over the Internet.

Identity Management – A security strategy built on a foundation of the enterprise directory (information catalog for users and systems), branching out to permissions, policy management, and authentication. Identity management ensures security, increases productivity and reduces operating costs in an environment requiring a constant, rapid flow of information within and across company networks between users and systems and between systems.

Internet – Sometimes called “the Net,” or “World Wide Web”. It is a worldwide system of interconnected computer networks - running TCP/IP and DNS to find message destinations. It was conceived by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first known as the ARPANET. The original aim was to create a network that would allow users of a research computer at one university to be able to “talk to” research computers at other universities. A side benefit of ARPANET’s design was that, because messages could be routed or rerouted in more than one direction, the network could continue to function even if parts of it were destroyed in the event of a military attack or other disaster.

The Internet is now the logical and physical network that connects computer users around the world.

Interoperability – The ability of software on different computers to communicate with each other and transfer data.

Intranet – A private network based on the Internet that is contained within the security of an enterprise. It may consist of many interlinked local area networks and use leased lines in the wide area network. Typically, an Intranet includes connections through one or more gateway

computers to the outside Internet. The main purpose of an Intranet is to share company information and computing resources among employees. An Intranet can also be used to facilitate working in groups and for teleconferences.

An Intranet uses TCP/IP, HTTP, UDP and other Internet protocols and in general looks like a private version of the Internet. With tunneling, companies can send private messages through the public network, using the public network with special encryption/decryption and other security safeguards to connect one part of their Intranet to another.

Typically, larger enterprises allow users within their Intranet to access the public Internet through firewall servers that have the ability to screen messages in both directions so that company security is maintained. When part of an Intranet is made accessible to customers, partners, suppliers, or others outside the company, that part becomes an Extranet.

IP (Internetworking Protocol) – A protocol that uses datagrams, or data packets, for sending data through networks. Data are encapsulated in packets that contain routing and identity information, so that the network knows where the data comes from and where it is supposed to go. Version 4 is currently the standard IP protocol. IPv6 will be adopted in the future.

IPSEC (IP Security protocol) – A standard for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the application layer of the communications model. IPSEC will be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. Security arrangements can be handled without requiring changes to individual user computers. Cisco includes support for IPSEC in its network routers.

IPX/SPX (Internet Packet Exchange/Sequenced Packet Exchange) – A Novell network communications protocol used by NetWare clients and servers to deliver messages within and between networks. SPX ensures reliable delivery of complete messages.

ISDN (Integrated Services Digital Network) – A digital network standard that supports voice, data, and video over a single telephone line. Basic rate interface (BRI) constitutes two 64 Kbps channels, while primary rate interface (PRI) uses 24 64 Kbps channels.

ISP (Internet Service Provider) – An organization that typically offers Email, Internet access, Web hosting services, and high-speed circuits to customers needing access to the Internet.

Local Area Network (**LAN**) – A network of interconnected workstations sharing resources within a relatively small geographic area such as a building or the floor of a building. A local area network may serve as few as two users or may serve several hundred. Typically, the number of users served is less than 200.

Local Area Network Server – Usually, a computer that has applications and data storage shared in common by multiple end users. The server provides localized hosting services to groups of users connected to an office LAN. These services (see Figure 4.1) include Hosting (file & print services, mass storage, e-mail), communications (pathway that connects the WAN Router to the Desktop), Applications & Data (for locally hosted applications & data bases), Technology Management (by the local System Administrators), and Security (such as local Bindview & Easy Service Monitoring). There are also Local Area Network servers used on laboratory and research LANs. These servers support real-time data acquisition processes and the specific computational needs of Laboratory instrumentation, data collection and storage. Laboratory Local Area Network servers are generally not connected to the WAN.

Mainframe - An industry term for a large computer, typically manufactured for running applications with large-scale computing purposes. Historically, a mainframe is associated with

centralized rather than distributed computing. Today, IBM refers to its large computers as servers, and the mainframe is often referred to as the Enterprise Server.

Metropolitan Area Network (MAN) – A network that serves a metropolitan area. This service provides the communication facility that allows buildings collocated in a campus or metropolitan area to be interconnected without having to exit internal network hardware. This facility usually makes use of high-bandwidth fiber optic channels to allow high-speed communication between Server/Hosts and between Server/Hosts and data storage networks.

Modem – Modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional copper twisted-pair telephone line and demodulates the incoming analog signal and converts it to a digital signal for the digital device. From early 1998, most new personal computers came with 56 Kbps modems though currently they are standard only in mobile computers.

Network Interface Card (NIC) – A network adapter that connects a personal computer to a local area network.

Personal Digital Assistant (PDA) – A pocket-sized personal computer. PDAs usually can store phone numbers, appointments, and to-do lists. Some PDAs have a small keyboard; others have only a special pen that is used for input and output. A PDA can also have a wireless fax modem.

Portability – The ease of transfer from one system to another; ease of use with a variety of platforms without modification. The term usually refers to software or data.

PSN (Public Switched Network) – The telecommunications network that supports normal dial-up telephone service.

Remote Access – The ability to access a computer or network from a remote location. In corporations, people at branch offices, telecommuters, and people who are traveling may need access to the corporation's network. Home users get access to the Internet through remote access to an Internet service provider (ISP). Dial-up connection through desktop, notebook, or handheld computer modems over regular telephone lines is a common method of remote access. Remote access is also possible using a dedicated line between a computer or a remote local area network and the "central" or main corporate local area network. A dedicated line is more expensive and less flexible but offers faster data rates. ISDN is a common method of remote access from branch offices since it combines dial-up with faster data rates. Wireless, cable modem, and DSL technologies offer other possibilities for remote access.

A remote access server is the computer and associated software that is set up to handle users seeking access to network remotely. Sometimes called a communication server, a remote access server usually includes or is associated with a firewall server to ensure security and a router that can forward the remote access request to another part of the corporate network. A remote access server may include or work with a modem pool manager so that a small group of modems can be shared among a large number of intermittently present remote access users.

Router – On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks to which it is connected. A router is located at any juncture of networks or gateway, including each Internet point-of-presence. A router is often included as part of a network switch.

A router creates or maintains a table of the available routes and their conditions and uses this information along with distance and cost algorithms to determine the best route for a given

packet. Typically, a packet may travel through a number of network points with routers before arriving at its destination. An edge router is a router that interfaces with an asynchronous transfer mode (ATM) network. A brouter is a network bridge combined with a router.

Scalability – The ability to easily change in size or configuration to suit changing conditions. For example, a company that plans to set up a client/server network may want to have a system that not only works with the number of people who will immediately use the system, but the number who may be using it in one year, five years, or ten years.

Server – 1) In general, a server is a computer program that is a "listener program" for other computer programs in the same or other computers. 2) The computer that runs a server program is also frequently referred to as a server (though it may contain a number of server and client programs). 3) In the client/server programming model, a server is a program that awaits and fulfills requests from client programs in the same or other computers. A given application in a computer may function as a client with requests for services from other programs and a server of requests from other programs.

Specific to the Internet, a Web server is the computer program that serves out requested HTML pages or files. A Web client or Web browser is the requesting program associated with the user that requests HTML files from Web servers.

Server Farm – A group of servers that collectively provide the services of a single server such as web server, terminal server or Instant Messaging Server.

Service-Oriented Architecture (SOA) – An IT architecture strategy for business solution (and infrastructure solution) delivery based on the concept of service-orientation and the use of services to support the requirements of software users. The architecture is a collection of services that communicate with each other, are self-contained, do not depend on the context or state of the other service, and work within a distributed systems architecture. In an SOA environment, applications make resources available to other participants as independent services that the participants access in a standardized way across a network.

Storage Area Network (SAN) – A high-speed network that connects multiple storage devices so that they may be accessed on all servers in a Local Area Network (LAN) or Wide Area Network (WAN).

Supercomputer – A supercomputer is a computer that performs at or near the currently highest computational speed for computers. A supercomputer is typically used for scientific and engineering applications that must handle very large databases or do a great amount of scientific computation (or both) very quickly. At any given time, there are usually a few well-publicized supercomputers that operate at the very latest and always incredible speeds. The term is also sometimes applied to far slower (but still impressively fast) computers. Most supercomputers are really multiple computers that perform parallel processing. In general, there are two parallel processing approaches: symmetric multiprocessing (SMP) and massively parallel processing (MPP).

Technology Architecture – The framework of IT hardware and software components that enable an organization to meet its information processing needs, i.e., process, store, and exchange data with internal and external entities; and the relationship and connectivity between the components.

Transmission Control Protocol/ Internet Protocol (TCP/IP) – The Transmission Control Protocol (TCP) on top of the Internet Protocol (IP). These protocols were developed by DARPA to enable communication between different types of computers and computer networks. The

Internet Protocol is a connectionless protocol that provides packet routing. TCP is connection-oriented and provides reliable communication and multiplexing.

Virtual Private Network (VPN) – A VPN is a secure, private network that is configured within a public network. VPNs provide the security of a private network through the use of access controls and encryption technologies, while using the built-in management facilities of a large public network.

Voice-over-Internet Protocol (VoIP) – The technology used to transmit voice conversations over a data network using the Internet Protocol. Such data network may be the Internet or a corporate Intranet.

Webinars – A Webinar is a seminar that is conducted over the World Wide Web. In contrast to a Webcast, which is transmission of information in one direction only, a webinar is designed to be interactive between the presenter and audience. A webinar is "live" in the sense that information is conveyed according to an agenda that allows for questions and answers in an interactive mode.

Wide Area Network (WAN) – A geographically dispersed telecommunications network that is a broader telecommunication structure than a local area network (LAN). A WAN may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks.

Wireless – A radio-frequency technology that allows laptop or handheld computer users in the vicinity of a "hotspot", or Wireless Access Point (WAP), to access the local area network or the Internet. Also available in Metropolitan Area Network access configurations.