HLS GEOSPATIAL ENTERPRISE ARCHITECTURE

ATTACHMENT G TECH 1
GEOSPATIAL TECHNICAL REFERENCE MODEL

GEOSPATIAL MANAGEMENT OFFICE

DRAFT VERSION 0.6.1

June 18, 2004

CONTENTS

ATTACHMENT A—DHS STANDARDS PROFILE

EXHIBITS

1.0 INTRODUCTION

The Homeland Security (HLS) Technical Reference Model (TRM) for the Department of Homeland Security (DHS) provides a common conceptual framework that will assist in effectively and efficiently coordinating the acquisition, creation, development, operation, and recapitalization of Information Technology (IT)-based systems within the DHS enterprise.

********** Important Note **********

The Geospatial Enterprise Architecture (GEA) version of the TRM emphasizes the role of Geospatial Information Technology (GIT) in the HLS Technical Architecture. It extends version 1.0 of the DHS EA TRM (DTCGHS-03-A-FLC035-001-0009A, published August 29, 2003). This version also reflects some recent enhancements to the DHS EA, which will appear in version 2.0 of the TRM.

The role of geospatial technology is highlighted in shaded text boxes throughout this version of the TRM, as illustrated here. Although not highlighted, most of the cross-cutting general purpose technology described herein also applies.

1.1 Background

The *Clinger-Cohen Act of 1996* (PL.104-106) established the Chief Information Officer (CIO) role in Federal government agencies in order to improve government performance through the effective application of information technology. Among other responsibilities, each CIO is charged with "developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture." This statement has evolved since then—Office of Management and Budget OMB Circular A-130, *Management of Federal Information Resources* uses "architecture" in its reference to an integrated Enterprise Architecture (EA), as follows:

> **Policy**
>
> The EA must also include a TRM and Standards Profile.
>
> (i) The TRM identifies and describes the information services (such as database, communications, intranet, etc.) used throughout the agency.
>
> (ii) The Standards Profile defines the set of IT standards that support the services articulated in the TRM. Agencies are expected to adopt standards necessary to support the entire EA, which must be enforced consistently throughout the agency.
>
> (iii) As part of the Standards Profile, agencies must create a Security Standards Profile that is specific to the security services specified in the EA and covers such services as identification, authentication, and non-repudiation; audit trail creation and analysis; access controls; cryptography management; virus protection; fraud prevention; detection and mitigation; and intrusion prevention and detection.

Under the DHS CIO, the Geospatial Information Officer (GIO) and the Geospatial Management Office (GMO) are responsible for defining the role of geospatial data and technology within the HLS EA.

1.2 Scope

The HLS TRM provides a common structure and vocabulary for describing all DHS information systems at all organizational levels and in all environments. This includes mission-focused systems as well as broad-use business ("back office") systems, shared application services, and infrastructure systems and components. This TRM covers all IT elements necessary to build or procure hardware, services, or applications described by IT project Exhibit 300s.

1.3 Purpose

As a key element of the DHS EA, the TRM establishes the basic guidance necessary to help ensure that proposed IT solutions are in compliance with the intent of the EA. Specifically, the TRM is intended to describe elements of proposed solutions using a standard vocabulary and categorization scheme to allow them to be compared to identify overlaps and gaps. While adherence to this TRM in those terms is mandatory, individual organizational elements of DHS may extend and refine the TRM where necessary. Extensions and refinements must be registered with and approved by the DHS CIO before use.

1.4 Goals

Establishing and institutionalizing a comprehensive TRM, and the associated standards profiles, will provide the guidance and direction DHS needs to function as an integrated enterprise capable of accomplishing all of the missions for which it is, or will be, responsible. The goals of the TRM and DHS standards profiles are as follows:

- Promote vendor independence through the use of standards-based products and interchangeable services and components,
- Improve interoperability, reuse, and information sharing across operational entities,
- Improve operational effectiveness and efficiency through the use of common concepts and tools,
- Improve security through the identification of common security services and standards,
- Improve development and integration efficiency and responsiveness through the identification of a common infrastructure for applications, and
- Improve development and integration quality through implementation of a Department-wide systems-assurance program.

1.5 Audience

This TRM is intended for use by IT managers, procurement officials, program and project sponsors, technical and systems architects, software developers and maintainers, IT operations management and staff, security personnel, the DHS enterprise infrastructure staff, systems integrators, vendors, and service providers. Strategic Planners, Investment Managers, and enterprise architects will also use it to guide the planning process, and to guide the creation and evolution of enterprise technical and systems architectures.

1.6 Intended Uses

The HLS TRM is intended to support three principal uses in conjunction with standards profiles:

- Ensuring interoperability among DHS systems and with external systems and users,

- Guiding the design of system and technical architectures, and
- Providing the basis for assessing architectural compliance for technical solutions.

Interoperability is the primary concern at the departmental level. The HLS TRM incorporates the elements of the Federal EA (FEA) TRM to ensure interoperability with Service Components supplied by organizations external to DHS as well as with external and internal users of DHS provided Service Components.

The HLS TRM provides a technology-focused, vendor-independent view of the hardware and software services that will support the enterprise. It is intended to be used by systems architects, engineers, developers, vendors, service providers, and others involved in defining and creating new systems and modifying existing systems. This view identifies the technical services and capabilities provided by the common DHS IT infrastructure that system and application architects and engineers must consider when defining new systems or modifying existing systems.

For the DHS boards involved in making IT investment recommendations and decisions, the TRM provides a framework for considering the impact of proposed solutions on the enterprise. It does this by providing a normative model for describing the structure and relationships among technology components.

1.7 Standards Profile

The implementation of a TRM is accomplished through definition of a Standards Profile. The initial DHS Standards Profile corresponding to this TRM is attached as Appendix A.

1.8 Relationship to the FEA Service Component Reference Model (SRM)

The HLS TRM must be viewed within the context of the FEA SRM. The functionally-oriented capabilities described in the SRM in terms of "Service Components" are enabled by technical services organized as described in the FEA TRM and this document. It is assumed that, as the FEA SRM matures and a DHS-specific SRM is developed, this TRM will change in response.

1.9 Approach

The conceptual structure and taxonomy used in this TRM reflect an evolving and maturing notion of the TRM and its intended uses and builds on work performed within the Federal government and commercial industry. It draws from foundational concepts established in the *Open Systems Interconnection (OSI) Seven Layer Reference Model, The Institute of Electrical & Electronics Engineers (IEEE) Guide to the POSIX Open Systems Environment (OSE)*, the Society of Automotive Engineers (SAE) *Generic Open Architecture (GOA) Model*, and the Open GIS Consortium's (OGC) *OpenGIS® Reference Model*. It also reflects various multi-tier reference models and architectural styles promoted by industry, as well as existing models being used by various government entities. The principal sources used in the development of this TRM were those of the Transportation Security Agency (TSA), U.S. Coast Guard (USCG), U.S. Customs, Federal Emergency Management Agency (FEMA), U.S. Secret Service (USSS), and the Immigration and Naturalization Service (INS).

1.10 Relationships to Other TRMs

This TRM responds to and satisfies the intent of the FEA TRM and System Component Reference Model.

1.11 Document Organization

This document describes the motivation and context for the HLS TRM, provides a high-level overview of how it relates to and differs from the FEA TRM, and finally, presents the TRM taxonomy through the use of a hierarchical structure keyed to the FEA TRM. See Exhibit 1 for the document structure.

Exhibit 1: TRM Document Organization

Section	Purpose
Section 1 Introduction	Provides the context for discussing the TRM
Section 2 TRM Overview	Provides an overview and walkthrough of the TRM
Section 3 TRM Description	The hierarchy of services that make up the TRM and their definitions.
Attachment A DHS Standards Profile	Describes the current set of standards (including a limited set of products) applicable to DHS IT systems.
Attachment B Acronyms	List of acronyms and abbreviations used in this document
Attachment C Glossary	Glossary of terms used in this document
Attachment D References	References used in preparing this document

1.12 Control

This document and the accompanying Standards Profile are under the authority and control of the DHS CIO.

2.0 TRM OVERVIEW

The HLS TRM is an integral part of a document set that is intended to describe the DHS EA. It presents a particular architectural view that is concerned with defining the basic technical elements that compose the broader architecture and the fundamental relationships among those elements. The HLS TRM is described in this document using two different "models." The first is visual, a diagram that presents the highest-level partitioning of the technical elements of the target ("To-Be") DHS technical environment, provided in Section 2.3. The second is a hierarchically organized set of service names and associated definitions that form a taxonomy for presenting and discussing technical components in a consistent manner across the DHS.

2.1 Design Drivers

The TRM focuses on the To-Be architecture, but nonetheless provides a normative model, describing current and planned IT applications and systems in terms of their technical components. While the HLS TRM is product-neutral, it does assume a particular architectural style and uses that as a key classification principle.

2.2 Terminology

The following terms and intended usage are presented to aid the reader. Their relationships are described in Section 2.3.

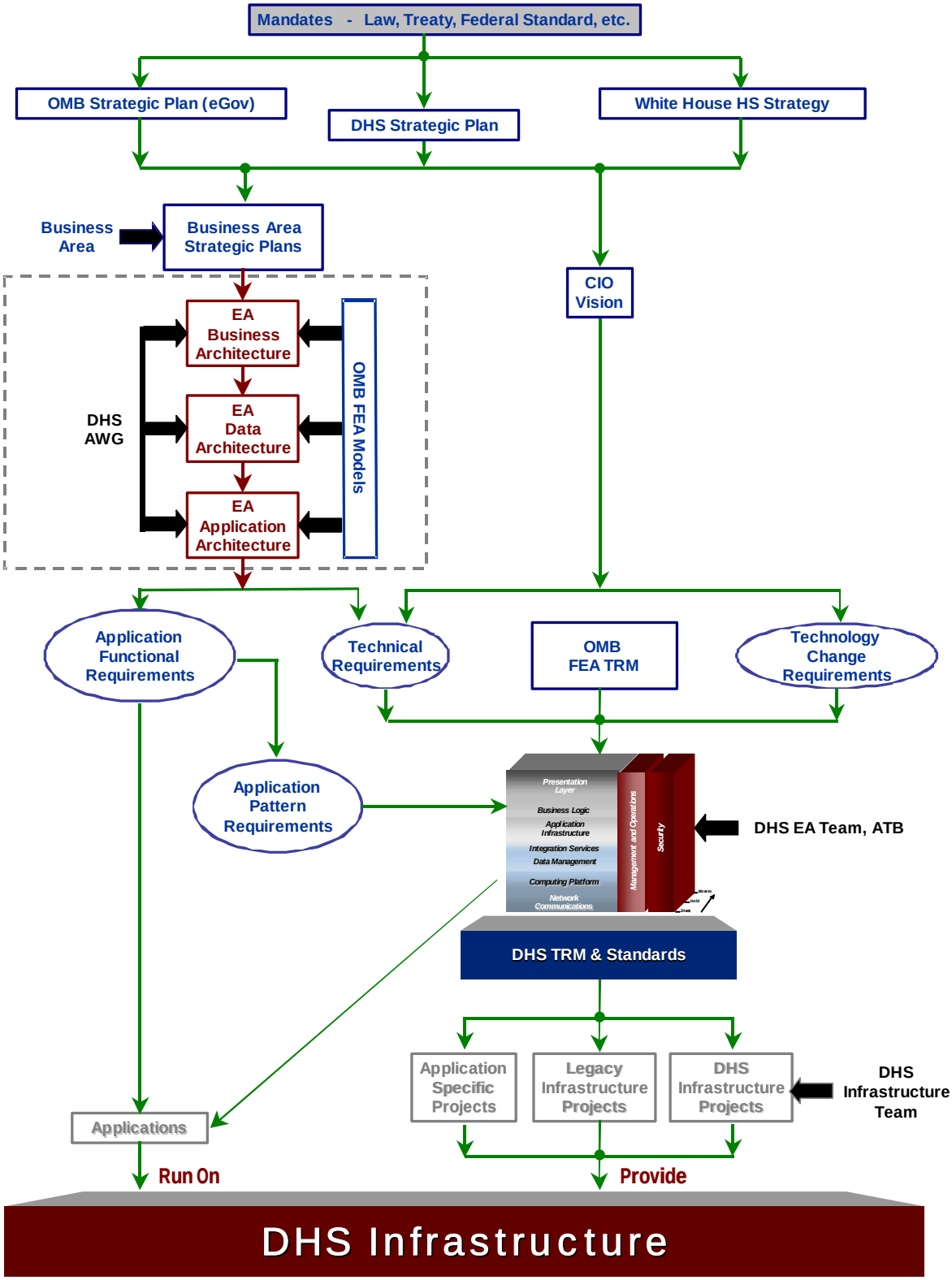
- **Application**—an automated business process or portion thereof. It is composed of components unique to the application as well as shared components.
- **Business Logic**—the portion of an application that is concerned with the encoding of business rules specific to the application**.**
- **Channel**—a mode of application access and delivery consisting of an end-point device, interface software, and a communications path to the application logic. An example is a Web browser executing on a Personal Digital Assistant (PDA) using a wireless protocol to access application on the Internet.
- **Data Store**—a logical data "container." An implementation of a data store may be a relational Database Management System (DBMS), a spatial data store (for geographic information system support), an indexed file system, a flat file system, an associative data store, or any other viable storage model.
- **End-user Device**—any device and associated operating system or other run-time software that is used to connect an end-user with an application. Examples are PDAs, cellular phones, printers, plotters, and desktop and laptop computers.
- **End-user**—a human interacting with a computer-based application.
- **Infrastructure Services**—software components that provide common-use functionality to applications and/or to other services and are application-neutral; that is the services can and are expected to be used by any arbitrary application. Examples are a Web portal and an application server.
- **Service Component**—as defined by the FEA Service Component Reference Model (SRM), a *service component* is the most granular level of the SRM framework. Service components are combined to provide specific business services organized by *service type* and *service layer* in the SRM. Examples are Data Access Services and Directory Services.
- **Service Framework**—a specific configuration of technical services, protocols, and interfaces grouped by similar functionality into conceptual layers.
- **Service Platforms**—application-neutral computing, storage, and communications devices and software that provide the technical environment required by the Service Framework. These are the computers, operating systems, storage subsystems, and networks that comprise the physical level of the DHS IT infrastructure.
- **Technical Component**—in contrast to the functional capability provided by a *service component,* a technical component is the software or hardware implementation of a specific technical function. A technical component may be custom developed or acquired from a vendor, through open source channels, or from other appropriate sources.
- **Technical Service**—in this document, a technical service is a technical component that provides functionality to applications and other technical services through well-defined and published interfaces.

The key terms used in defining the role of geospatial technology in the HLS enterprise are found in the *Geospatial Business Language* (see HLS Geospatial Business Language: Key Terms, Attachment G.Bus.1.) These terms form the basis for a consistent, common language, a *lingua franca*, for describing the role of geospatial in HLS Business Activities. The geospatial semantics of the HLS mission are embodied in these terms (concepts), and thus they form a basis for the HLS business ontology.

2.3 The HLS TRM in Context

The HLS TRM both reflects the intent of the FEA TRM and provides the specificity needed for Directorate and Organizational Element implementation. Exhibit 2 illustrates the context of the HLS TRM and its relationship to the FEA Model.

Exhibit 2: HLS TRM in Context

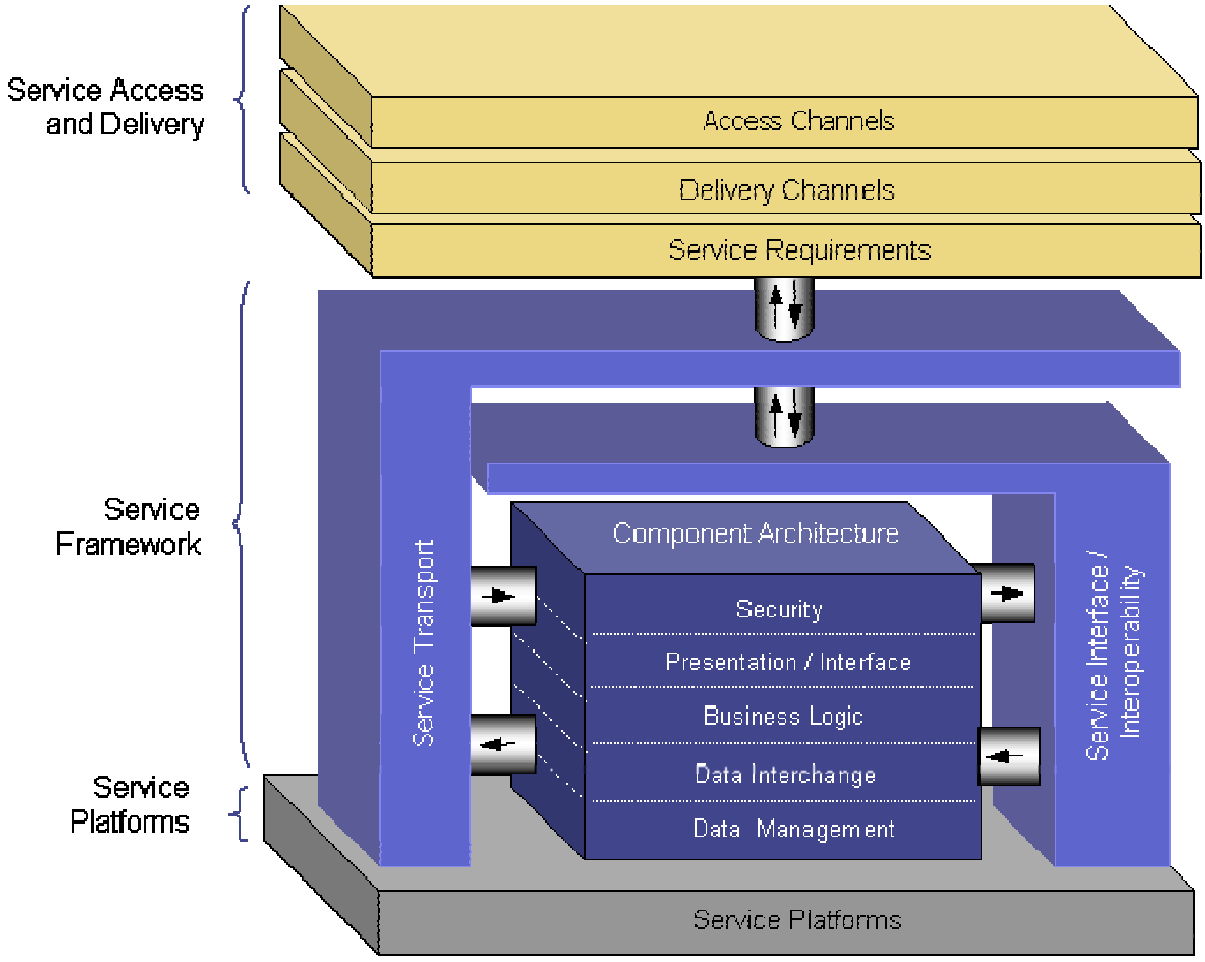


The HLS TRM incorporates the taxonomy as well as the technical services, protocols, and interfaces specified in the FEA TRM. This ensures interoperability across agencies for service components provided and consumed by DHS. The HLS TRM extends and refines the FEA TRM where necessary to satisfy "local" DHS needs for additional functionality and to ensure interoperability across DHS. DHS Directorates and Organizational Elements may, with approval, further extend the HLS TRM to satisfy their own local and unique needs.

2.3.1 FEA TRM View

The FEA TRM provides a view of technical services, protocols and interfaces that are primarily concerned with supporting the implementation of *Service Components*, as defined in the FEA SRM. This section presents a discussion of the FEA TRM in terms of how it provides context and has been incorporated into the HLS TRM (see Exhibit 3).

Exhibit 3: FEA TRM



2.3.1.1 Service Access and Delivery

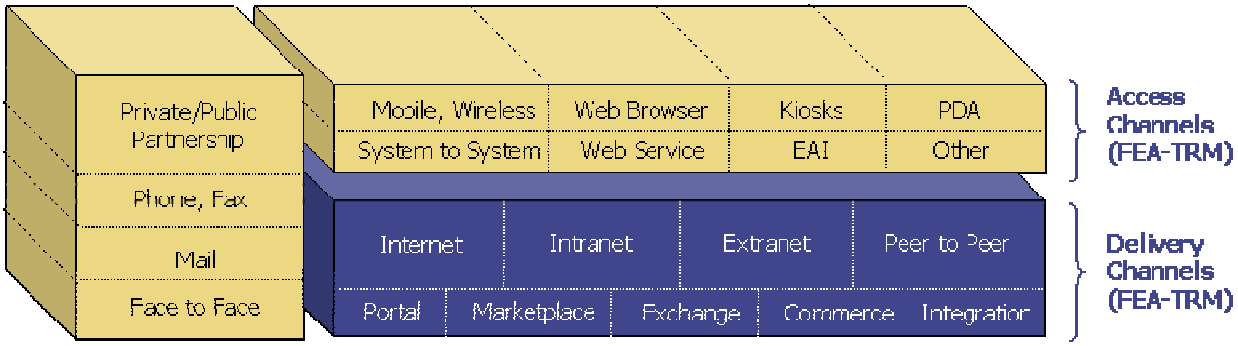
The *Service Access and Delivery Tier* of the FEA TRM is viewed as an instance of the logical subset of the components that make up the HLS TRM. The use of the channel abstraction is viewed as an architectural driver rather than a structural component. Therefore, the HLS TRM

does not specifically include the notion of channels as part of its taxonomy. The definition of any specific channel will include:

- An end-point device consisting of hardware and a browser or other client software,
- A communications path incorporating a specific logical network or other communications mechanism, and
- An appropriate set of transport protocols.

Exhibit 4, extracted from the "Agency Briefing" that presented the Draft SRM and TRM[1], identifies possible components of access and a delivery channels.

Exhibit 4: Access and Delivery Channels



2.3.1.2 Service Framework and Service Platforms

The Service Framework tier of the FEA TRM, together with the Service Platforms tier, reflect a more traditional view of a TRM; one that is more familiar to the technologists who will design the systems and components that implement its architectural direction.

2.3.2 DHS View

The DHS View of the TRM—shown in Exhibit 5—is primary for DHS and its subordinate organizations. Following its guidance will ensure compliance with the FEA TRM as well as with DHS direction. The HLS TRM uses the concept of functional layers. General characteristics of these layers are:

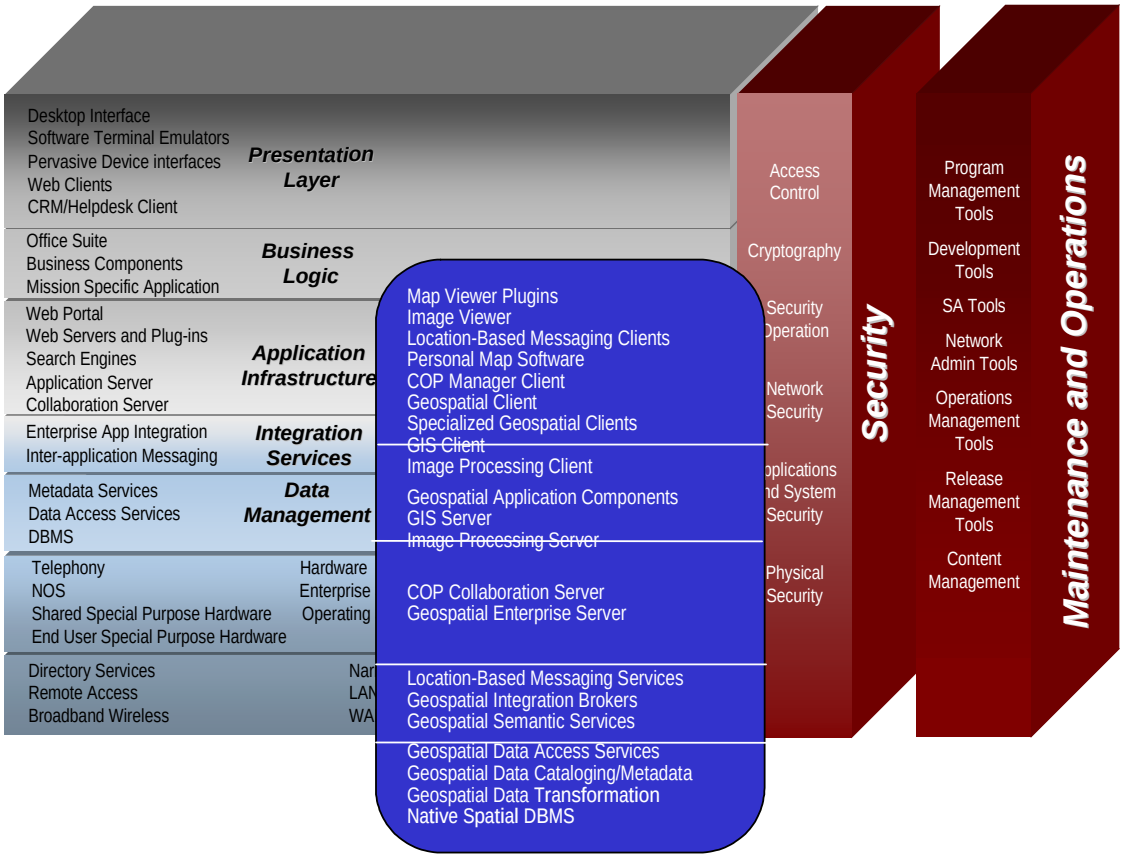
- A layer contains logically consistent groupings of services, and
- Layers "higher" in the TRM use the services of those "lower" in the TRM.

Services in one layer should not interface with services in other layers except through clearly defined paths.

---

[1] Federal Enterprise Architecture (FEA), Draft Service Component Reference Model (SRM), Draft Technical Reference Model (TRM), Agency Briefing, January 29,2003

Exhibit 5: HLS (Geospatial) TRM



External users at the public level will have access to HLS services via the Web. This access is provided at the Application Infrastructure Layer, with underlying services from all layers below.

External government users (including state and local) will have access at the Integration Services Layer, in the long term, primarily through Web services. Access to these services will be controlled by user role based security policies.

The main types of geospatial components are illustrated in the blue window.

2.3.2.1 Service Framework

The DHS Service Framework corresponds to the structure of the FEA Service Framework with two exceptions: an Application Infrastructure layer and a Data Interchange layer.

An Application Infrastructure layer has been added between the business logic and Data Interchange layers that contains the services needed to manage and execute business logic. The fundamental concept is one used to describe the Java 2 Enterprise Edition (J2EE) architecture and applies as well to other run-time environments such as Windows .Net services and even to the IBM Customer Information Control System (CICS) environment. Application components are managed by and execute within application environments called *containers*. Containers also

provide access, via *connectors*, to all of the various lower-level services and resources needed by applications such as databases, naming and directory services, asynchronous messaging and transaction services, and e-mail systems. Connectors are the Application Programming Interface (API) and protocols used to interchange data among application components and services. As a result of this change, some of the technical services and components included in the Platform Services tier of the FEA TRM are included in this layer. This approach better reflects the physical layering of services that exist in current vendor and Open Source products.

The Data Interchange layer of the FEA TRM has been extended to specifically include the functionality provided by integration brokers and related enterprise integration products. In addition, the protocols that make up the FEA TRM *Services Transport* area have been included here to reflect the more robust nature of the layer and to align with more traditional usage. The layer has been renamed the *Data Interchange/Integration* layer.

The layers of the HLS TRM Service Framework are as follows:

- **Presentation**—the technical services required to create and present application interfaces to end users,
- **Business Logic**—application-specific logic representation; that is, "software,"
- **Application Infrastructure**—the technical services required to allow business logic, and other application logic to function,
- **Integration Services**—the technical services and components required to interchange data among applications and services, and
- **Data Management** —the technical services and components required to access and modify data of all types.

As illustrated in Exhibit 5, the main types of geospatial components are:

Presentation Layer

-- Map Viewer Plugin

-- Image Viewer

-- Location-based Messaging Client

-- Personal Map Software

-- COP Manager Client

-- Geospatial Client

-- Specialized Geospatial Clients (67 types)

-- Geographic Information System (GIS) Clients

-- Image Processing Clients

Business Logic Layer

-- Geospatial Application Components

Application Infrastructure Layer

-- Geospatial Server
-- GIS Server
-- Image Processing Client
-- Geospatial Enterprise Services
-- Data Discovery Service
-- Service Discovery Service
-- Map Publication Service
-- Activity Report Service
-- After Action Report Service
-- Alert Warning Report Service
-- Emergency Declaration Report Service
-- Incident Report Service
-- Location (Site) Report Service
-- National Security Special EVENT (NSSE) Service
-- Situation Report Service
-- Suspicious Activity Report Service
-- Coverage Portrayal Report Service
-- Web Map Service
-- Web Terrain Service
-- Style Management Service
-- Geocoder/Reverse Geocoder Services
-- Geolocate Service
-- Gateway Service
-- Route Service
-- Navigation Service
-- Monitoring Service
-- Tracking Service
-- Weather Service
-- Traffic Service
-- Model Access Service
-- Geoparser Service
-- Sensor Planning Service

-- Sensor Collection Service

-- Sensor Alert Service

Data Interchange/Integration Layer

-- Geospatial Information Broker

Data Management Layer

-- Gazeteer Service

-- Web Map Service

-- Web Coverage Service

-- Web Feature Service

-- Web Terrain Service

-- (Location) Directory Service

-- Image Archive Service

-- Web Annotation Service

-- Spatial Query

-- Data Transformation Services

-- Coordinate (and Unit) Transformation Service

-- Topology Service

-- ETL

-- Native Spatial DBMS

-- Symbology Format

-- Geospatial Data Formats

-- Simple Features

-- Coverages

-- Registry Information Model

-- Service Information Model

-- Observations and Measurements

-- Sensor Model

-- Geography Markup Language

-- Sensor Model Language

2.3.2.2 Platform Services

The HLS TRM subdivides the FEA TRM Platform Services tier into two parts. Web Servers and Application Servers have been moved to the Application Infrastructure layer, as described previously. Storage is consolidated with Computing Platform. This layer now includes only those services and components that are completely application and programming model neutral.

- **Computing Platform**—physical hardware and operating system services that support the components of the Service Framework, and
- **Networking and Communications**—the devices, software, and communications media used to transport data among infrastructure components and to end-point devices.

2.3.2.3 Other Services

Three other refinements of the FEA TRM have also been made. *Security* is now shown as a vertical slice through both Platform Services and the Service Framework to indicate that security services are not monolithic, but distributed throughout the TRM.

The protocols and data format standards contained in the *Service Interface/Interoperability* area have been reallocated to appropriate layers:

- ***Data Format*** is now included in the Data Management layer,
- ***Data Exchange/Delivery*** is now included in the Integration Services layer,
- ***Service Discovery*** is now included in the Application Infrastructure layer, and
- ***Service Description/Interface*** is also included in the Application Infrastructure layer.

Finally, another category has been added to the TRM taxonomy and, as with security, appears as a vertical stack: *Management and Operations*. While many of the services required operating and managing DHS IT systems are or will be included in the FEA and/or DHS SRM (an SRM for DHS does not currently exist), there are technical services and components needed to enable those services. The Management and Operations area of the TRM includes those elements.

3.0 TRM DESCRIPTION

This section presents the structure and taxonomy for the HLS TRM. The layers are organized to reflect the technical tiers of the FEA TRM.

3.1 Service Framework Tier

3.1.1 Presentation Layer

The presentation layer includes a wide variety of user interface devices for desktop and mobile environments as well as supporting interfaces, protocols and services. The purpose of this layer is to provide flexibility in how information is presented to users by abstracting the means of presentation from the business logic. Ideally, a single application can be used over a variety of access channels using a variety of end-point devices.

This layer includes several types of clients, but the Web browser is preferred. Other client types should be used only when using a Web browser-based user interface would severely degrade performance or severely reduce availability.

3.1.1.1 Desktop Interface

The Desktop Interface is a Graphical User Interface (GUI) to a computer Operating System (OS). It allows a user to start and stop applications, manage files, and where allowed by the user's role, to manage the hardware and software, installing and uninstalling hardware and software.

This Tier maps to the FEA TRM Component Framework Presentation /Interface Category.

3.1.1.1.1 Desktop

The Desktop is the graphical environment on which Window Manager and Desktop Manager display windows, icons, and other graphic objects. The Desktop *may* be the primary handler of user interaction. Specific division of functionality may vary from one windowing environment to another. The behavior of the GUI is controlled at this level. In some systems the desktop is inherently tied to a single computer, in others it can transparently manage interaction with processes on multiple machines. The desktop may be spread across more than one physical display and may integrate windows owned by multiple users.

3.1.1.1.2 Assistive Technologies (Section 508)

The Desktop can provide various basic assistance services including keystroke alternatives to mouse actions, window magnifiers, special fonts and themes and integrated voice input and text to speech capabilities. Services covered in this category are only those inherent to or integrated with the desktop.

3.1.1.2 Web Client

Web browsers provide a generalized, standards-based client to deliver applications and services to end-users via devices that support Hypertext Transfer Protocol (HTTP)/HTTP Secure (HTTPS) delivery channels. Web browsers use plug-ins to render non-standard formats of Web pages. Plug-ins utilize standard interfaces to the browser. Web browsers are essentially ubiquitous in personal computers and workstations and "thin" workstations, and are beginning to appear in smaller pervasive service platforms such as PDAs and cellular telephones. Web browsers are the preferred application clients for DHS.

This Tier maps to the FEA TRM Service Access and Deliver Access Channel Category.

3.1.1.2.1 Web Browser

The Web Browser is the standard thin client for DHS. Web browsers are standards based and generally support local file access, remote file access using file transfer protocol (FTP), and remote file access and content rendering using HTTP or HTTPS. Browsers generally provide local print access to local print services and file services to print and save files locally. Browsers render files according to their Multipurpose Internet Mail Extensions (MIME) type. Universally supported types are Hypertext Markup Language (HTML), Text File (TXT), Graphic Interchange Format (GIF), and Joint Photographic Experts Group (JPEG). Most browsers support client side scripting via JavaScript and script interaction with browser Document Object Model (DOM) objects.

Most browsers also support additional MIME types via plug-ins.

3.1.1.2.2 PDA Web Browser

The PDA Web Bowser allows you to view full HTML web pages on PDA devices over the wireless and non-wireless Internet.

3.1.1.2.3 ActiveX Control

In the Microsoft Internet Explorer environment, the browser may be extended using locally installed or downloaded "controls." These controls may interact with the user and/or the operating environment at any level. Controls may be used to render special MIME types or they may be used to interface peripheral devices to the browser. The Microsoft standard for these controls is called ActiveX.

Specific ActiveX controls may be utilized to extend the browser's functionality for application interaction purposes. Historically ActiveX controls have represented security vulnerabilities. DHS discourages the use of ActiveX and will not allow its use in applications and components developed under the EA.

3.1.1.2.4 Java Virtual Machine Plug-in

Plug-ins may also provide generalized services to the browser. Java is enabled in current Web browsers through a plug-in, which makes available the services of the Java Virtual Machine (JVM).

3.1.1.2.5 Document Plug-in

Various specialized document formats may be rendered by plug-ins. Some plug-ins are strictly renderers, others implement interaction with the document, as in fillable forms.

3.1.1.2.6 Map Viewer Plug-in

The means to visualize and interact with geospatial data in rendered map form. Provides tools to select base map/image data for viewing, select optional graphics overlays (geospatial features/locations/structures/routes/observations/mobile-objects), set view window, display chosen view, measure and pinpoint, navigate through view with pan and zoom, etc. Optionally choose symbology, map display template or select previous views.

3.1.1.2.7 Other Plug-in

Multiple vendors offer other plug-ins such as those that render custom multi-media (sound, animation, video) in the browser. Some plug-ins are strictly renderers, others implement interaction with the document, as in speed, volume, and viewpoint controls.

3.1.1.2.8 Graphics and Drawing Viewer

An application that provides the capability to take a snapshot of an original drawing, particularly CAD drawings, and then to markup the drawing. All changes to the drawing take place on the snapshot, while the original file remains on the server. This allows all the changes to be committed to the drawing at one time. A web-based drawing viewer can also used to publish and view CAD drawing files and other related schematic, picture, imaging and document formats.

An application that provides the capability to take a snapshot of an original drawing, particularly CAD drawings, and then to markup the drawing. All changes to the drawing take place on the snapshot, while the original file remains on the server. This allows all the changes to be committed to the drawing at one time. A web-based drawing viewer can also used to publish and view CAD drawing files and other related schematic, picture, imaging and document formats.

3.1.1.2.9 Image Viewer

The means to visualize and interact with geospatial images (rectified or unrectified). Provides tools to select image and optional graphic overlays for viewing (geospatial features/locations/structures/routes/observations/mobile-objects), set view window, display chosen view, measure and pinpoint, navigate through view with pan and zoom, etc. Optionally choose symbology, image display template or select previous views.

3.1.1.2.10 Audio Player

Multiple vendors offer plug-ins that render custom sound formats. These typically allow interaction through volume and other sound controls..

3.1.1.2.11 Video Player

Multiple vendors offer plug-ins that render custom video formats. These include both streaming video and two-way interactive video for conferencing.

3.1.1.2.12 Animation

Animation software allows insertion and display of motion in still pictures and video.

3.1.1.3 Messaging Client

Delivery to and sending of asynchronous messaging services to and from the desktop requires a presentation layer client. Message clients may be standalone or integrated with other products and may implement single or multiple protocols.

This Tier maps to the FEA TRM Service Access and Deliver Access Channel Category.

3.1.1.3.1 E-Mail Client

An e-mail client is a program that uses DNS Mail Exchange (MX) records and Simple Mail Transfer Protocol (SMTP) to send and get electronic mail from a server. An e-mail client normally has fields of From, To, Subject, and Body, cc, bcc, attachments, date, and content type. The content encoding of e-mail message can either be American Standard Code for Information Interchange (ASCII), or MIME type that enables any binary attachments; such as sound, image, HTML, etc. E-mail clients at a minimum allow receiving, viewing, composing and sending of simple text messages over a local network or the Internet. More capable e-mail clients allow file enclosures, rendering of MIME types and interaction with an E-Mail server to manage mailboxes, mailing lists, and rules.

3.1.1.3.2 PDA E-Mail Client

General-purpose wireless PDAs and other similar special purpose dedicated e-mail devices are capable of viewing E-Mail and in some cases composing and sending it. Both simple and complex clients exist.

3.1.1.3.3 Defense Messaging Service Client

A Defense Messaging Service (DMS) client is an e-mail client capable of interoperating with a server on the DMS network.

3.1.1.3.4 Calendar Client

Simple calendar clients may be regarded as messaging clients and are frequently integrated with e-mail clients. The calendar client interacts with a calendar server to schedule meetings and display meeting schedules. More capable clients are capable of inviting attendees and allowing selective views of prospective attendee's schedule. As with e-mail clients, calendar clients may utilize enclosures and may render MIME types. Calendar clients may be capable of generating meeting reminders. A Calendar client is typically closely integrated with e-mail and with a directory.

3.1.1.3.5 Facsimile

Desktop Facsimile (FAX) clients permit sending and receiving FAX transmissions, either via a local modem or via a FAX server and shared modem. Facsimile display is usually in image form, but some FAX clients implement Optical Character Recognition (OCR) allowing conversion of an incoming FAX to a text file. Fax transmission may be done from simple text or optionally from more complex document formats. Actual transmission is in bit-mapped format.

3.1.1.3.6 Threaded Discussion

Threaded discussion clients allow asynchronous interaction with groups or groups of groups. Text is typically transmitted to the discussion server as e-mail or via a Web client. Successive messages and replies are displayed by the client in subject and time order.

3.1.1.3.7 Location-Based Messaging Client

The means to visualize location-based messages and 'reports' (messages with embedded geospatial elements). Example messages and reports include alerts, warnings, emergency declarations, situation reports, after-action reports, suspicious activity reports, activity reports, location reports and National Security Special EVENT (NSSE) Reports.

3.1.1.4 Office Suites and Personal Productivity Tools

Office suites and personal productivity tools are a set of programs required in an office environment, typically comprised of a spreadsheet, a word processor, a presentation generator, a scheduler, a note manager, a desktop database program, personal financial package, etc. The programs are normally produced or packaged by a single vendor and may work together seamlessly. Personal Productivity Tools are commercial off-the-shelf (COTS) tools similar to office tools, but of more limited scope.

This Tier maps to the FEA TRM Service Access and Deliver Access Channel Category.

3.1.1.4.1 Word Processor

A word processor is a tool for composing, editing and formatting text documents, most commonly in letter or short document format. Word processors may incorporate graphical tools and allow generation of compound documents (for example, a letter with an embedded spreadsheet).

Should support the means to incorporate geospatial products in map and report form.

3.1.1.4.2 Spreadsheet

Spreadsheets are display, calculation, and formatting tools. A spreadsheet typically is comprised of a grid of cells possessing content and rules or formulas. A spreadsheet may incorporate graphing capabilities tied to the contents of cells.

3.1.1.4.3 Presentation Tool

A presentation tool is typically intended to produce paper or electronic presentations formatted according to a standard design or template. Presentation tools typically include an outliner and graphics tools, particularly clip art tools. Presentation tools may be capable of generating animations and incorporating sound and other media in the presentation.

Should support the means to incorporate geospatial products in map and report form.

3.1.1.4.4 Desktop Database

A desktop database is a database intended for personal or small group use. It is typically characterized by a sophisticated graphical user interface and a relatively less powerful database engine. Desktop databases may utilize Structured Query Language (SQL), but generally hide details from the user.

3.1.1.4.5 Web Page Editor

Many office suites now incorporate a Web page editor. A Web page editor is generally intended to produce HTML for small or personal Web sites. They utilize a GUI and relieve the user of the need to edit HTML code. Tools in this category are those bundled with office suites and are generally less capable than the category of Web Site Tool.

3.1.1.4.6 Project Manager

A project manager is a component of an office suite designed to capture and document schedules and resource allocation and expenditures. These tools are generally highly graphical in nature and are capable of generating many types of graphs or views of a project.

3.1.1.4.7 Desktop Budget Tool

A Desktop Budget Tool is incorporated in some office suites or bundled with workstation packages. These tools are usually designed for personal financial management, but may be capable of performing simple budget functions for small offices or groups.

3.1.1.4.8 Desktop Compression Tool

A Desktop Compression Tool is a wrapper for a standardized data compression and file aggregation and archiving tool. These tools may be used in a single user environment for recovering disk space, or in e-mail or collaboration for compressing files before transmission. Care must be taken in choosing compression tools to assure interoperability.

3.1.1.4.9 Desktop Drawing and Diagramming

A desktop drawing and charting tool may implement one or more of a variety of functions including: freehand drawing, object based drawing composition, structured drawing based on templates, rules and methodologies, and production of charts from numeric input, frequently via a spreadsheet.

This software may embed map functionality and/or other geospatial tools.

3.1.1.4.10 Portable Document Generator

A portable document generator is a tool that converts text or complex text documents to a format commonly supported by free or inexpensive viewer software. (The viewer may be stand-alone or a plug-in.) The generator may be used to generate locked or encrypted documents or fillable forms.

3.1.1.4.11 CD/DVD Authoring

CD/DVD Authoring software allows assembling of content for transfer to a CD or DVD and provides a simple user interface to the CD/DVD recorder control functions.

3.1.1.4.12 Investigative Software

Investigative software is a category of tools used in law enforcement, financial investigation, and background checking. This category may include both COTS and government off-the-shelf (GOTS) packages.

This software may embed map functionality and/or other geospatial tools.

3.1.1.4.13 Personal Map Software

Personal Map-GIS Software includes a variety of tools for viewing, annotating and manipulating map data. Typically includes map data for standalone operations. Often includes Global Positioning System (GPS) capability for applications involving mobile assets, persons, goods, cargo and conveyances. Includes Commercial Mapping or GIS software for desktop or PDA.

3.1.1.4.14 PDA Office Suite

High end PDAs commonly come bundled with a minimal office suite, including a word processor and spreadsheet.

3.1.1.4.15 Desktop Publishing

Desktop Publishing applications are designed to assist in the page layout process. These applications help integrate text, diagrams, charts, and images into a cohesive, visually pleasing whole, prior to the document being printed and distributed. They are often used to create newsletters or other small documents for public or private distribution.

3.1.1.4.16 Multimedia and Graphics Editing

The software used to edit multimedia data, which combines various elements, such as images, icons, audio, video and hypertext to create a multimedia presentation.

3.1.1.4.17 Training Software

The set of applications that are used to create, distribute, manage or use Computer Based Training (CBT) courses and training programs.

3.1.1.5 Collaboration Client

Collaboration covers a wide range of services, many characterized by two-way, synchronous interaction among two or more participants. Collaboration is a team enabler that permits reduction in travel and increased productivity. A user's collaboration client may interact with another on a peer-to-peer basis or via a collaboration server.

This Tier maps to the FEA TRM Service Access and Deliver Access Channel Category.

3.1.1.5.1 Full Featured Collaboration Client

A full-featured collaboration environment is similar in philosophy to an office suite. It uses a set of related tools to provide a set of related, interoperable services. Typical functions include.

- Discussions groups
- Chat
- Conference management
- Document sharing
- Contacts list sharing
- Tasks management
- Project Timelines
- Team Folder support
- Subproject Home Page support
- Activity View
- Geospatial-temporal based COP and Mission-Specific Operating Picture (MSOP). See COP Manager.

Collaboration Clients may be Web Based or Based on a fat client.

3.1.1.5.2 Desktop Video Conferencing

Video conferencing is an important form of collaboration. Desktop video enables this form of conferencing without use of a dedicated conference facility.

3.1.1.5.3 Voice over IP Client (VoIP)

Voice over IP (VoIP) networks are increasingly being used to replace long distance telephone calling. VoIP is available through dedicated terminal units (VoIP Phones) or through software on the desktop. Desktop and terminal solutions may interoperate, and gateways to the public switched network allow calling to conventional phones.

3.1.1.5.4 Real-time Whiteboard

Technologies exist that allow real-time interaction and sharing of concepts via a virtual or real whiteboards. The desktop real-time whiteboard is a software program that shares a drawing and access to drawing tools among two or more participants at different desktops.

This software includes geospatial tools for visualizing and interacting with the COP and MSOP. See COP Manager.

3.1.1.5.5 Instant Messaging

Instant Messaging (IM) is a server-mediated capability for one to one teletype style interaction. Instant Messaging clients maintain lists of prospective participants and provide alerts when a participant is available and willing to participate. Public IM is not encrypted. Private IM services may provide encryption.

3.1.1.5.6 Chat Room

Chat is similar to IM, but with multi-party participation. A chat room is the set of participants in the conversation. Access may be either pre planned and limited in scope, by invitation, by discovery, or publicly advertised. Some public chat systems allow for exclusion by vote of the participants. As with IM, public chat is not encrypted. Private chat services may provide encryption.

3.1.1.5.7 Facilitation Tools

Meeting facilitation, either local or virtual can be facilitated by tools that allow a leader or moderator to focus the discussion, take votes and establish consensus based either on public or anonymous discussion.

3.1.1.5.8 Distance Learning Tools

Distance Learning tools provide collaboration in a virtual classroom setting. Emphasis is on interaction with an instructor and on on-line testing.

3.1.1.5.9 Information Visualization

Information Visualization and virtual reality clients may be used in a collaborative environment. These tools may be used for collaborative analysis or collaborative planning.

This software includes geospatial tools for visualizing and interacting with the COP and MSOP. See COP Manager.

3.1.1.5.10 Wireless Collaboration

Various collaboration tools are implemented in the wireless environment. This category covers all standards and products specific to the wireless environment, and also specifies any other generic collaboration tools that *may* be used in the wireless environment.

3.1.1.5.11 COP Manager Client

The COP Manager provides the means to manage the scope and resources associated with a COP, select and allocate resources, manage and monitor collaboration activities, monitor status and performance of resources, and monitor and manage external communications. The distinction between the COP Manager and other operations applications is that the COP Manager is managing the big picture, whereas other applications focus on MSOP and other mission-specific operation activities.

3.1.1.6 Customer Relationship Management (CRM) /Helpdesk Client

CRM tools and Helpdesk support tools enable an enterprise to assure timely and consistent service internal and external and external service users.

This Tier maps to the FEA SRM Customer Services Type.

3.1.1.6.1 Customer Relationship Management Client

A CRM client may be client/server or Web based, typical features include:

- Searchable Knowledge Base
- Create, View, Update, and close support items
- Remote control capabilities
- Create, View, Update, and delete appointment entries
- Generate and review log entries
- View contact demographics and history (in geospatial context)
- Provide guided real-time ad hoc query capabilities against a customer database
- A CRM client typically is utilized in "sales" or order taking environment
- Map functionality and/or other geospatial interaction tools with customer locations.

3.1.1.6.2 Helpdesk Tool

Helpdesk tools usually are a subset of CRM emphasizing trouble diagnosis, reporting and tracking. Helpdesk systems are focused on trouble tickets and systematic problem resolution.

3.1.1.7 Document Management

Document management broadly focuses on access to documents, document workflow, dissemination, and review processes. Tools in this category frequently overlap, but frequently do not interoperate.

This Tier maps to the FEA SRM Digital Assets Services Type.

3.1.1.7.1 Document Management Client

A document management client typically accesses a server with workflow capabilities. This server manages receipt (including scanning and OCRing), searching, cataloging, routing and managing of structured review processes. The client provides user access to a set of the server's capabilities appropriate to the user's role.

3.1.1.8 Software Terminal Emulator

Traditionally Mainframe and Unix clients were specialized hardware devices. Today almost all client access to mainframes and to Unix systems is done through software based terminal emulation programs. These programs provide the look, feel, and functionality of legacy system hardware terminals on the desktop.

This Tier maps to the FEA TRM Service Access and Deliver Access Channel Category.

3.1.1.8.1 Dumb Terminal

Dumb terminals are a class of terminals with no or minimal local processing capability. This class includes simple teletype emulators, various generations of mainframe terminal emulators, (including IBM 3270 series emulation), and typical Virtual Memory System (VMS) and Unix command line interface terminals (VT100 series etc). Dumb terminal emulators provide the functionality of these devices in a window on the desktop. These emulators may include simulation of attached peripherals such as printers. A major issue with dumb terminal emulators is security. The protocols supported on the original hardware were no encrypted and did not support any strong form of authentication. This problem is addressed by utilizing upgraded protocols, mediated by an intermediate client/relay server running on the source machine.

3.1.1.8.2 Windows Client

It is not normally possible to remotely run desktop processes from Windows based PCs. To allow this capability, add on systems called terminal servers and Windows Clients have been developed. The Windows client is a thin client that supports only the basic window management and display capabilities of the Windows operating system. Windows clients may be implemented on hardware similar to browser based thin clients, or may simply consist of an emulator running on a full featured Windows platform.

3.1.1.8.3 X-Windows Server

An X-Windows Server is a *client* that allows both local and remote access to windowed content and controls. X-Windows is usually associated with Unix , but may run on a variety of OSs. X Servers running on Windows platforms allow communication with the Unix environment.

3.1.1.8.4 Remote Desktop Protocol

Remote Desktop Protocol (RDP) includes clients based on the Microsoft RDP protocol, other than Citrix and other full featured remote Windows implementations. This includes browser based clients, and clients implemented on non–Windows environments.

3.1.1.9 Pervasive Device Interfaces

Pervasive computing devices utilize a number of distinct interface types. The objective of pervasive computing integration is to allow all types of devices in this category to participate within the enterprise.

3.1.1.9.1 Handheld PDA

Handheld PDAs typically have a small display with overall resolution in the 320 x 240 pixel range. PDAs do not generally utilize a multiple window paradigm. PDAs usually use stylus or function key input. Handheld PDAs may be equipped with a keyboard, but generally are not.

This Tier maps to the FEA TRM Service Access and Deliver Access Channel Category.

3.1.1.9.2 Wireless Email

Wireless e-mail devices generally are single or multi line text only displays. Devices capable of sending as well as receiving generally have a built in keyboard. Devices in this class do not generally have a pointing device, but rely on the keyboard for control.

3.1.1.10 Geospatial Client

A desktop client, either thick or thin, that provides visualization and interaction with geospatial data, including vector, raster, 2D and 3D. For 3D display, supports image drape over digital terrain model (DTM), with color and texture controls. Also provides access to associated Application Components and Geospatial Services.

3.1.1.10.1 Specialized Geospatial Clients

Various specialized geospatial clients exist within the HLS EA (

Table 1). The following table lists the HLS applications that involve geospatial data and technology, each which may have a Geospatial Client and one or more Application Components and/or Geospatial Services.

Table 1 - HLS Geospatial Clients & Application Components

HLS Geospatial Clients & Application Components	
Asset Inventory Management	Monitor Locations
Biographical Analysis	Monitor Parties
Case Analysis	Monitor Recovery
COP Manager	National Security Special Event Reporting
Countermeasure Planning	Operational Planning
Critical Infrastructure Inventory Management	Performance Planning & Analysis
Damage Assessment	Post Mission Analysis
Data Acquisition/ Generation	Preparation Planning
Data Collection Management	Program Planning
Data Collection Planning	Public Information Outreach
Disaster Assistance	Recovery Planning
Electronic Navigation	Response Planning
Emergency Reporting	Risk Analysis
Evacuation Planning & Management	Screening and Risk Analysis
Event Analysis	Search and Rescue Planning
Event Planning & Analysis	Search and Rescue Response
Exercise Planning	Security Planning
Facility Mapping & Management	Security Protection & Management
Geospatial Data Transfer	Sensor Management

Geospatial Integration & Test Tools	Site Analysis
Hazard Mapping	Situation Awareness
Health & Safety Monitoring	Suspicious Activity Reporting
Hydraulic-Hydrographic Modeling	Tariff Management
Incident/Event Management	Threat Analysis
Incident Reporting	Threat Consequence Assessment
Location Search & Reporting	Threat Detection
Logistics Planning	Training Exercise Simulation
Map Publication	Training Planning & Support
Mission Planning	Travel Planning
Mission Rehearsal	Vulnerability Analysis
Mitigation Planning & Analysis	Warning/Alert Management
Monitor Assets	Waterway Management
Monitor Conveyances	Weather Modeling & Analysis
Monitor Goods	

3.1.1.10.2 GIS Client

A general purpose Geographic Information System (GIS) client, either thick or thin, that provides visualization and interaction with geospatial data. Also provides access to underlying Geospatial Application Components and Geospatial Services.

The primary client capabilities are summarized below.

3.1.1.10.3 Image Processing Client

A desktop client, either thick or thin, that provides visualization and interaction with geospatial imagery data. Many specialized geospatial imagery applications may exist within the HLS EA. May also provide access to underlying Application Components and bundled Geospatial Services.

3.1.1.11 Narrow Band Wireless Access

Narrow Band Wireless is a wireless telecommunication technology that carries voice information in a narrow band of frequencies.

3.1.2 Business Logic Layer

The business logic layer contains encoded logic in various forms used to implement business rules and related functionality.

3.1.2.1 Application Components

An Application Component is a program, screen, datastore, or control member inside an application. An Application Component can be shared by more than one application.

This Tier maps to the FEA SRM Services Domain.

3.1.2.1.1 Common Business Components

Common Business Components are a category of application components that serve business functions common to multiple applications. These components may be custom developed, COTS or may be built by wrapping legacy systems with a Web services or other standardized service interface.

3.1.2.1.2 Geospatial Application Components

The Geospatial Clients defined in

Table 1 may have one or more server-side Application Components. These components contain geospatial business logic and exploit Geospatial Enterprise Services (see 3.1.3.8), which are common geospatial services that are available throughout the enterprise.

3.1.2.2 Office Suite Components

Modern integrated office suites and other integrated software environments frequently are designed to expose powerful, well documented interfaces. These interfaces allow use of this class of application as a service provider.

This Tier maps to the FEA SRM Services Domain.

3.1.2.2.1 Word Processor

Word Processor Components are common business components that specialize in rich text formatting.

Includes the means to insert Geospatial Products into word documents for publication.

3.1.2.2.2 Spreadsheet

Spreadsheet Components are common business components that specialize in computation.

Includes the means to insert Geospatial Products into spreadsheet documents for publication.

3.1.2.2.3 Desktop Database

Desktop Database components are common business components that specialize in managing structured data and providing query services.

Includes geospatial data management capabilities.

3.1.2.2.4 Project Manager

Project Management Components are common business components that specialize in scheduling and charting.

Includes geospatial project management capabilities.

3.1.2.3 Business Intelligence Components

Business Intelligence (BI) is a set of applications and technologies for collecting, storing, analyzing, presenting data to enhance business decision making process. BI includes decision support systems, query and reporting, searching, online anaylytical processing, statistical analysis, forecasting, pattern matching, and data mining.

This Tier maps to the FEA SRM Business Analytic Services Type.

Includes geospatial BI capabilities.

3.1.2.3.1 Data Mining

Data mining tools process data to identify patterns and relationships among data items. Data mining may include associating, sequencing, classifying, clustering, and forecasting of data.

Includes geospatial data mining capabilities.

3.1.2.3.2 Data Warehouse/Data Mart

Data Warehouse and Data Mart tools manipulate collections of data to support decision-making. The data may cover diverse sources, but presents a cohesive business picture. Tools for development of Data Warehouses and Data marts include features of data extraction from operating systems and data access via database systems. A Data Warehouse is enterprise wide data store; while a Data mart is more narrowly focused data store.

Includes geospatial data warehouse and data mart capabilities.

3.1.2.3.3 On-Line Analytical Processing

On-Line Analytical Processing (OLAP) is a set of software tools that enables in-depth analysis of data stored in a database. The analyzed data can be multi-dimensional, aggregated, or metadata, from multi database server, in multi-tier environment.

3.1.2.3.4 Knowledge Management

Knowledge Management (KM) is the category of applications and technologies designed to support the systematic process of finding, selecting, organizing, distilling and presenting information in a way that improves a user's comprehension in a specific interest area.

This includes geospatial knowledge management capabilities.

3.1.2.3.5 Decision Support Tools

Software that supports model-driven "what if" analysis for business decisions wherein decision-makers vary one or more variables within the model and the software calculates the changes that result from the decision.

3.1.2.4 Search Services

Search services provide the ability to search documents, folders, images, multi-media, web pages etc. on a computer, network, website or the Internet. This Tier maps to the FEA SRM Business Analytic Services Type.

3.1.2.4.1 Pattern Matching

Pattern Matching is a powerful, real-time, user-defined filtering option. With Pattern Matching, users can create unique rules with Boolean expression, wildcards, Regular Expression or any other methods offered by Pattern Matching tool. Those rules limits elements within user requested data and present the matched data to users.

Includes geospatial-temporal pattern and trend capabilities.

3.1.2.4.2 Search Engine

A Search Engine is a program that searches documents that contain keywords specified by user and returns list of resulting documents. A search engine contains a spider program that does the searching and an indexer program that reads resulting. It documents and creates an index based on the keywords contained in each document.

This includes geospatial-temporal (2, 3, & 4D) indexing and search capabilities.

3.1.2.5 Customer Relationship Management Tools

CRM refers to all aspects of interaction between an enterprise and it's customer. CRM includes customer data collection, centralized customer information database, sophisticated data analysis, customer-centric interaction, improving customer satisfaction.

This Tier maps to the FEA SRM Customer Services Type.

Includes map functionality and other geospatial analysis tools.

3.1.2.6 Rules Engines

A Rules Engine is an application module that enables creating, storing, modifying, and applying business rules. Rule Engine separates business rule from control logic, data storage, and user interface modules.

3.1.2.7 Geospatial Servers

3.1.2.7.1 GIS Server

The Geographic Information System (GIS) server comprised of bundled services that support the generation, revision, management, processing, and output of geospatial data. Consists of the server-side Geospatial Application Components comprising a GIS.

These server capabilities match up with the client-side capabilities listed in section 3.1.1.10.2.

3.1.2.7.2 Image Processing Server

The Image Processing System (IPS) server comprised of bundled services that support the generation, revision, management, processing, and output of geospatial image data. Consists of the server-side Geospatial Application Components comprising an IPS.

These server capabilities match up with the client-side capabilities listed in section 3.1.1.10.3.

3.1.2.8 Search Engine

A Search Engine is a program that searches documents that contain keywords specified by user and returns list of resulting documents. The search Engine is often used for document search of World Wide Web, file systems, and etc. A search Engine contains a spider program that does the searching and an indexer program that reads resulting documents and creates a index based on the keywords contained in each document.

Includes geospatial-temporal (2,3 & 4D) indexing and search capabilities.

3.1.2.9 Rules Engines

A Rules Engine is an application module that enables creating, storing, modifying, and applying business rules. Rule Engine separates business rule from control logic, data storage, and user interface modules.

This Tier maps to the FEA TRM Component Framework Business Logic Category.

3.1.3 Application Infrastructure Layer

The application infrastructure layer provides the technical services and components needed to manage and execute business and other application logic and to interact with end-users (via access and delivery channels) and/or with other service components.

3.1.3.1 Web Portal

Web portals are multi-part Web pages that provide a single, personalized Web-based user interface as the common entry point to multiple applications and optionally to multiple application clients. Web portals should have a hierarchical, topical directory, search engine service, and latest relevant news headlines. Example Web portals are www.yahoo.com and www.egov.gov.

This Tier maps to the FEA TRM Service Platform and Infrastructure Delivery Services Category.

3.1.3.1.1 Personalization

Personalization is a commonly implemented Portal service that allows the user to customize the content and functionality of portal pages to suit individual needs. An example of personalization is MyYahoo!

3.1.3.1.2 Pervasive Device

Pervasive Device support allows access to Portal services from diverse device interfaces. Typically the portal services are served as eXtensible Markup Language (XML) and gateway services format the content in the manner best suited to the target device.

3.1.3.1.3 Portal Content Management

Portal Content is frequently dynamic and/or stored in a database. Portal Content Management services perform retrieval and translation functions based on requirements of the user and of the user's personalization and device choice.

3.1.3.1.4 Wireless Portal

Specialized Portal products exist for use in the Wireless environment. These products include tools for reformatting "legacy" Web content for wireless transmission and display, as well as implementation of XML based presentation protocols.

3.1.3.2 Web Server and Plugins

A Web server provides the interface between end users using Web browsers and business logic or Web-based content. The Web server accepts and responds to requests for service, via HTTP, HTTPS, Lightweight Directory Access Protocol (LDAP), Network News Transfer Protocol (NNTP), FTP, and etc. Optionally, a Web server may also authenticate the client, via passwords or Public Key Infrastructure (PKI) certificates, establish an encrypted path to the client using HTTPS and enable access to restricted resources and services. Static HTML pages are accessed and transmitted directly by the Web server while more complex tasks are forwarded to application servers.

This Tier maps to the FEA TRM Service Platform and Infrastructure Delivery Services Category.

3.1.3.2.1 Web Server

The Web Server is the component that responds to content requests from the Browser, the Web server may obtain content directly from a file or may pass through the request to one of a number of backend services. Backend services may be implemented in a number of ways, through CGI, applets or servlets, or through components bound to the server through various plugin architectures.

3.1.3.2.2 Server Plug-ins

A server plug-in is generally statically bound to the Web server and may function in a number of ways: through scripting, through, control by external factors (say a time service or traffic camera) or by passing control parameters from the requestors Universal Resource Locator (URL). A typical example would be a charting plug-in that dynamically generates a stock chart based on external data, and a ticker symbol request passed from the browser to the server.

3.1.3.3 Application Server

An Application Server (AS) provides the execution environment for the business logic tier in a three- or n-tier software architecture. An application server is a server program or a group of programs running on a computer in a distributed network that provides the business logic and transactional processing for an application. The application server is generally viewed as the intermediary between a Web server and a database server, although it may interact with other applications servers also. The application server may closely integrate with Web server to translate HTML commands so databases can interpret them.

This Tier maps to the FEA TRM Service Platform and Infrastructure Delivery Services Category.

3.1.3.3.1 Open Standard AS

An "open standard" AS is one based on some form of an open standards based architecture. Generally, a J2EE based AS would be regarded as open in that multiple vendors conform to the

same published standard. The standard itself is not strictly open however in that it is controlled exclusively by a single vendor.

3.1.3.3.2 Proprietary AS

Proprietary AS also exists both in niche areas, and with major market share from major vendors.

3.1.3.3.3 Wireless AS

An AS specifically designed, or incorporating components designed for formatting and managing data for display on and interaction with a Wireless PDA or similar device.

3.1.3.4 Electronic Mail Server

An electronic mail (e-mail) service manages the exchange of text and other document-based data between a sender and one or more receivers. This service only addresses the message store(s) and interfaces. The e-mail clients used to read and/or create and send messages are considered to be enterprise applications. To exchange e-mail with outside of an enterprise, electronic mail server may be located in Demilitarized Zone (DMZ). Examples of electronic mail servers are Microsoft Exchange Server. An e-mail server provides SMTP, Post Office Protocol version (POP3), and/or Internet Message Access Protocol (IMAP) services. Example electronic mail servers are Sendmail, CC:Mail, and Microsoft Exchange Server.

This Tier maps to the FEA TRM Service Platform and Infrastructure Delivery Services Category.

3.1.3.4.1 IMAP Server

Internet Message Access Protocol (IMAP) allows a client to access and manipulate electronic data messages on a server; permitting manipulation of remote message folders, called “mailboxes”, in a way that is functionality equivalent to local mailboxes. IMAP also provides the capability for an offline client to resynchronize with the server.

3.1.3.4.2 POP3 Server

Post Office Protocol 3 (POP3) server is an email server that implements and supports use of the POP3 protocol for delivering email to clients.

3.1.3.4.3 MIME Server

An email server which implements the MIME standard(s) for receipt and delivery of non-ASCII email and attachments.

3.1.3.4.4 SMTP Server

An SMTP server represents a pure open standard based solution. SMTP servers may act as end point servers or as intermediate relay servers. SMTP has advantages of openness and wide compatibility, but has serious drawbacks from a security and an operational viewpoint. SMTP addressing may be trivially spoofed, and the protocol does not guarantee delivery or provide automatic notification of delivery.

3.1.3.4.5 Proprietary Server

Many proprietary E-Mail server solutions exist, most will interoperate with SMTP and all provide extensive lists of additional features addressing the shortcomings of SMTP. Most can only interoperate via SMTP however.

3.1.3.4.6 Email Gateway

An Email Gateway is a relay server that is capable of locally routing to named addresses within a local subdomain and that generally has filtering capabilities that allow enforcement of a variety of policies dealing with enclosures, message size and origin and destination.

3.1.3.4.7 Email Monitoring

Email monitoring – many organizations utilize e-mail monitoring to scan internal and internet e-mail to enforce organizational regulations and to prevent loss or compromise of sensitive information.

3.1.3.5 Collaboration Server

A Collaboration Service (CS) manages the exchange of e-mail, instant messages, and other data between a sender and one or more receivers and maintains shared calendars and other group collaboration resources. Examples of collaboration services are America On Line (AOL) IM, Microsoft IM, and WebEx Web Conference.

This Tier maps to the FEA TRM Service Platform and Infrastructure Delivery Services Category.

3.1.3.5.1 Wireless CS

A CS specifically designed, or incorporating components designed for formatting and managing data for display on and interaction with a Wireless PDA or similar device.

3.1.3.5.2 Desktop Video Conferencing Server

A server that manages the synchronous video and audio communications between two or more clients, often providing support for multicasting, video stream compression and/or stream translation into a different format.

3.1.3.5.3 Voice over IP Server

A server that manages the connection between two or more workstations capable of VoIP and provides connection related services.

3.1.3.5.4 Real-time Whiteboard Server

A server that provides the ability for two or more clients to edit, simultaneously and synchronously, a drawing (whiteboard) hosted on the server. Servers providing this service typically only send changes to the drawing to clients, limiting the amount of network traffic generated by the server and clients.

3.1.3.5.5 Instant Messaging Server

A server that manages and relays real-time, synchronous, text-based messages between two clients. These servers often support encryption and logging of messages and a feature related to

the client establishing a “virtual presence” whereby the server indicates to other clients if a client is currently logged on, active, or has set an “away message.”

3.1.3.5.6 Chat Room Server

A server that supports the real-time, synchronous, text-based communication between two or more clients whereby the clients post messages in real-time to the server, and all clients in the “chat room” receive the message automatically. Message receipt is based upon the client’s presence in the “chat room” rather than then client’s identity.

3.1.3.5.7 Facilitation Tools Server

Applications which assist one or more moderators, leaders or facilitators to focus the discussion, take votes and establish consensus based on public or anonymous discussion.

3.1.3.5.8 Distance Learning Server

A server hosting one or more tools which optimize collaboration in a virtual classroom setting between an instructor and one or more students. These tools typically include display of presentation or course content materials, the ability to take tests online, and tools which facilitate the interaction between the instructor and a student or students.

3.1.3.5.9 Information Visualization Server

Server-side software which takes data, formats it, and outputs a video or audio stream, for monitor(s), projector(s), speaker(s), which enable a user to view a data set in a variety of visual and audio formats. Information Visualization Servers are differentiated from Information Visualization Clients by the Server’s ability to drive multiple monitors, projectors, and/or speakers and the server’s ability to generate complex visualizations of massive, complex data sets, such as those generated by supercomputers, rapidly.

3.1.3.5.10 COP Collaboration Server

A CS for managing and monitoring shared COP/MSOP resources and the collaborative exchange of geospatial data.

3.1.3.5.11 Web Notification Service (WNS)

A service by which a client may conduct a dialog with one or more other services. This service is useful when many collaborating services are required to satisfy a client request, and/or when significant delays are involved is satisfying the request, which is often the case in the geoprocessing realm.

3.1.3.6 CRM/Help Desk Server

CRM tools and Helpdesk support tools enable an enterprise to assure timely and consistent service internal and external and external service users.

This Tier maps to the FEA TRM Service Platform and Infrastructure Delivery Services Category.

3.1.3.6.1 CRM Server

A CRM server may be client/server or Web based, typical features include support for:

- Searchable Knowledge Base
- Create, View, Update, and close support items
- Remote control capabilities
- Create, View, Update, and delete appointment entries
- Generate and review log entries
- View contact demographics and history
- Provide guided real-time ad hoc query capabilities against a customer database

3.1.3.6.2 Helpdesk Server

Helpdesk servers usually are a subset of CRM emphasizing trouble diagnosis, reporting and tracking. Helpdesk systems are focused on trouble tickets and systematic problem resolution.

3.1.3.7 Geospatial Server

Geospatial Servers specialize in dealing with geospatial data. Depending on vendor 'packaging', these may be available as a bundled set of related components, or as unbundled services.

3.1.3.7.1 GIS Server

The GIS server is comprised of bundled components that support the generation, revision, management, processing, and output of geospatial data. Consists of the server-side components comprising a GIS.

3.1.3.8 Geospatial Enterprise Services

The Geospatial Enterprise Server provides the means to publish, access, and process geospatial data via services that are accessible throughout the enterprise. These geospatial enterprise services are the building blocks for geospatial applications, and the means for non-geospatial applications to readily access geospatial functionality.

This category includes Location-Based Services (LBS) for wireless applications.

3.1.3.8.1 Data Discovery Service

Able to search for and locate desired data through open, standard publish-find mechanisms. Search requests may be defined in terms of geospatial-temporal, mathematical and statistical filters for discovering data and data relationships, and optionally storing the metadata results as a new data set.

3.1.3.8.2 Service Discovery Service

Able to search for and locate desired services through open, standard publish-find mechanisms. Search requests may be defined in terms of filters for discovering services and service-data relationships, and optionally storing the metadata results as a new data set.

3.1.3.8.3 Map Publication Service

Able to automatically generate and publish Maps of interest for inclusion in a plan, report, or other Geospatial Product, with select content and symbolization (map template). To produce a Map for inclusion in a word or graphic document.

3.1.3.8.4 Activity Report Service

Able to generate an Activity Report for any location-based activity.

3.1.3.8.5 After Action Report Service

Able to generate an After Action Report with the geospatial context of the root cause, status and recommendations pertaining to post-incident recovery operations.

3.1.3.8.6 Alert-Warning Report Service

Able to generate an Alert-Warning Report with information about a location-based alert or warning messages.

3.1.3.8.7 Emergency Declaration Report Service

Able to generate an Emergency Declaration Report with the geospatial extent and nature of an emergency.

3.1.3.8.8 Incident Report Service

Able to generate an Incident Report with information about a location-based incident message.

3.1.3.8.9 Location (Site) Report Service

Able to generate a Location Report with information about an HLS data object’s location, related entities, and geospatial context. Example objects include geospatial feature, person, asset, conveyance, goods, cargo, device, etc.

3.1.3.8.10 National Security Special EVENT (NSSE) Report Service

Able to generate a NSSE for an EVENT.

3.1.3.8.11 Situation Report Service

Able to generate a Situation Report with the geospatial extent and nature of an operational situation.

3.1.3.8.12 Suspicious Activity Report Service

Able to generate a Suspicious Activity Report for a location-based suspicious activity.

3.1.3.8.13 Coverage Portrayal Service (CPS)

The CPS is chained to a Web Coverage Service (WCS) to convert geospatial coverage data (grid/image) to a map. The resultant map can be overlayed with data fetched from other servers for reference and orientation.

3.1.3.8.14 Web Map Service (WMS)

The means to render 2D maps. See 3.1.5.2.4.

3.1.3.8.15 Web Terrain Service (WTS)

The means to render 3D views of geospatial data. See 3.1.5.2.7.

3.1.3.8.16 Style Management Service (SMS)

The means to create, update and manage styles and symbols. The SMS must manage distinct objects that represent styles and symbols and provide the means to discover, query, insert, update, and delete these objects. Styles provide the mapping from feature types and feature properties and constraints to parameterized Symbols used in drawing maps. Symbols are bundles of predefined graphical parameters and predefined fixed graphic "images".

3.1.3.8.17 Geocoder/Reverse Geocoder Services

Able to determine geospatial coordinates, given an address (Geocoder), or determine address, given geospatial coordinates (Reverse Geocoder). A Geocoder transforms a description of a feature location, such as a place name, street address or postal code, into a normalized description of the location, which includes coordinates. A Geocoder Service receives a description of a feature location as input and provides a normalized address with coordinates as output. The feature location descriptions are any terms, codes or phrases that describe the features, and that are well-known to the Geocoder Service, such as a street addressing or postal coding scheme.

These services are very important across the HLS enterprise, as they enable enterprise users to exploit the geospatial-temporal context of the wide diversity of HLS business data that contain Location References, such as address, building name, census tract, etc. They are also key to correlating, integrating and fusing dissimilar data on the basis of geospatial-temporal characteristics.

3.1.3.8.18 Geolocate Service

The means to determine a location for a fixed or mobile object of interest (e.g., geospatial feature, person, asset, conveyance, goods, cargo, device, etc.) Mobile Objects must be equipped with GPS, Radio Frequency ID (RFID), and/or other position determination technologies.

3.1.3.8.19 Gateway Service

The Gateway Service determines the geospatial position of a known mobile terminal from a wireless network. Position is expressed in geographic coordinates. Mobile terminals (cell phones, PDAs, etc) must be equipped with GPS or some other position determination technology. An important service used in LBS, in the wireless realm.

3.1.3.8.20 Route Service

Able to determine (or fetch a predetermined) route and navigation information for autonomous or semi-autonomous navigation between two or more points on a network. An important service used in LBS, in the wireless realm.

3.1.3.8.21 Navigation Service

An enhanced version of the Route Service, which determines routes between two or more points with enhanced navigation information. An important service used in LBS.

3.1.3.8.22 Monitoring Service

Able to determine (or fetch a predetermined) location/time/identity/status/activity series for a Location.

3.1.3.8.23 Tracking Service

Able to determine (or fetch a predetermined) location/time/velocity/identity/status/activity series (track) for a mobile object (e.g., persons, goods, assets, devices, etc.)

3.1.3.8.24 Weather Service

The means to access weather conditions for an area of interest or location for a specified time period.

3.1.3.8.25 Traffic Service

The means to access traffic information regarding incidents and/or conditions for a specified area of interest, road, or road segment, for a specified time period.

Also, the means to access traffic information regarding incidents and/or conditions for a designated route (that has been determined by a Route Service or Navigation Service) for a specified time period.

3.1.3.8.26 Model Access Service

Able to determine and access the extent and nature of a Toxic Dispersion Model (e.g., plume) for a chemical or biological event in air or water. The model output is characterized by features.

“Toxic Dispersion” refers to the effects of introducing a chemical, radioactive or biological agent into the atmosphere or a water supply at a point source. Simulation is employed to understand the effects of a toxic agent within its medium. The objective of the simulation is to ascertain contamination levels in a geospatial-temporal context, and thus, to understand the nature of toxic

plumes, danger zones, warning zones, and related features, and to be able to view or analyze the output from a simulation run in conjunction with any other geospatial data, e.g., as plumes or danger/warning zones within a geospatial decision support tool.

Also, the ability to determine and access weather, hydrographic and other environmental parameters through environmental simulation. The simulation output is characterized by observations.

3.1.3.8.27 Geoparser Service

Geoparsing refers to the capability to scan and parse a textual document, identifying key words and phrases that have geospatial-temporal context. A Geoparser Service works in the context of two bodies of information: a reserved vocabulary (a dictionary of place names, a gazetteer or a directory of points of interest (POIs) and a text source (e.g., a newspaper or cable.). The Geoparser returns all occurrences of the use (in the text source) of any term in the reserved vocabulary. Each occasion establishes a geolinks (geospatial/temporal-aware hyperlink) between text terms and the geospatial location associated with the reserved word. That result is an annotated text document with geolinks.

3.1.3.8.28 Sensor Planning Service (SPS)

A service by which a client[2] can determine sensor collection feasibility for a desired set of collection requests for one or more mobile sensors/platforms, or the client may submit collection requests directly to these sensors/platforms.

3.1.3.8.29 Sensor Collection Service (SCS)

A SCS is a service by which a client can obtain observations from one or more sensors/platforms (can be mixed types). Clients can also obtain information that describes the associated sensors and platforms.

3.1.3.8.30 Sensor Alert Service (SAS)

The SASs produce alert messages when given observation conditions are met by a sensor. Provides the means for client services/users to specify and register user profiles that contain user information, applicable sensors/observations, alert conditions (e.g., maximum/minimum values), and alert actions (what happens if conditions are met). Also, the means for client services/users to update user profiles. Clients are able to control the nature of alerts. For example, a client is able to activate/deactivate an alert capability. Also provides the means to support push/pull capabilities, e.g., to wait for observation input from associated sensors (for on/off sensors like a detector), or to actively poll for (current/historical/predicted) sensor observations.

3.1.3.9 Transaction Processing Servers

This Tier maps to the FEA TRM Service Platform and Infrastructure Delivery Services Category.

---

[2] Client, as used here, means any software component or application that invokes a Web service.

3.1.3.9.1 TP Manager

A TP Manager manages routing and transaction processing of a service request. It manages global transactions and coordinates transaction resolution and failure recovery.

3.1.3.9.2 Transaction Server

Transactions contain a datum or data along with an associated command to be performed on the data. Transaction Servers verify that the command completed successfully on the data before the transaction completes. Transactions that do not complete successfully may be "rolled back" to a prior state.

3.1.3.9.3 OLTP

On-Line Transaction Processing (OLTP) is a class of software program that facilitates and manages transaction-oriented applications; typically for data entry and retrieval transactions in a number of industries, including banking, airlines, mail order, supermarkets, and manufacturers.

3.1.3.10 Document Management Server

A server which stores metadata concerning documents and supplies one or more document management functions including a library system, document routing, document searching and indexing. More sophisticated Document Management Servers provide support for the management of additional MIME file types.

3.1.3.10.1 Library System

A library system is a subset of a full document management system that emphasizes document access, cataloging, and search capabilities.

3.1.3.10.2 Document Routing

Document routing is a subset of document management focused on the workflow of a document. A routing system tracks the whereabouts of a real or virtual (checked out) document, and automates the handoff of a document from one recipient or process to the next.

3.1.3.10.3 File Sharing

Document management can include simple File Sharing with manual or automated search for document location.

3.1.3.10.4 Search and Indexing Tools

Tools that enable the discovery of data within text files in a library or other document store. At minimum, these tools support keyword and Boolean keyword searches. More sophisticated tools allow searches within structured documents. Indexing tools provide for the automated extraction of keywords and phrases from documents and may be used to generate human searchable indexes such as KICK indexes, or in developing indexes for other search engines.

3.1.3.10.5 Graphic Image Management

Software and standards for managing additional MIME types related to graphic images and other forms of "rich" media in a document management framework.

3.1.3.11 Remote Desktop Server

The server-side software and standards for enabling one or more remote clients to interact with the server as if the client was local to the server, through a GUI or "green screen" interface.

3.1.3.11.1 Microsoft Graphical Desktop Environment

The software and standards required to enable one or more clients to access a Microsoft Windows GUI interface on a remote server.

3.1.3.11.2 UNIX Graphical Desktop Environment

The server-side software and standards required to enable one or more clients to access a GUI interface on a remote UNIX server. X-client is the standard software and protocol suite for accomplishing this.

3.1.3.11.3 Telnet

The server-side software and protocols for allowing one or more clients to establish a telnet or other shell type connection to the server, in a manner that allows them to run, access, or administer applications or data on the server or the server itself.

3.1.4 Data Interchange/Integration Layer

The data interchange and integration layer consists of the set of services, interfaces and protocols that enable the exchange of data among technical services and components. Vendors and the trade press variously refer to the products in this area as "middleware," "enterprise application integration" (EAI) software, "integration software," or, most recently, "integration buses" and "integration platforms." The services are meant to ease the integration of heterogeneous systems at the interface, syntactic, and even semantic levels. These services will be very important to DHS as it transitions from the myriad "legacy" systems to a more uniform target technical environment.

3.1.4.1 Inter-Application Services

Enterprise Applications are complex, scalable, distributed, component-based and mission-critical business applications. Enterprise Applications may be deployed on heterogeneous platforms across enterprise intranet, extranet, and the Internet. They are data-centric and have Web-based interfaces.

This Tier maps to the FEA TRM Service Interface and Integration Category.

3.1.4.1.1 EAI Broker

Integration broker is a Web service-based middleware that move data from a source system or service to a destination system or service, and possibly transform it, based on routing rules. A broker may move data between internal systems or to and from external systems. Integration Brokers use hub-spoke based frameworks to integrate information efficiently and effectively. The communication between integration broker and applications is in the form of messages.

3.1.4.1.2 EAI Server

An Enterprise Application tool that integrates core business systems with multiple internal and external applications. The EAI Server supports the integration process, integration operational environment, and minimal programming during integration.

3.1.4.1.3 EAI Adaptors

Software connecting two applications that were not originally designed to communicate with each other. Integration Adapters include service adapter and event adapter. Server adapter responds to message request and invokes a specific function in the underlying Enterprise information system (EIS). Event adapter propagates information from EIS to application server. The request and repose messages are in standard XML format.

3.1.4.1.4 Geospatial Information Broker

A key component used in moving geospatial data between systems. Involved in data sharing and collaboration operations in support of the COP and MSOP. Involved in Geospatial Data Rollup (GDR) Operations.

3.1.4.2 Web Services

Web Services is a Web-based service that facilitates communications between software applications in a data language. The communications of Web services are implemented in standard Internet protocols, such as HTML, SMTP, FTP; XML for data tagging, WSDL for meta-data format, SOAP for data access, UDDI for service discovery are Web Services components.

This Tier maps to the FEA TRM Service Interface and Integration Category.

3.1.4.2.1 Service Discovery

Service Discovery is a process for organizations to find each others to conduct business. Universal Description, Discovery, and Integration (UDDI) is the standard protocol for service discovery.

3.1.4.2.2 Service Access

Service Access is the interface to access Web services. Simple Object Access Protocol is the standard protocol. Service access should be platform, and transport protocol independent.

3.1.4.2.3 Service Description

The capabilities required to describe accurately and fully a web service in a format that enables internal and external consumers to consume the information and determine if the web service fulfills their requirements.

3.1.4.2.4 Service Inspection

The capabilities required to determine if the web service is functioning correctly.

3.1.4.2.5 Service Publishing

The capabilities required to post the description of a web service to a centralized repository in a format that allows internal and external consumers to access and use the web service.

3.1.4.2.6 Service Security

The capabilities required to ensure that the web service is used in a secure manner, and that messages passing between entities as part of the web service are secure.

3.1.4.2.7 Service Semantic Interoperability

Fully autonomous service interoperability is only possible when clients can locate and access services on-the-fly through publish-find-bind-orchestration patterns that subscribe to well-known service semantics. In particular, the semantics of the request-response message pairs must be well-known between client and service. A Service Information Model (SIM) is required as a general container model for the common semantic framework associated with service description and access.

Service semantic interoperability is made possible by having each Community of Interest (COI) develop standards for the semantics of shared services. Standards are needed for: 1) Service Parameter Dictionaries, which are exposed through registry services, and 2) Semantic Service Profiles (SSP), which define the common semantic framework associated with service description, choreography and orchestration, and also are exposed through registry services. This supports autonomous publish-find-bind-orchestration operations through Geospatial Semantic Services.

Further, within the domain of geospatial, the semantics of each service interface must be well-known. Thus, each geospatial service component must have a well-known, published SIM and SSP Profile. This supports autonomous publish-find-bind operations through Geospatial Semantic Services.

3.1.4.3 Inter-application Messaging Services

Messages are specially formatted data exchanged between applications. Messaging service is the process of client-program exchange messages with a messaging server. Messaging service can either be point-to-point or publish/subscribe. Messaging is asynchronous. Heterogeneous programs, written in different languages, running on different platforms, can communicate through messaging server via common messaging format and protocol.

This Tier maps to the FEA TRM Component Framework Data Interchange Category.

3.1.4.3.1 Message Broker

A Message Broker is a middleware program that translates a message from the sender's formally defined message format to the receiver's formally defined message format. A Message Broker may perform message routing and may utilize Message-oriented Middleware.

3.1.4.3.2 Message-oriented Middleware

Message-oriented middleware (MOM) is software that resides in both portions of a client/server architecture and typically supports asynchronous calls between the client and server applications.

Message queues provide temporary storage when the destination program is busy or not connected.

3.1.4.3.3 Location Based Messaging Broker

The means to support routing and processing (e.g., translation) of location-based messages (messages with embedded geospatial elements). Location-based messages include alerts, after action reports, warnings, emergency declarations, location reports, situation reports and NSSE Reports.

The Location Organize Folder (LOF) is a standard message container model for capturing multi-media data in a geospatial context. It is based upon eXtensible Markup Language (XML) and Geography Markup Language (GML).

3.1.4.3.4 Electronic Data Interchange (EDI)

The EDI is a set of published and standardized formats in exchange of business data among networked computers. The EDI prescribe the formats, character sets, and the data elements used in business documents, such as purchase orders and invoices. The EDI standard is technology independent. An EDI document can be transmitted via dial-up modem, or Internet. The format of EDI document enables same data on paper and in electronic form. An EDI Gateway provides an interface to legacy value-added EDI networks.

3.1.4.3.5 Electronic Funds Transfer

Electronic Funds Transfer (EFT) (also Electronic Money or Digital Money) is form of cash or transactions over computer networks in a secure and trust worth manner. It sometimes refers to the technologies such as cryptography, enabled the form of cash or transaction.

3.1.4.4 Data Exchange/Delivery

This Tier maps to the FEA TRM Component Framework Data Interchange Category.

3.1.4.4.1 Wireless Data Exchange/Delivery

This category defines standards and protocols for exchange and delivery of data in the wireless environment.

3.1.4.4.2 Structured Data Tagging

Structured Data Tagging is a way to associate a data item with data's property in a hierarchical categorization. XML is a standard structured data tagging language. Data tagging facilitates information sharing among applications in an internet Web services environment.

GML is the standard language for representing geospatial data over the Internet.

3.1.4.4.3 File Transfer

The following standard types are applicable to this layer. This is a minimum set and is responsive to the standards specified in the FEA TRM.

- Data Transformation
- Data Format

Should support the means to transfer geospatial data in well-known data exchange formats, and transform these data, if necessary.

3.1.4.4.4 Data Semantic Interoperability

Open, robust data interoperability is only possible when clients can locate and access data on-the-fly through publish-find patterns that subscribe to well-known data semantics. In particular, the semantics of geospatial metadata and data must be well-known between client and data access service.

Data semantic interoperability is made possible by having each COI develop standards for the semantics of data they share. Standards are needed for: 1) Data Dictionaries, which are exposed through registry services, and 2) Semantic Data Profiles (SDP), which define the common semantic framework associated with data description and access, and also are exposed through registry services. This supports autonomous publish-find operations through Geospatial Semantic Services.

3.1.4.5 Business Process management

The capabilities required to monitor and manage the current state of a business process and elements within the process as well as to monitor and manage the health and efficacy of the process as a whole.

3.1.4.5.1 Workflow

The tools, protocols and software necessary to manage the transfer of data between defined roles in a business process, require those actors to act according to those roles, and pass the data on to the next actor in accordance with rules defining the business process.

This should support the means to invoke, monitor, and report on workflows that involve geospatial applications and services.

3.1.4.5.2 Business Activity Monitoring

The tools, protocols, and software required to monitor the current state, health, and/or efficacy of a business activity or business process.

This should support the means to invoke, monitor, and report on workflows that involve geospatial applications and services.

3.1.4.6 Semantic Interoperability Services

Fully autonomous business, service and data interoperability is only possible when clients can locate and access business, service and data on-the-fly through publish-find-bind-orchestration patterns supported by services that utilize well-known business, service and data semantics.

3.1.5 Data Management Layer

The data management layer is concerned with defining, logically storing, and retrieving data in all forms: structured, unstructured and semi-structured. Physical data storage is part of the Platform Services tier.

3.1.5.1 Enterprise Reporting Tools

Enterprise Reporting Tools support the capability of accessing all of the information assets in the enterprise to allow the enterprise to gain a better understanding of its business by putting critical information in the hands of all those who need it – employees, managers, partners, and customers.

3.1.5.1.1 Report Generator

A Report Generator enables specification of report format, retrieval of data into the report from a data source, and display and print of the formatted report.

3.1.5.2 Data Access Services

Data Access Service is middleware designed to provide direct access to enterprise data regardless location and format of data. The SQL is an accepted industry standard data access interface to relational databases or other databases. The data access service consists of client, data server, and Data Management System Interface (DMSI). Open Database Connectivity (ODBC) is widely used client interface.

This Tier maps to the FEA TRM Service Interface and Integration Category.

3.1.5.2.1 Database Access Middleware

Software and standards that provide uniform or simplified access to data stored in a variety of repositories through a standard interface.

3.1.5.2.2 Digital Rights Management

Digital Rights Management Services provide secure, managed access to geospatial data provided by private providers/stewards for mission-critical HLS business activities. This is crucial for operations that involve Critical Infrastructure and Key Assets.

3.1.5.2.3 Gazeteer Service

The Gazetteer Service is able to access a Gazetteer, which is a directory of well-known places and their locations. It generally consists of point features. A Gazetteer Service is a network-accessible service that retrieves one or more features, given a query (filter) request. This filter request must support selection by well-known feature properties. Queryable feature properties include, but are not limited to, feature type, feature name, authority, or identification code. Each instance of a Gazetteer Service has an associated vocabulary of identifiers. Thus, a Gazetteer Service may apply to a given region, such as a country, or some other specialized grouping of features. The returned features will include one or more geometries expressed in a well-known Coordinate Reference System.

3.1.5.2.4 Web Map Service

A Web Map Service (WMS) is able to access vector and raster data and render it in the form of a map for display (combines access and portrayal). Independent of whether the underlying data are features (point, line and polygon) or coverages (such as gridded digital terrain model or images), the WMS produces an image of the data that can be directly viewed in a web browser or other picture-viewing software. A WMS labels its data as one or more “Layers,” each which is

available in one or more “Styles.” Upon request a WMS makes an image of the requested Layer(s), in either the specified or default rendering Style(s). Typical output formats include Portable Network Graphics (PNG), Graphics Interchange Format (GIF), Joint Photographic Expert Group format (JPEG), and Tagged Image File Format (TIFF).

3.1.5.2.5 Web Coverage Service

Able to access geospatial coverage data (e.g. imagery and DTM). The WCS supports the networked interchange of geospatial data as “coverages” containing values or properties of geographic locations. Unlike the Web Map Service, which filters and portrays spatial data to return static maps (server-rendered as pictures), the Web Coverage Service provides access to intact (unrendered) geospatial information, as needed for client-side rendering, multi-valued coverages (such as multi-spectral images and terrain models), and input into scientific models and other clients beyond simple viewers.

3.1.5.2.6 Web Feature Service

The Web Feature Service (WFS) supports the query and discovery of geographic features (represented in vector form). In a typical Web access scenario, WFS delivers GML representations of geospatial features. Clients (service requestors/consumers) access geographic feature data through a WFS by submitting a query for just those features that are needed for an application. The client generates a request and posts it to a WFS server on the Web. The WFS instance executes the request, returning the resulting geographic features to the client encoded in GML. A GML-enabled client can manipulate or operate on the returned geographic features.

3.1.5.2.7 Web Terrain Service (WTS)

The WTS extends the WMS interface to allow the access and portrayal of three dimensional geospatial data. This service can be exploited to perform tasks such as terrain analysis, mission planning, and fly-throughs.

3.1.5.2.8 (Location) Directory Service

The (Location) Directory Service provides access to online directories of persons, places, products and/or services (e.g., Yellow/White/Green/Blue Pages, Restaurant/Travel/Entertainment Guides, Community Services, etc). This service is ordinarily used to find the location of a *specific* or *nearest* person, place, product and/or service. It is an important service used in LBS.

3.1.5.2.9 Image Archive Service

The Image Archive Service accesses archived images. It makes use of WCS (see 3.1.5.2.5) and Image Catalog Service (see 3.1.5.3.1).

3.1.5.2.10 Web Annotation Service

The Web Annotation Service is a specialized WFS that accesses map/image annotations. It is based upon the XML for Image and Map Annotation (XIMA), which defines an XML vocabulary to encode annotations on imagery, maps, and other geospatial data. This vocabulary draws on the GML to express the positions of these annotations in geographic (real world) or

image-pixel coordinates, and to associate each annotation with the geospatial resource(s) it describes. The XIMA encoding is useful for any activity that requires linking or tagging geospatial data in order to present and discuss it with others, to make joint decisions, or to communicate spatially.

3.1.5.3 Data Cataloguing and Registration Services

This technical component contains the functions required to record and describe the attributes of a data set, and expose that data set for use by other programs.

3.1.5.3.1 Web Registry Service

The Web Registry Service (WRS) provides a common mechanism to classify, register, describe, search, maintain and access information about geospatial *resources* available on a network. Resources are network addressable instances of typed data or services. Types of registries are differentiated by their role such as registries for cataloging geospatial resource types (e.g., types of geographic features, coverages, sensors, symbols, services, etc), online data instances (e.g., geospatial and image datasets and repositories, application schema, and symbol-style libraries), and online instances of services.

3.1.5.3.2 Catalog Service

The Catalog Service defines common information models and standard operations that allow applications and services to interact with registry instances, regardless of their role or content, in order to discover, access and manage geospatial resources (data and services). Specialized Catalog Services may exist for specific data classes, e.g., an Image Catalog Service (ICS).

3.1.5.4 Metadata Management Services

The software and standards for accessing, modifying, organizing and indexing metadata. This can include managing multiple metadata formats, integrity and security rules, and managing the metadata's location within a distributed system. Metadata services also enable end users/applications to define and obtain data that are available in the database.

3.1.5.5 Data Query Tools

Query tools are a category of tools capable of generating ad hoc queries to a database and dealing with the resultant output. The simplest tools in this category are simply command line style tools capable of sending SQL queries to a database engine. Higher-level tools use wizards or graphical interfaces and diagramming tools to construct queries.

This Tier maps to the FEA TRM Service Interface and Integration Category.

(See Geospatial Data Access above)

3.1.5.5.1 Spatial Query

Spatial Query provides the service to query, analyze, and map data in support of decision-making.

3.1.5.5.2 Non-Spatial Query

A Non-Spatial is a query that does not include the use of spatial data or map data.

3.1.5.6 Data Transformation Services

A data transform service (DTS) provides mechanisms to transform data from disparate data into meaningful information. Transformations may be accomplished in real- or near-real time or may be done off-line or in the background using extract/transform/load products. In addition to providing integration services, this type of service is also used to extract operational data and populate operational data stores, data marts and data warehoused for decision support and other analytical purposes.

This Tier maps to the FEA TRM Service Interface and Integration Interoperability Category.

3.1.5.6.1 Coordinate (and Unit) Transformation Service (CTS)

The ability to transform geospatial data between different coordinate reference systems, datums and units. Support map re-projections on-the-fly for map viewing, as well as permanent coordinate transformations that result in a transformed output data set.

3.1.5.6.2 Geospatial Data Exchange and Transformation Services

The ability to import/export, manipulate and convert geospatial data, through standard data exchange and transformation services. Formats include GML, MapInfo, ESRI, Intergraph, etc

3.1.5.6.3 Topology Service

The ability to detect topology errors (e.g., overshoots and undershoots of common linear and polygonal features within a definable tolerance), automatically correct errors, if possible, and define topological relationships between connected/collocated linear, polygon, and point features.

3.1.5.6.4 ETL

Software and standards for extracting data from one data source, transforming it into another format and loading it into a target data source.

3.1.5.7 Database Management System (DBMS)

A DBMS is a suit of software programs designed to manage a database; it serves as an interface between database users and database, carrying out users commands to database and deliver feedbacks from database to users.

This Tier maps to the FEA TRM Service Interface and Integration Category.

3.1.5.7.1 Enterprise DBMS Mainframe

Very large scale DBMS implemented on a traditional mainframe (IBM compatible) platform.

3.1.5.7.2 Enterprise DBMS UNIX

Very large scale DBMS implemented on a Unix OS platform.

3.1.5.7.3 Departmental UNIX DBMS

A small to medium scale DBMS implemented on a UNIX or Linux Operating System.

3.1.5.7.4 Enterprise x86 Server DBMS

Large scale DBMS implemented on the Windows Operating System.

3.1.5.7.5 Departmental x86 Server DBMS

A small to medium scale DBMS implemented on the Windows Operating System.

3.1.5.7.6 Non Relational

Any non-relational data base management system

3.1.5.7.7 Native Spatial DBMS

The Enterprise DBMS should provide native support for storing and managing all types of geospatial data. Capabilities should include geospatial indexing, open SQL query support with geometry and topology operators, geospatial analytics, geospatial data mining, coordinate transformation and linear referencing.

3.1.5.8 Data Formats

This Tier consists of formats for storage and transmission of enterprise data.

This Tier maps to the FEA TRM Service Interface and Integration Category.

3.1.5.8.1 Audio Format

Data formats for audio information

3.1.5.8.2 Computer Graphics Format

Digital image formats.

3.1.5.8.3 Calendar Format

The specification and format for the transmission of calendar information, particularly from one calendar agent to another in a groupware application or between groupware applications.

3.1.5.8.4 Print Format

Specifications, languages and formats for communicating with printers.

3.1.5.8.5 Symbology Format

The format and specifications for the creation of barcodes and map graphics.

3.1.5.8.6 Time Format

The format and specifications for the encoding and transmission of time data, particularly across a network.

3.1.5.8.7 Video Format

Formats and specifications for the encoding, storage and playback of video information.

3.1.5.8.8 Voice Over IP Format

The format(s) for transmitting voice conversations, especially using a telephone or telephone-like device, over an IP network.

3.1.5.8.9 Message Format

The formats and specifications for transmitting messages between applications.

3.1.5.8.10 Geospatial Data Format

Data formats for the storage, retrieval, and use of geographic information and geographic information data sets.

3.1.5.8.11 XML Schema

An XML DTD which defines the acceptable format, tags, and structure of an XML document for a subject area.

3.1.5.8.12 Wireless Format

A data format which is optimized for transmission to broadband and narrowband wireless devices. These formats are often characterized by extensive use of error checking and correction.

3.1.5.9 Data Models

This Tier consists of the standard data models that support the interoperable exchange of data.

3.1.5.9.1 Simple Features

A standard model that supports storage, retrieval, query and update of simple geospatial features. A simple feature may have both geospatial and non-geospatial attributes.

3.1.5.9.2 Coverages

A standard schema that supports storage, retrieval, query and update of coverage data. Must handle a wide range of imagery and grid data from raw to thematically classified image/grid coverages.

3.1.5.9.3 Registry Information Model

The RIM provides a blueprint or high-level schema for the content associated with the Catalog/Registry Service. It specifies the type of metadata that is stored in the registry as well as the relationships among metadata Classes. The Registry Information Model defines what types of objects are stored in the Registry and how stored objects are organized in the Registry.

3.1.5.9.4 Service Information Model (SIM)

The content model for describing Geospatial Web Services. Shares many capabilities and characteristics of more generally defined Web Services, but also has features unique to geospatial needs. SIM defines the semantics and structure for packaging metadata about services necessary for a client to make use of (i.e., "consume") a service. SIM is a vocabulary comprised of several parts for describing different aspects of a service.

3.1.5.9.5 Observations & Measurements

The content models and encodings for observations and measurements made by sensors or humans. Expressed in GML.

3.1.5.9.6 Sensor Model Language (SensorML)

SensorML provides a schema for defining the geometric, dynamic, and observational characteristics of a sensor. Sensors are devices for the measurement of physical quantities. The purpose of SensorML is to encode general sensor information in support of data discovery, support the processing and analysis of the sensor measurements, support the geolocation of the measured data, provide performance characteristics (e.g. accuracy, threshold, etc.), and archive fundamental properties and assumptions regarding sensor.

3.1.5.10 Data Encoding

The means to encode data in standard interoperable structures and schema.

3.1.5.10.1 Geography Markup Language

The Geography Markup Language (GML) is an XML encoding for the transport and storage of geographic information, including the geometric, topologic and other schema-specific properties of geographic features. Supports the ability to handle complex properties. The means to represent geospatial data expressed as any Geospatial Entity Type or collection of types, including Location, Feature, Coverage, Route, Observation, Structure and Mobile Object.

3.1.5.10.2 Observations and Measurements Language

The means for encoding observations and measurements made by sensors or humans.

3.1.5.10.3 Sensor Model Language

The means for encoding sensor parameters.

3.2 Service Platforms Tier

3.2.1 Computing Platform Layer

The computing platform layer includes the hardware and software, both specialized and general purpose, which enables the technical services and components in the layers of the Services Framework. Computing platforms are application and service-neutral configurations of computer and peripheral hardware and operating system software. "Servers" and "Services" of the various types described in the document are hosted on these platforms.

3.2.1.1 Operating System

An operating system provides a set of basic software services needed to host applications, servers and services. An operating system schedules tasks, manages memory, handles the interface to peripheral hardware, and presents an interface to user. Operating Systems may be dependent on specific computer hardware or may be capable of being used on a wide range of computer hardware from different vendors.

This Tier maps to the FEA TRM Service Platform and Infrastructure Hardware/Infrastructure Category.

3.2.1.1.1 Mainframe Enterprise Server OS

A Mainframe OS is generally a proprietary operating system that controls multiple user processes in one or more Central Processing Units (CPU). A Mainframe OS is characterized by support of large numbers of processes and extremely high input/output bandwidth..

3.2.1.1.2 Unix Enterprise Server Clustering

Unix is a proprietary but open source operating system utilized on a wide range of hardware platforms. Unix High performance computing in the Unix environment may be obtained by clustering multiple computer systems on a high speed network, allocating processes and sharing virtual memory and other resources among systems and processes. Both proprietary, hardware vendor specific, and open, OS specific solutions exist and are included in this category.

3.2.1.1.3 Unix Enterprise Server OS

High-end Unix Enterprise Servers generally are based on proprietary hardware and utilize a manufacturer specific Unix OS with extensions to support data center management, manufacturer specific multiprocessor support, etc. A Unix OS supports one or more sets of standard interfaces; Government owned systems are generally required to support the Portable Operating System Interface (POSIX) standard. Open source Unix OS flavors (including Linux) are just beginning to be utilized in this area.

3.2.1.1.4 Unix Departmental OS

Unix Departmental Servers generally are based on proprietary hardware and may require a manufacturer specific Unix variety. Open source Unix OS flavors (including Linux and BSD flavors) are also widely utilized in this area.

3.2.1.1.5 x86 Enterprise Server OS

An operating system, using a x86 processor architecture, which is deployed to support a large number of users, who may be contained within one organizational unit, but which typically span multiple organizational units.

3.2.1.1.6 x86 Departmental Server OS

x86 Departmental Servers as a class are based on generic x86 (Intel, Advanced Micro Devices (AMD) or similar processor family) hardware and as such may utilize a proprietary or open source Unix OS flavor (including Linux and BSD flavors) or other proprietary server OS (including Windows Server OS). x86 Servers are typically utilized on LANs and may support specific features of a Network Operating System (NOS).

3.2.1.1.7 Desktop OS

The operating software for a standalone PC, such as an IBM Compatible PC, UNIX or Mac desktop, notebook or laptop.

3.2.1.1.8 Handheld OS

The operating software for a handheld standalone computing device, such as a Palm or a Microsoft Pocket PDA (personal digital assistant).

3.2.1.1.9 Wireless Platform OS

The operating system for devices for which the primary mode of communication is intended to be via a broadband or narrowband wireless, typically non-IP, network. These devices are usually designed to be portable and have limited processing and battery power.

3.2.1.2 Computer Hardware

Computer hardware consists of the physical computer equipment that runs the software required to provide services. Those equipments include CPU, main memory, storage, and input/output devices.

This Tier maps to the FEA TRM Service Platform and Infrastructure Hardware/Infrastructure Category.

3.2.1.2.1 Mainframe Enterprise Server

A Mainframe Enterprise Server is the highest capacity category of computer used by an enterprise. Salient characteristics are massive internal memory, high-capacity external storage, fast high-throughput I/O, high reliability, and high-quality technical support. Mainframes are typically fully proprietary in hardware and in operating software. A Mainframe Enterprise Server may employ enterprise level storage architectures, which may be shared across a data center among both mainframe and Unix servers.

3.2.1.2.2 UNIX Enterprise Server

A Unix Enterprise Server is typically characterized by proprietary hardware and open software. An Enterprise Server is typically operated in a data center by dedicated operators and administrators utilizing high level management and support tools. Data center servers are typically the most reliable category of server and provide services based on SLAs. A Mainframe Enterprise Server may employ enterprise level storage architectures, which may be shared across a data center among both mainframe and Unix servers.

3.2.1.2.3 UNIX Departmental Server

A Unix Departmental Server is typically characterized by use of open system software (this may include Linux). Hardware may be proprietary or generic x86 architecture. Typical use is as an application or Web server. A Departmental Server is typically operated in a local office by operators with other collateral responsibilities. A Departmental Server may be locally administered or may be subject to remote administration. Departmental servers are typically controlled by and responsive to local management.

3.2.1.2.4 x86 Enterprise Server

A high-end server which uses processors based on the x86 architecture. These servers contain multiple processors, typically four or more, are quite fault tolerant, and usually host large, multi-user applications.

3.2.1.2.5 x86 Departmental Server

An x86 Departmental server is characterized by generic x86 hardware and Windows server software. Typical use is as a file and print server. An x86 Departmental Server is typically operated in a local office by operators with other collateral responsibilities. A Departmental Server may be locally administered or may be subject to remote administration. Departmental servers are typically controlled by and responsive to local management.

3.2.1.2.6 CAD/3D/Virtual Reality Workstation

A CAD Workstation is a high-end proprietary or x86 based workstation used for Computer Aided Design tasks. CAD workstations may be UNIX or Windows based and typically are characterized by large memory, multiple large screen video, and special input and output devices such as tablets and plotters.

3.2.1.2.7 Geospatial Processing Workstation

A Geospatial Processing Workstation is a high-end workstation dedicated to GIS, Image Processing and other demanding geospatial processing tasks. Geospatial Processing workstations may be Unix or Windows based. They typically are characterized by large memory, large screen video, and massive disk storage.

3.2.1.2.8 Scientific Workstation

A Scientific Workstation is a high-end proprietary or x86 based workstation dedicated to analysis tasks. Scientific workstations may be Unix or Windows based. They typically are characterized by multiple processors, large memory, large screen video, and massive disk storage. Scientific workstations are typically used on multiple tasks..

3.2.1.2.9 Desktop Computer

A Desktop Computer or personal workstation is a computer small enough to fit on top of a office desk. In the DHS environment, this is an x86 architecture device. A desktop computer normally participates on a LAN, sharing resources on LAN servers. A desktop computer may also support standard local devices through standard interfaces.

3.2.1.2.10 Laptop Computer

A laptop computer is a computer that can be fit into a suitcase and carried around during traveling. It has a bulletin display and is powered by battery and AC. May have built in peripheral devices, such as CD-ROM drive, keyboard, trackball or touch pad, internal modem, wired wireless network interface card, USB interface, serial interface, and etc. In the DHS environment this is typically

3.2.1.2.11 Tablet Computer

A tablet computer is a personal computer that has an input method of either handwriting with a stylus or a foldable keyboard. The intention of the tablet computer is to use it as user's primary computer and note taking tool.

3.2.1.2.12 Handheld Computer

A handheld computer is a computer that can conveniently be stored in a pocket and used while the user is holding it. Wireless Mobile Hardware

3.2.1.2.13 Wireless Mobile Hardware

Wireless Mobile Hardware is hardware with a mobile application and wireless platform.

3.2.1.2.14 Graphics Workstation

A graphics workstation is a computer which is optimized for the editing of multiple types of media, particularly graphic images. These computers are characterized by large amounts of RAM, large screens for graphic editing, and often use alternative input devices, such as drawing tablets, for image editing.

3.2.1.3 Enterprise Storage

A storage system is a combination of software and hardware being tailed and specialized to disk storage management and to the storage demands of multiple hosts in order to enhance reliability availability, scalability and performance.

This Tier maps to the FEA TRM Service Platform and Infrastructure Database/Storage Category.

3.2.1.3.1 File System

A file system is a component of an operating system that defines the way that files are named, stored, retrieved, organized, and located. File system often uses hierarchical directory to organize files and uses path to locate files.

A file server provides for the physical storage of data in a file system. A file system is an element of an operating system and may be local to an instance of that operating system or may be distributed across multiple instances of like or dissimilar operating systems. Distributed file systems such as the Network File System (NFS) and the Common Internet File System (CIFS) are examples.

3.2.1.3.2 Network Attached Storage

Network Attached Storage (NAS) systems are dedicated filer servers that attach to local area networks as would a traditional file server using a general purpose operating system. Users access storage devices via network access. It is in contrast to server attached storage devices, NAS does not have the overhead imposed by server and it's operating system. Thus NAS has better performance than traditional server attached storage.

3.2.1.3.3 Storage Area Network

Storage Area Network (SAN) is a storage system architecture that high-speed subnetwork links together shared storage devices. All storage devices in a SAN are visible to all server in a WAN

or LAN. This architecture separates function of running business application and and function of accessing storage devices, and locate them in server and SAN respectively. There better performance is achieved by server and storage device. SANs include various forms of high-speed connectivity to computing platforms as well as isolated, very high-speed backend networks to move data between storage devices. SANs provide the ability to replicate data across physical devices and to move data to near-line and archival storage independent of compute platforms.

3.2.1.3.4 DASD Direct Attached

The hardware and protocols for creating an externally powered disk storage array and for directly attaching the array to a server.

3.2.1.3.5 Tape Direct Attached

The hardware and standards for devices which store digital data on a magnetic tape and which are directly attached to a server. These devices are characterized by accessing a limited number of tapes and having a relatively limited number to tape drives with which to access stored data.

3.2.1.3.6 Tape Silo

The hardware and standards for devices which provide automated access to multiple (typically a very large number) tape spools or cassettes and is usually attached to a network. This category includes very large capacity systems (silos).

3.2.1.4 Shared Special Purpose Hardware

Special purpose equipment is generally completely contained functional hardware (and software) device that has some embedded computing capabilities, but is not meant for general purpose computing tasks as designed. Common examples of these types of devices include printing and plotting devices, Global Positioning System devices, and the new generation of cell phones and PDAs such as Blackberry RIM and the Palm Pilot. More esoteric examples for these types of devices could include Point of Sale terminals, time tracking equipment etc.

This Tier maps to the FEA TRM Service Platform and Infrastructure Hardware/Infrastructure Category.

3.2.1.4.1 Card Production Device

Many DHS organizations issue identification or access credentials in card form. High volume personalization of card media is performed at government and contractor facilities on special purpose devices that interface to the DHS network.

3.2.1.4.2 Bulk Scanner

High capacity document scanners are employed to convert paper source documents to digital form for processing or storage. Bulk scanners are characterized by high speed and automatic document feeders. Bulk scanners may integrate OCR to provide automatic conversion of text to machine-readable form, either as ASCII text or directly complex document formats.

3.2.1.4.3 Shared Plotter

A shared plotter is a device (either attached directly to the LAN, or made available from a server or workstation as a shared device) that plots large diagrams using either a moving pen or another printing device such as an ink jet. Shared Plotters typically support formats and may be either drum or flatbed type devices.

3.2.1.4.4 Large Format Plotter

Large Format Plotter for printing Maps from GIS applications.

3.2.1.4.5 Shared Printer

A shared printer is a device (either attached directly to the LAN, or made available from a server or workstation as a shared device) that prints either on single sheets or on continuous paper. Many technologies are utilized including laser, ink jet, and impact technologies. Shared printers typically are characterized by being controlled and queued by a LAN server print service.

3.2.1.4.6 Color-Separation/Pre-press

The hardware, software, and standards for taking an analog or digital photograph and separating the colors, particularly into masks, which can then be used by a printer to print large quantities of the photograph.

3.2.1.4.7 CD and DVD Production

DHS produces documents and presentations in CR-ROM and DVD formats for internal and external use. CDs and DVDs may be produced in small qualities on individual, workstation attached CD or DVD writers. Volume production requires special purpose hardware, this category includes CD and DVD volume production devices, feeders and label printers and attachers.

3.2.1.4.8 Video Production Equipment

The electronic equipment used to create, edit, format and display videos.

3.2.1.4.9 Shared Fax

In office environments where Facsimile Transmission (FAX) is utilized in the business process, it is convenient to allow users to send and receive FAX from their desktop workstation. In large office environments this can be economically achieved by sharing one or more FAX telephone circuits. This sharing is accomplished by a FAX server that incorporates and shares software and special purpose modem hardware.

3.2.1.5 End User Special Purpose Hardware

Single user hardware which directly or logically attaches to a single user’s desktop, laptop, wireless hardware or PDA.

This Tier maps to the FEA TRM Service Platform and Infrastructure Hardware/Infrastructure Category.

3.2.1.5.1 Network Interface Cards

Network Interface Cards (NIC): Network connection adapter for wired networks.

3.2.1.5.2 Personal Desktop Scanner

A personal desktop scanner is a single user, workstation attached device that converts document pages and images to digital form, either in black and white or in color. This category includes flatbed and handheld type devices.

3.2.1.5.3 LCD Projector

An LCD Projector functions in place of or in addition to a standard workstation or laptop display. It is normally interfaced to a standard monitor port. It functions by projecting an image of the workstation desktop (or other images) on a screen for group viewing. This category includes technologies other than LCD, such as light valve.

3.2.1.5.4 Personal Fax

In office environments where FAX is utilized in the business process, it is convenient to allow users to send and receive FAX from their desktop workstation. In small office environments this may be achieved use of a directly connected FAX modem that may be used with special purpose software or with standard Windows OS drivers.

3.2.1.5.5 Cellular Telephone

Standard cellular telephones may participate within the enterprise environment as voice mail clients. Many standard cellular phones also support Short Message Service (SMS) that may send and receive messages via the e-mail environment.

3.2.1.5.6 Enhanced Cellular Phones

Most cellular phone networks now support Web browsing services. Enhanced data access services are covered by this category.

3.2.1.5.7 Advance Cellular Telephone

Video, collaboration and other advanced features are also becoming available. This category covers still and motion video and collaborative environment features.

3.2.1.5.8 Digital Encrypted Radio

Special hardware can communicate wirelessly using digital modulation and the transmissions of which are encrypted.

3.2.1.5.9 Digital Non-Encrypted Radio

A radio which uses digital modulation but which, by itself, is not capable of encrypting its transmissions.

3.2.1.5.10 Analog Encrypted Radio

A radio which uses analog modulation but which is capable of encrypting its transmissions.

3.2.1.5.11 Analog Non-Encrypted Radio

A radio which uses analog modulation but which, by itself, is not capable of encrypting its transmission.

3.2.1.5.12 Removable Storage

A storage device designed to be easily removable and transportable from one computer to another. Examples of these devices include USB "Pen" Drives, and removable hard drives in a specialized drive cage.

3.2.1.5.13 Wireless Device Storage

Wireless devices use many of the same storage technologies as desktop and laptop computers. The distinguishing factor is normally size and power consumption. This category specifies standards and products particular to the wireless environment.

3.2.1.5.14 Desktop Plotter

A desktop plotter is a non-shared plotter that is typically smaller than a shared plotter but utilizing similar technologies.

3.2.1.5.15 Desktop Scanner

A desktop scanner is typically a single user device, not shared on the network and not equipped with a feeder or automatic OCR capability.

3.2.1.5.16 Personal Desktop Printer

A non-shared printer. Typically of lower capacity than a shared plotter but utilizing similar technologies.

3.2.1.5.17 Portable Printer

A non-shared printer specifically designed for use with a laptop computer. May be battery or line current operated, but typically has a very small footprint and very low speed.

3.2.1.5.18 Collaboration Peripherals

This category includes all devices used in support of local or remote collaboration including such devices as electronic whiteboards, but excludes video and telephonic conferencing devices.

3.2.1.5.19 Fingerprint Devices

DHS uses fingerprint readers for purposes of registering and identifying individuals for benefit or enforcement purposes. This category includes devices used with the Automated Biometric Identification System (IDENT) system and other identity applications. It does not include devices used only for biometric authentication of credentials or access control.

3.2.1.5.20 Barcode Reader

A barcode reader is a handheld or stationary input device used to read a one or two dimensional barcode. Barcode readers may directly convert the barcode to a standard digital for or may require host software for pattern recognition and data conversion. DHS uses Barcodes on identity documents and for inventory and document control

3.2.1.5.21 Uninterruptible Power Supply

An Uninterruptible Power Supply (UPS) is a device or system that provides continuous electric power supply to critical equipment that can not shutdown unexpectedly. The UPS is inserted between a power source and the critical equipment to mitigate the effect of temporary power outage.

3.2.1.5.22 Section 508 Assistive Devices

Any auxiliary hardware device utilized to assist the handicapped user in operating IT systems. This could include special input devices, Braille printers, etc.

3.2.1.5.23 Border Security Sensors

Sensor devices utilized at the border that interface directly to the IT environment.

3.2.1.5.24 Global Positioning System Devices

Any device that uses GPS to determine and indicate the position of a person or vehicle.

3.2.1.6 Remote Sensing Hardware

Any hardware that is associated with the acquisition of digital or photographic data acquired remotely using aerial, satellite, or ground based platforms.

This Tier maps to the FEA TRM Service Platform and Infrastructure Hardware/Infrastructure Category.

3.2.1.6.1 Photogrammetric Cameras

Cameras that are specialized for the remote capture and measurement of panchromatic (350-1100 nm) data of the earth's surface. These units are typically mounted on airborne craft and produce photographs that can be transformed into a geo-registered image product using specialized photogrammetric software applications.

3.2.1.6.2 Multi-spectral Scanners

Any device that is specialized for measuring radian energy of the earth's surface using discrete bands of spectral data ranging from the blue to the near-infrared portions of the electromagnetic spectrum.

3.2.1.6.3 Hyper-spectral Scanners

Any device that is specialized for measuring radian energy using contiguous bands of spectral data across a broad range of electromagnetic spectra. The resulting image can be visualized as a 3-dimensional dataset with two spatial and one spectral dimension, which is often referred to as an image cube.

3.2.1.6.4 Light Detection and Ranging (LiDAR)

LiDAR is an active remote sensing system that can be operated in either a profiling or scanning mode using pulses of light to illuminate the terrain. By accurately measuring the round trip travel

time of the laser pulse from the aircraft to the ground, a highly accurate spot elevation can be calculated.

3.2.1.6.5 Synthetic Aperture Radar (SAR)

A microwave instrument that transmits radar pulses very rapidly. In fact, SAR is generally able to transmit several hundred pulses while the platform passes over a particular object. Many backscattered radar responses are therefore obtained for that object, which can be manipulated such that the resulting image looks like the data were obtained from a big, stationary antenna. In general, the synthetic aperture is the distance traveled by the spacecraft while the radar antenna collected information about the object.

3.2.1.6.6 Interferometric SAR (IFSAR)

Interferometric Synthetic Aperture Radar (InSAR) is a technique that enables measurement of very small movements of the earth's surface, as subtle as centimeters or less. The SAR interferometry technique acquires a pair of images from two radar measurements, taken from two marginally displaced coherent observations of the surface. For each pixel corresponding to the same ground area in both images, phase values are differenced to produce an interferogram, which, using the orbit parameters, is subsequently used to produce a Digital Elevation Model.

3.2.1.7 Telephony Equipment

The HLS TRM incorporates all categories of telephone equipment employed by the Department.

This Tier maps to the FEA TRM Service Platform and Infrastructure Hardware/Infrastructure Category..

3.2.1.7.1 H.323 Terminal

A H.323 Terminal is an end-user handset device that provides real-time, two-way voice, video, or data communication in VoIP environment.

3.2.1.7.2 Automatic Call Directors (ACDs)

A telephone facility that manages incoming calls and handles them based on the number called and an associated database of handling instructions.

3.2.1.7.3 VoIP Media Gateway

Media Gateway provides the mapping and translation between IP and telephony networks.

3.2.1.7.4 VoIP Signaling Gateway

Signaling Gateway provides the interworking of the H.323 and SS7 ISUP signaling operation. Signaling Gateway is controlled by Gateway Controller.

3.2.1.7.5 VoIP Media Gateway Controller

Media Gateway controller controls both Media Gateway and Signaling Gateway. It works with H.323 Gatekeeper. It authenticates and monitors network connections.

3.2.1.7.6 Private Branch Exchange (PBX)

A PBX is a telephone switching center owned by companies or organizations and is not owned by a telephone company or a common carrier. A PBX circuit-switches calls between internal users without involvement of public switch telephone network (PSTN); and route calls between internal user and external user into or from PSTN.

3.2.1.7.7 Switch Software

Software for transmitting calls between a VoIP infrastructure and a POTS infrastructure.

3.2.1.7.8 Call Management Unit

The device or service that performs the telephone call management functions, such as call waiting, forwarding, voice mail, etc

3.2.1.7.9 Channel Service Unit

A CSU is provided by the communication carrier to customers who wish to use their own equipment to retime and regenerate the incoming signals. The customer must supply all of the transmit logic, receive logic, and timing recovery in order to use the CSU, whereas a digital service unit DSU performs these functions.

3.2.1.7.10 Conference Bridge

Hardware, software, and protocols for enabling telephone conferencing functionality on telephones which do not have this native capability.

3.2.1.7.11 Distribution Frame

The hardware and standards for constructing a central location for the main hub of a telephony network.

3.2.1.7.12 Fax Server

The FAX server incorporates and shares software and special purpose modem hardware. The shared software to send and receive FAXes from various users is the FAX server software.

In office environments where Facsimile Transmission (FAX) is utilized in the business process, it is convenient to allow users to send and receive FAX from their desktop workstation. In large office environments, this can be economically achieved by sharing one or more FAX telephone circuits.

3.2.1.7.13 Voice Mail

A device or service that allows telephone callers to leave messages for the called party.

3.2.1.7.14 Voice Response Units

VRU is an automated system that plays recorded messages in response to caller's actions, which can include either pressing of touch-tone or uttering of verbal commands. The VRU offer different options and route the call according to caller's inputs.

3.2.1.7.15 Handsets

A multi-line conference phone.

3.2.1.7.16 VoIP Handsets

A VoIP telephone or conferencing phone.

3.2.1.7.17 VoIP Switch

A network switch, which is capable of transmitting power over Ethernet and which supports the provision of quality of service services to connected devices.

3.2.1.8 Security

3.2.1.8.1 Smart Card

A reprogrammable hardware card or token that can store a limited amount of information and transmit this information to a smart card reader. Smart cards typically contain embedded memory and are often used to store digital certificates of biometric authentication data.

3.2.1.8.2 Smart Card Reader

A smart card reader reads from, and optionally writes to, a smart card device. Readers may be contact type or contactless and may incorporate other functions, such as biometric verification.

3.2.1.9 Utilities

Utilities are general purpose applications used for system maintenance, administration, or operation of hardware devices.

3.2.1.9.1 General Utilities

This describes the set of applications that are used for general-purpose system maintenance and administration.

3.2.1.9.2 Peripheral Support

This describes the set of applications, which are necessary to enable a peripheral to operate on a particular type of computer.

3.2.1.10 Position Navigation and Timing (PNT) Technology

Devices that are used to determine and/or use geographic positions and/or navigation data.

3.2.1.10.1 Global Positioning System Devices

Any device that uses the Global Positioning System to determine and indicate the position of a person or vehicle.

3.2.1.11 In-Situ Sensors

Any device that senses its local environment.

3.2.1.11.1 Boarder/Facility Security Sensors

Sensors utilized at the border and facilities that are used to sense intruder threats. Sensors that detect motion, heat, and visual changes.

3.2.1.11.2 Chemical Sensors

Sensors that are used to detect chemical threats.

3.2.1.11.3 Biological Sensors

Sensors that are used to detect biological threats.

3.2.1.11.4 Radiological Sensors

Sensors that are used to detect radiological threats.

3.2.1.11.5 Meteorological Sensors

Sensors that are used to sense weather and air quality conditions.

3.2.1.11.6 Hydrological Sensors

Sensors that are used to sense hydrologic and water quality conditions.

3.2.2 Networking/Communications Layer

The networking/communications layer includes all physical communications devices, media, and the services that enable communication among distributed devices. It provides the IP networks needed to communicate among DHS elements, other Federal organizations, state and local government entities, and the general public. It also provides communications for mobile users that may or may not use IP-based protocols.

Data Communication services provide interconnectivity among applications, systems, and people. This layer is implemented both inside the enterprise (e.g., local area networks) and external to the enterprise (e.g. a public telephone network carrier). Included in this layer are local and wide area data networks, voice networks, video networks, and wireless networks. This layer also includes telephone switches, ACDs (automatic call distribution), network routers and switches, load balancers, firewalls, and network security monitoring systems.

The focus of communications services is on the secure, reliable transport of voice, video or data between endpoints. It includes the protection of information in transit, the protection of communication systems from external disruptions, and response to network issues and incidents.

3.2.2.1 Directory Services

A Directory Service consists of a data store of information concerning the “objects” that comprise the enterprise IT system and the mechanisms to query and maintain that information. The objects contained in the data store typically include information about individual users, groups of users, software modules, services, and the locations and capabilities of IT equipment. The X.500 directory standard is full-scale directory service standard. But most directory service implementation is based on the LDAP, a down sized version of X.500.

This Tier maps to the FEA TRM Service Access and Delivery Service Transport Category.

3.2.2.1.1 Directory Server

A Directory Server is a server that offers directory services, providing information in directory to other applications or users. There can be X.500 directory server and LDAP directory server.

3.2.2.1.2 Meta-directory

Meta-directory is a directory integration tool to connect and join information between data sources, including directories, database, and files. The connection process identifies in real-time the changes in connected data store. The join process is to determine identical data object in two data sources. Also the join process maps schema and object names, filters unwanted information, custom-processes and transforms data. Meta-directory also enable sharing of portions of separate directories in a extranet environment.

3.2.2.1.3 Application Integration

Application Integration describes the process that applications use LDAP program API to operate LDAP commands and access data on LDAP server.

3.2.2.1.4 Directory Federation

Directory Federation is a directory technology that creates real-time directory access to other types of data stores, such as relational databases and file systems. A directory federation software extracts data directly from other data stores using native access methods and passes the data to application that made the request to directory federation software.

3.2.2.1.5 Directory Management

Software tools for set up, administering, maintaining and monitoring of a directory or system of directories.

3.2.2.1.6 Directory Shadowing

Directory Shadowing is a directory service feature that creates one or more copies of an original master directory. Those copies of original directory are called shadow directory. Shadow directory is read-only, and is synchronized with master directory. Directory shadowing contributes to load-balancing and fall-back.

3.2.2.1.7 Directory Security

LDAP data store capability can be used for storing authentication and authorization information. LDAP enabled directory can store access control information, user credentials, pre-shared keys, and digital certificates. Secure Socket Layer (SSL) is the option available for encrypting the link between client and LDAP server.

3.2.2.1.8 Directory Replication

Directory Replication is the process of exactly copying data between directories. The directory replication serves the purpose of geographic distribution of data, load balancing, scalability, and fallback. IETF is creating a standard, Lightweight Directory Update Protocol (LDUP) to be used for directory replication.

3.2.2.1.9 Dynamic IP Services

The software and standards that enable a client to obtain dynamically an IP address, typically from a centralized directory server that keeps a directory associating a client's unique identifier with an IP address.

3.2.2.1.10 Name Services

The software and standards necessary for a client to query a directory server with a name and for the directory to resolve the name to a specific client, application, resource, or other element within the directory.

3.2.2.1.11 Time Services

The software and standards that provide the ability for a client to query and retrieve the current time from the directory server.

3.2.2.1.12 Directory API

The software and standards for application programming interfaces for applications to query, retrieve, update and manage directory information in local or remote directories.

3.2.2.1.13 Directory Information Exchange

The software and standards for exchanging information between one or more separate directories. This is different from replication in that the directories contain different information, may be managed by separate entities, and not all of the data within each directory may be exchanged. Typically only a specific subset of the data within the directory is exchanged.

3.2.2.2 Network Equipment

The physical hardware and standards for this hardware that makes up the infrastructure of a wireless or wired WAN, MAN, or LAN or Personal Area Network and provides connectivity, remote access, and security.

3.2.2.2.1 Hubs, Concentrators, Bridges

This describes the set of hardware devices used to connect together multiple computers, LANs, or subnets, without routing at any of the layers in the OSI model. These devices are marked by the ability of any machine, subnet, or LAN, plugged into such a device to see all of the network traffic transiting the device.

3.2.2.2.2 Switches and Routers

This describes the set of hardware devices which are used to connect multiple computers, LANs, subnets, MANs or WANs. These devices typically provide the ability to route one or more of the layers within the OSI model. These devices are marked by the inability of any connection to hear the traffic of any other connection beyond the traffic which is addressed to it.

3.2.2.2.3 Firewall Appliance

A hardware device which screens, analyzes and blocks incoming traffic according to a set of rules determined by an administrator, typically between secure and less secure networks. A Firewall is a network gateway that controls flow of network traffic between secure and less

secure networks. It can be as simple as filtering traffic according to the traffic's starting and destination address or port number, to as complicated as screening the data the traffic contains. Firewalls typically are capable of analyzing and screening multiple, if not all, layers within the OSI model to determine if the network traffic is dangerous or legitimate.

3.2.2.2.4 VPN/Remote Access Appliance

A hardware device which provides the ability to create a secure connection, over the Internet, between a remote client or location and the VPN/Remote Access Appliance, which is typically used to allow the client to access resources inside of the firewall. VPN/Remote Access functionality is often combined with Firewall functionality as part of a combination VPN/Firewall appliance.

3.2.2.2.5 Secure Socket Layer Appliance

A hardware device designed for the management and acceleration of SSL connections between one or more servers and multiple client devices. The SSL appliance handles the encryption and decryption of SSL encrypted traffic between the server(s) and clients, as well as the key generation associated with creating an SSL tunnel.

3.2.2.2.6 Traffic Monitoring, Management and Control Appliance (includes Load Balancing appliances)

Hardware devices which monitor and manage and control the type and flow of network traffic over a network. These devices can contain a range of functions including traffic queuing, traffic type (by application) detection and reporting, bandwidth management, and network availability and usage. Additionally these devices may be capable of dynamically distributing load (typically in the form of HTTP requests) across multiple servers, which prevents variation in load from overwhelming a server and enables the usage of cheaper, less capable servers without any degradation in performance.

3.2.2.2.7 WLAN Infrastructure

Wireless access points.

3.2.2.2.8 WLAN Antennas and Accessories

WLAN specific antennas which may be deployed to increase the coverage area for the WLAN access point or to allow one access point to service multiple, disparate areas through the use of remote antennas.

3.2.2.3 Local Area Network

A LAN is a data communications network that covers a short-distance, and uses a fully controlled transmission media, such as Ethernet or Token Ring. A LAN connects personal computers, workstations, data and file servers, printers, and other network devices and enables sharing of services provided by network devices.

3.2.2.3.1 Data Transport Services

Data Transport Services comprise the services provided by, and protocols supported on, the LAN. These include the primary data transport protocols and any out-of-band control, status, or

monitoring signaling. These may typically include high bandwidth file and print service protocols not typically supported on a WAN.

3.2.2.3.2 Video Transport Services

Video Transport Services are those services necessary to deliver specified video content from an originator to a user or an intermediate server. These services encompass the delivery and control protocols for multi-channel broadcast service, on demand service and two-way and conference services. On the LAN, these are likely to include dedicated channels for security and surveillance cameras, and peer-to-peer video services.

3.2.2.3.3 IP Print Management Services

IP Print Management Services provide printing services on the LAN for non-Windows based computer systems.

3.2.2.3.4 Voice Transport Services

The software and protocols necessary to transmit voice data over a local area network.

3.2.2.4 Wide Area Network

A WAN is data communication network that covers long-distance, and often uses shared transmission media, such as Public Switched Telephone Network (PSTN), satellite communication, microwave communication, and etc. WAN technologies function at the physical, the data link, and the network layer of OSI model.

This Tier maps to the FEA TRM Service Access and Delivery Service Transport Category.

3.2.2.4.1 Data Transport Services

Data Transport Services comprise the services provided by, and protocols supported on, the WAN. These include the primary data transport protocols and any out-of-band control, status, or monitoring signaling.

3.2.2.4.2 Video Transport Services

Video Transport Services are those services necessary to deliver specified video content from an originator to a user or an intermediate server. These services encompass the delivery and control protocols for multi-channel broadcast service, on demand service and two-way and conference services.

3.2.2.4.3 Content Delivery Network

Content delivery or “Edge” networks deliver high demand static content by automatically replicating the content at distributed server locations and transparently translating address requests to serve the content from the local server rather than from a central server over the WAN

3.2.2.4.4 Satellite

Satellite services utilize geosynchronous and low altitude satellites to transport data. Satellite services may be utilized as point-to-point links or may incorporate switching. Satellite services are useful in remote areas or when quick setup is required. Latency may limit the usefulness of

satellite in some applications. Transport protocols supported are the same as for terrestrial links, but additional unique control and circuit setup protocols may be required.

3.2.2.4.5 Laser

Laser links may be used for short haul extension of high bandwidth networks in rough terrain or in urban areas. A laser link is inherently line of sight and has security advantages in that it has low dispersion. Laser links incorporate only the transport and data link layers.

3.2.2.4.6 Encrypted Voice Radio on WAN

Various proprietary techniques and protocols may be used to transport encrypted voice signals. These may be used to connect radio base stations for long-range relay of portable voice radio conversations via the WAN.

3.2.2.4.7 Voice Transport Services

The software and protocols necessary to transmit voice data over a wide area network.

3.2.2.5 Remote Access (RA)

The remote access is the ability to access a computer network or a server from the outside of LAN or WAN network. The common remote accesses are dial-up via modem and PSTN line, ISDN line, wireless connection, DSL line, or the Internet. There may be firewall, remote access server, VPN provides security and routing of traffic to proper servers. Remote Access is often used by telecommuters, remote offices, etc. to access enterprise network resources.

This Tier maps to the FEA TRM Service Access and Delivery Service Transport Category.

3.2.2.5.1 RA via Internet

Remote Access connections via the Internet may be enabled and controlled by a Remote Access server that implements access control and IP address translation.

3.2.2.5.2 RA via Dial-Up

Remote Access connections via the Dial-up Network may be enabled and controlled by a Remote Access server that implements modem pooling, modem control, access control and IP address translation. Dial-up RA servers may be used to implement dial-back access control. Remote Access servers may also support non IP services.

3.2.2.5.3 RA via VPN

Remote Access connections over the Internet may be secured by encryption and routing to give the appearance of an extension of a private Intranet. This type of connection is referred to as a Virtual Private Network or VPN. It is enabled and controlled by a Remote Access server that implements encryption, access control for initial connection setup, and IP address translation.

3.2.2.6 Narrowband Wireless Network

A wireless telecommunication network that may carry data, video, or voice information over a limited bandwidth wireless network.

This Tier maps to the FEA TRM Service Access and Delivery Service Transport Category.

3.2.2.6.1 Data Transport Services

Software and protocols specific to data communication over a narrowband wireless data network.

3.2.2.6.2 Video Transport Services

Software and protocols specific to one-way or two-way video streaming over a narrowband wireless data network.

3.2.2.6.3 Voice Transport Services

Software and protocols specific to voice communication over a narrowband wireless data network.

3.2.2.6.4 Switching

The hardware, software and standards for determining the location of a wireless recipient and ensuring that the appropriate data is transmitted by a transmitter in the recipient's location, particularly in order to prevent other transmitters from needing to also transmit this data.

3.2.2.6.5 Relay

The hardware, software and standards for retransmitting a data packet or data stream, especially to a particular recipient who is not in range of the original transmission.

3.2.2.7 Broadband Wireless Network

A wireless telecommunication network that may carry data, video, or voice information over a wireless network with relatively large amount of bandwidth.

3.2.2.7.1 Data Transport Services

Software and protocols specific to data communication over a broadband wireless data network.

3.2.2.7.2 Video Transport Services

Software and protocols specific to one-way or two-way video streaming over a broadband wireless data network.

3.2.2.7.3 Voice Transport Services

Software and protocols specific to voice communication over a broadband wireless data network.

3.2.2.7.4 Site Survey and Management System

The software and hardware necessary to evaluate the suitability of a particular site for placement of a broadband wireless network antenna or tower.

3.2.2.7.5 WWAN/WMAN

Wireless Wide Area Network (WWAN) and Wireless Metro Area Network (WMAN) is the hardware, software, and protocols specific to broadband, point to point, connections between disparate geographic points in a WAN or MAN.

3.2.2.7.6 Wireless Personal Area Network

A Wireless Personal Area Network (WPAN is a short distance wireless network that supports mobile computing devices, such as laptop, PDA, cell phone, set-top box, and other consumer electronic devices, to form a ad hoc network to exchange information. Bluetooth is the widely used WPAN standard.

3.2.2.7.7 Wireless Security

The hardware, software, and protocols specific to providing security over a broadband wireless network

3.2.2.8 Wireless LAN (WLAN)

A WLAN is a network that permits mobile users to connect to a LAN. The IEEE standard 802.11 is the protocol, with 802.11b, 802.11a, 802.11g, and 802.11h variations. Because electromagnetic wave does not have physical protection as wired network do, security is critical to WLAN. The old security protocol, Wired Equivalent Privacy (WEP), has security flaws and can be breached with modest effort. The Wireless Application Protocol (WAP) is more secure protocol, and based on Wireless Markup Language (WML). The Bluetooth is another less used WLAN standard.

This Tier maps to the FEA TRM Service Access and Delivery Service Transport Category.

3.2.2.8.1 WLAN Protocols

Among WLAN protocols, IEEE 802.11 is dated and offers limited bandwidth 2 Mbps; IEEE 802.11b is widely used and offers maximum 10 Mbps bandwidth; IEEE 802.11g is to be finalized and offers 54 Mbps bandwidth. All above protocols use 2.4 GHz radio frequency. IEEE 802.11a offers maximum 54 Mbps bandwidth, and use less crowded 5 GHz radio frequency. It's drawback is that equipment can be more expensive.

3.2.2.8.2 Wireless Security

The most common and failed security mechanism for WLAN is WEP, wired equivalent protection. WLAN security should relay on VPN, wireless gateway, 802.1x compliant products rather than WEP. Wireless gateway provides security control. 802.1x is a port access control protocol as part of 802.11i WLAN protocol.

3.3 Cross Cutting Services

3.3.1 Security Layer

As discussed previously, security services should not be viewed as a "layer" since the desired level of security is achieved by placing security mechanisms at the most appropriate locations in the technical environment. Therefore, specific technical security services and supporting interfaces and protocols exist within each layer of the TRM.

This section of the TRM identifies the *technical* security services that enable the security capabilities identified in the *Security Management* service component of the FEA SRM.

3.3.1.1 Access Control

An access control service enforces end-user and service access to system resources. An object, such as an end user or service executing on behalf of an end user whose identity has been authenticated must also be authorized to access system resources. And Access Control has evolved into enterprise identity management system, which manages user accounts and access privileges at enterprise level with centralized control.

3.3.1.1.1 Identification and Authentication

An authentication is a process to identify and validate a user, a network device, or a computer application. The common authentication method is id and password. The more secure authentication methods PKI certificate, biometrics, and etc.

3.3.1.1.2 Authorization

An authorization is a process of verifying whether a user, a network entity, or an application requesting an action has the privilege to take the action. Authentication shall always precede authorization. Authorization may be facilitated by a database assigned privileges.

3.3.1.1.3 Non-Repudiation

A concept that insures contract agreed over Internet can not be denied by any of the signing parties. The Non-repudiation is achieved by attributing the signature to the holder and only the holder of the private key in asymmetrical key algorithm used in PKI. Non-repudiation is essential in E-Gov. Non-repudiation includes non-repudiation of origin --- a sender cannot deny having sent a message, and non-repudiation of receipt --- a receiver cannot deny having received a message.

3.3.1.1.4 Enterprise Identity Management System (EIMS)

EIMS is an IT infrastructure that centralizes the management of user identity, authentication and authorization information. EIMS should have centralized directory service for user information, should have centralized control and administration of user addition, change, maintenance, and termination into enterprise systems and other access privileges. It can accommodate different security level of authentication methods, from simple password to PKI certificate and to biometrics. EIMS should inherit Single Sign-On at Enterprise level.

3.3.1.1.5 Single Sign-On (SSO)

A SSO is a process that enables a user, network entity, or application to authenticate once to access one network resource and does not have to authenticate for accessing other network resources within the limit of predefined session time.

3.3.1.1.6 Biometrics

In computer security, biometrics refers to an authentication technique that relies on measurable human physical characteristics that can be stored and checked automatically. Finger print is often used in biometrics authentication. Biometrics authentication is among the strongest authentication methods.

3.3.1.1.7 Digital Signature

An electronic method of marking a document in such a manner that the mark can be attributed to one.

3.3.1.1.8 Wireless Access Control

Software and standards specific to authenticating users and computers accessing the network wirelessly.

3.3.1.2 Cryptography

A cryptography service provides the capability to encrypt and decrypt data and is a fundamental technical security service. The algorithms used for encryption and decryption have to be approved by National Institute of Standards and Technology (NIST) for SBU information, approved by National Security Agency (NSA) for classified information. Triple-Data Encryption Standard (DES) and AES (Advanced Encryption Services) are approved for SBU information. Skip-Jack and Two-Fish are approved for classified information encryption.

3.3.1.2.1 Cryptographic Module (CM)

A CM is a set of hardware, software and firmware that implements a set of security functions such as cryptographic algorithms and key generation and is contained in a cryptographic boundary. Smart cards and smart tokens are two kinds of CM

3.3.1.2.2 Symmetric Key Management

Symmetric Key Management Services provide an automated mechanism to exchange encryption "keys" in systems where each encryption end-point is a peer to other end-points. Symmetric keys are changed often to maintain security. That process can be difficult to mange if not automated.

3.3.1.2.3 Secure Hash

Secure Hash is a process of generating one-way message digest from original message and a secret key. Secure Hash is to protect integrity of messages. NIST standard FIPS 180 prescribes that Secure Hash Algorithm (SHA1) is the algorithm of choice to generate secure hash for SBU information.

3.3.1.2.4 Public Key Infrastructure

A Public Key Infrastructure (PKI) provides the mechanisms to store and manage "keys" in the form of digital certificates for purposes of user authentication and user authorization to access system resources. This includes issuing, tracking, and revoking digital keys. PKI is a generic term for a set of integrated key management mechanisms managing public keys. DHS PKI needs to cross-certify with Federal PKI Bridge, which enables validating certificates issued by all participating agencies.

3.3.1.2.5 Key Escrow

The hardware, software, and standards which implement a procedure whereby the encrypted communications between two parties may be decrypted by a third party. This is often used in the

context of government agencies that need to decrypt messages encrypted by other which they suspect to be relevant to national security.

3.3.1.2.6 Steganography

A system of confidential communication whereby the existence of the message is hidden within another object, such as a picture. Stenography is a secret communication where the existence of the message is hidden. Stenography shall have a cover message, such as a picture, an article, etc. In computer forensics, there are software tools that can reveal hidden messages in a picture.

3.3.1.2.7 Internet Cryptographic Applications

There are many internet cryptographic applications. Secure Socket Layer (SSL) or the later version Transaction Layer Security (TLS) are used extensively Web and other network communication; IPS provides encryption at network layer; Secure Shell (SSH-2) enables certificate based secure command line connection; Wireless Application Protocol (WAP) enable secure wireless communication.

3.3.1.2.8 IPSec

Standards and software for encrypting IP layer data using the IPSEC protocol. IPSEC encrypts the data portion of the IP packet, thereby providing transparent security to all the protocols and layers above the IP layer.

3.3.1.2.9 Laptop Encryption

Software and standards specifically for the encryption of data on laptops. This software is often configured to encrypt the entire hard drive so that in the event that the laptop is lost or stolen, no data can be comprised.

3.3.1.2.10 PDA Encryption

The Standards and products of this category will be applied. Software, hardware and standards specifically for the encryption of data on a PDA or other type of handheld device.

3.3.1.2.11 Removable Media Encryption

Software, hardware and standards specifically for the encryption of removable storage devices.

3.3.1.2.12 Wireless Security Encryption

The software, hardware, and standards providing encryption for the communications of wireless, particularly wireless, mobile, handheld devices such as mobile phones, Blackberry, and PDAs. Wireless encryption is differentiated from encryption used for other means due to the limited battery, processing power, and memory of the machines on which it is typically deployed.

3.3.1.3 Operation Security

Operation Security includes identifying the vulnerabilities of and threats to computer operations and formulates and implements security controls for transaction processing, system administration tasks, and external operations. These controls include repair problems and maintain auditing and monitoring processes.

3.3.1.3.1 Control and Protection

Controls are used to protect network resources from threats in the operation environment, from intruders, operators who stepped beyond their privileges. Operation controls include resources protection and user privilege control.

3.3.1.3.2 Audit Trail

A chronological record of system activities and attempted system activities to enable examination, reviewing, and reconstruction of past events to identify when and who did what in where in an information technology environment.

3.3.1.3.3 Vulnerabilities Scanning

A proactive and automated process of identifying the flaws in the configuration of networked devices. The process is conducted by a software and with a databases of known flaws. The software tests the presence of the flaws and generates reports to enable mitigation of those flaws in a network.

3.3.1.3.4 Digital Forensics

The First Digital Forensic Research Workshop defined digital forensic science as "[t]he use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." It includes computer forensics, forensic programming, and network forensics.

3.3.1.3.5 Risk Management

Risk Management is a process of identifying, controlling, mitigating, and eliminating uncertain events that may have detrimental effect on continuation of IT business. Certification and Accreditation is one example of Risk Management.

3.3.1.3.6 Policy Implementation Tools

In conjunction with Identification and Authentication, Policy Implementation Tools implement the business rules associated with role base access.

3.3.1.3.7 Antivirus

Software which identifies, protects against, and can remove computer viruses and worms.

3.3.1.4 Network Security

Network Security includes structures, transmission methods, transport formats, and security mechanisms that provide confidentiality, integrity, availability, and accountability for transmissions over intranet or Internet. It is also to prevent and detect misuse of network resources.

3.3.1.4.1 Network Protocols

Standards for providing authentication, non-repudiation, and/or confidentiality to voice, video or data traffic transmitted across a network.

3.3.1.4.2 Firewalls

A Firewall is a network gateway that controls flow of network traffic between secure and less secure networks. It can be as simple as filtering traffic according to traffics starting and destination address or port number, as complicated as data content the traffic contain. Firewall is often deployed in a Demilitarized Zone that is a small network served as security buffer zone.

3.3.1.4.3 Intrusion Detection and Prevention

An Intrusion Detection Service (IDS) monitors system or network activity in order to detect unauthorized access attempts. These services can detect intrusions is real or near-real time or after the fact, as the result of analysis of stored information. IDS can be host-based to protect a host, or network-based located at entry point of a network. Intrusion prevention is an added service to some IDS systems.

3.3.1.4.4 Boundary Protection Service

A Boundary Protection Service enforces a network security boundary. Components such as security guards, proxies, filters, and firewalls provide boundary protection services. There is a need to create Demilitarized Zone (DMZ) in boundary protection. The new trend is to combine IDS with DMZ

3.3.1.4.5 Virtual Private Network

A Virtual Private Network (VPN) is a network security system that manages the creation, encryption, and termination of secure communication channels over non-secure networks. VPN can be end-to-end, which is between client machine and server machine, or point-to-point, which is between two gateways of two distant networks. The later is more efficient.

3.3.1.4.6 Remote Access Authentication

A Remote Access Authentication system provides centralized authentication for remote client accessing a network. A centralized database maintains users' credentials, passwords, and user profiles that can be accessed by remote access control server, which arbitrates remote client's access request.

3.3.1.5 Application and Operating System Security

Security Services provided by the operating systems and the applications, and they include the following three components: OS Hardening, Database Security, and Programming Security.

3.3.1.5.1 Database Security

Database Security is a set of mechanisms that protect confidentiality, integrity, availability of data and system in the database. Database security should include authentication and access control to users and applications that need accessing data, encryption of data during transit and storage, audit trail of data accesses.

The means to control and manage access on the basis of geospatial properties (i.e., Geosecurity).

3.3.1.5.2 Programming Security

Programming Security is also called software security. It is a set of software programming practices. It includes input parameter sanitation, buffer overflow checking, proper handling of run time variables that contains sensitive data, and etc.

3.3.1.6 Physical Security

Physical Security includes identifying threats against, analyzing vulnerabilities of, and taking measures to protect personal, data, systems, buildings, and their related infrastructures in a physical environment. The threats can be man-made or natural events, and inadvertent or malicious.

The following geospatial applications (application components) may play a role in physical security: Security Planning, Security Protection and Management, Critical Infrastructure Inventory Management, Facility Mapping and Management, Incident Management, Incident Reporting, Monitor Assets/Locations/Parties, Risk Analysis, Sensor Management, Situation Awareness, Suspicious Activity Reporting, Threat Analysis, Threat Consequence Assessment, Threat Detection and Vulnerability Analysis.

3.3.1.6.1 Facility Administrative Control

Administrative Control includes choosing a secure site, designing a secure site, physical access audit trail, formulating emergency procedures, and personnel background checking.

3.3.1.6.2 Intrusion Detection and Alarm

Intrusion Detection and Alarm is a mechanism to identify and reveal in real-time any unauthorized attempt to penetrate the perimeters of a facility, physical or electronic.

3.3.1.6.3 Wireless Intrusion Detection

Hardware, software, and standards for detecting an unauthorized attempt to access and wireless access point or other type of wireless access.

3.3.1.6.4 Environmental and Safety Control

Environmental and Safety Control is physical control to sustain computer operation environment and the personnel's safety environment. It includes electrical power supply and safety, fire detection and suppression, heating, ventilation, and air conditioning (HVAC).

3.3.1.6.5 Inventory Control

Inventory Control is a physical control that protects equipments in a facility from theft or damage. The technologies include cable locks, port controls, switch controls for power switches, electronic security boards to control rebooting computers.

3.3.1.6.6 Facility Access Control

Facility Access Control is physical control to administrator personnel access to the facility. The technologies for facility access control are security access cards such as photo-image cards and digital coded cards, wireless proximity readers, biometric devices. The trend is to combine physical access card function and PKI smart cards into one card.

3.3.2 Management and Operations

Management and Operations is included here as an extension to the FEA TRM. As with Security, it is depicted as a vertical "slice" of the TRM in the HLS TRM diagram (Exhibit 4, HLS TRM). It includes the technical services required to deploy, deliver and operate software applications that make up the service components identified in the FEA Service Component Reference Model (SRM) and service components to be built or acquired by DHS. Some of these services are identified in the current SRM but others should be added to IT service management. It also includes the development and systems assurance functions required to guarantee the quality and suitability of components operated within the DHS environment.

The role of geospatial weaves throughout this "slice" of the TRM. There are management and operation tools for HLS geospatial resources. Also, there are many location-enabled management tools throughout the HLS mission.

3.3.2.1 Program Management Tools

Program Management tools are Software programs that support the coordinated management of a portfolio of projects to achieve optimal results that are strategically important. It is a comprehensive management of competing projects from planning, design, implementation, and to completion, against a single bottom line of quality, cost, and schedule that measures the success of a program.

3.3.2.2 Development Tools

Tools to support Software design and development. Specific Categories are assigned to specific Tiers above.

3.3.2.2.1 508 Compliance Tools

Software development tools that assist in adding or supporting Section 508 compliance features to an application. For example, text to voice interpreter.

3.3.2.2.2 Requirements Management Tools

Software development tools that assist in gathering, documenting, analyzing, publishing and maintaining requirements for IT systems, such as requirements traceability matrix generator.

3.3.2.2.3 Platform Independent Application Development Tools

Tools for developing applications in one or more computer languages that are machine or operating system independent. Machine or operating system independence is the ability to run an application on multiple types of systems using the same source code, through recompiling the source code for the specific system may be required. C/C++ and JAVA are examples of platform independent computer languages.

3.3.2.2.4 Platform Dependent Application Development Tools

Tools for developing applications in one or more computer languages that are not machine or operating system independent. In this case, the same source code is not able to run on multiple types of systems without modifying the source code or the language may be completely platform or machine specific.

3.3.2.2.5 Scripting Language Development Tools

Software development tools that assist in developing, maintaining, and sharing of scripts used in developing Web applications.

3.3.2.2.6 Database Development Tools

Tools for creating databases and database specific applications using one or more database specific languages such as PL/SQL, Transact-SQL, or SQL.

3.3.2.2.7 Wireless Device Client-side Application Languages

3.3.2.3 System Assurance Tools

Tools to support Configuration Management, Quality Assurance, and Test and Evaluation. Specific Categories are assigned to specific Tiers above.

3.3.2.3.1 Configure Management Tools

The system assurance tools that assist in performing configuration management of system artifacts.

3.3.2.3.2 Document Management Tools

The system assurance tools that assist in management of system documents.

3.3.2.3.3 QA Tools

The system assurance tools that assist in quality assurance and management of the system products and artifacts.

3.3.2.3.4 Test and Evaluation Tools

The testing tools which aid in setting up a test environment, maintaining the test cases and test database, and executing the tests, recording the results, and publishing the test reports.

3.3.2.4 Network Admin Tools (Network Management Tools)

Any hardware and software tools that supports controlling, planning, allocating, deploying, coordinating, diagnosing, and monitoring network resources. Other functions to be supported are frequency allocation, fault management, load balancing, security management, traffic routing, audit management, configuration management, and performance management.

3.3.2.5 Operations Management Tools

The Operations Management Tool is a software application that automates Operations Management process. The Operations Management is an IT business function that concerns with the production of IT products and services. It deals with the management of input resources and delivery of finished products and services to customers.

3.3.2.5.1 Asset Management Tools

Tools and software for identifying, tracking and managing IT equipment and the software loaded on the equipment. This software can typically identify assets that are plugged into the network and track them if they are moved to a different location on the network.

3.3.2.5.2 Automated Operations Tools

The tools and software required to automate IT operations tasks such as patching systems, virus scanning (if virus scan must be initiated externally), or defragging.

3.3.2.5.3 EPR/Account Management

Tools and software to manage user accounts and roles for application, network and other IT access.

3.3.2.5.4 Forms Management Tools

The software and tools to create, manage and maintain standardized, electronic, fillable forms.

3.3.2.5.5 Printshop Management Tools

3.3.2.5.6 Process Asset Library Tools

3.3.2.5.7 Drive Imaging

Drive Imaging describes the set of applications, which can be used to create a bit for bit "image" of a storage drive and store this image on another storage device.

3.3.2.5.8 Backup and Recovery

Automated software and standards for copying data from a server to another storage device in a format that permits the current state of the server to be recovered if the current data on the server is corrupted or deleted.

3.3.2.6 Release Management Tools

Release Management tool is one of configuration management tool that enables automation of creating a version of product; i.e., a release. The "release" of a software package is a bundle of related or inter-operating executable files that function as an application.

3.3.2.7 Content Management Tools

Content Management Tool is an advanced Web development tool that enables Web developer to store, index, search, retrieve, organize and grow items to be stored on a Web server. The items can be texts, links, graphics, images, audio or video clips, scripts, applets or anything that can be categorized logically and stored on Web server for browser to access.

3.3.2.8 Wireless Systems Management

Software and standards for managing the systems that provide wireless access to a network.

3.3.2.9 Performance and Capacity Management

Software and standards used to analyze the status, speed, health, and other characteristics of one or more networks, network links, servers, applications, or transactions.

3.3.2.9.1 Transaction Processing Monitoring Tools

Tools that measure the rate at which transactions are being processed. These tools often can provide statistics on the speed of particular parts of a transaction. Some of these tools are capable of monitoring and notifying the administrator if there is a failed or "stuck" transaction.

3.3.2.9.2 Network Performance Monitoring Tools

Software and standards which monitor the speed of a network or network link, and the characteristics of the traffic transiting the network.

3.3.2.9.3 Application Monitoring Tools

Software and standards for monitoring the status and health of an application and the speed at which it is executing. These products can often determine if there is a problem with the application and notify the administrator in the event that the application ceases to function or slows down beyond a certain, set, point.

3.3.2.9.4 Server Capacity and System Monitoring Tools

Software and standards for determining the current load on a server or set of servers, the capacity of the server to handle the load, and the health of the server or servers.

3.3.2.10 Modeling Tools

Software and standards, such as a standardized set of symbols, for developing an abstract representation of a system that approximates and accurately represents the behavior of a real or proposed system for specific analytical purposes.

3.3.2.10.1 Data Modeling

Software and standards used to develop representations of the data elements, relationships between data elements, and how data is used within a system. Tools such as ERWIN or Popkin's System Management, which provide the facilities to develop and save data models.

Attachment A

DHS Standards Profile

(See Attachment O of the Target Enterprise Architecture)

Attachment B

Acronyms

ACD	Automatic Call Distribution
ADO	ActiveX Data Object
AES	Advanced Encryption Services
AMD	Advanced Micro Devices
AOL	America On Line
API	Application Programming Interface
AS	Application Server
ASCII	American Standard Code for Information Interchange
ASP	Application Services Provider
ATB	Applied Technology Board
BCP	Business Continuity Plan
BI	Business Intelligence
BSD	Berkeley Software Distribution
CAD	Computer Aided Design
CD-ROM	Compact Disk-Read Only Memory
CICS	Customer Information Control System
CIFS	Common Internet File System
CIO	Chief Information Officer
CLR	Common Language Run-time
CM	Cryptographic Module
COI	Community Of Interest
COP	Common Operating Picture
COTS	Commercial Off-The-Shelf
CPS	Coverage Portrayal Service
CPU	Central Processing Unit
CRM	Customer Relationship Management
CS	Collaboration Service
CSS	Communications Support Systems
CTS	Coordinate Transformation Service
DBMS	Database Management System
DES	Data Encryption Standard
DHS	Department of Homeland Security
DHTML	Dynamic HyperText Markup Language
DMS	Defense Messaging Service
DMSI	Data Management System Interface
DMZ	Demilitarized Zone
DOM	Document Object Model
DRP	Disaster Recovery Plan
DTM	Digital Terrain Model
DTS	Data Transform Service
DVD	Digital Video Disc
EA	Enterprise Architecture
EAI	Enterprise Application Integration
ebXML	Electronic Business eXtensible Markup Language
EDI	Electronic Data Interchange
EFT	Electronic Funds Transfer
EHTML	Extended HyperText Markup Language
EIMS	Enterprise Identity Management System

EIS	Enterprise Information System
ESP	Enterprise Standards Profile
FCC	Federal Communications Commission
FEA	Federal Enterprise Architecture
FEMA	Federal Emergency Management Agency
FTP	File Transfer Protocol
GDR	Geospatial Data Rollup
GEA	Geospatial Enterprise Architecture
GIF	Graphics Interchange Format
GIO	Geospatial Information Officer
GIS	Geographic Information System
GIT	Geospatial Information Technology
GML	Geography Markup Language
GMO	Geospatial Management Office
GOA	Generic Open Architecture
GOTS	Government Off-The-Shelf
GPS	Global Positioning System
GUI	Graphical User Interface
HLS	Homeland Security
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
I/O	Input/Output
ICS	Image Catalog Service
IDENT	Automated Biometric Identification System
IDS	Intrusion Detection Service
IEEE	Institute of Electrical & Electronics Engineers
IFSAR	InterFerometric SAR
IM	Instant Messaging
IMAP	Internet Message Access Protocol
INS	Immigration and Naturalization Service
IP	Internet Protocol
IPS	Image Processing System
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
J2EE	Java 2 Enterprise Edition
J2ME	Java 2 Micro Edition
JDBC	Java Data Base Connectivity
JOLAP	Java On-line Analytical Processing
JPEG	Joint Photographic Expert Group
JSP	Java Service Pages
JVM	Java Virtual Machine
KM	Knowledge Management
KWIC	Key Words In Context
LAN	Local Area Network
LBS	Location-Based Services
LCD	Liquid Crystal Display

LDAP	Lightweight Directory Access Protocol
LDUP	Lightweight Directory Update Protocol
LiDAR	Light Detection and Ranging
LOF	Location Organizer Folder
MIME	Multipurpose Internet Mail Extensions
MOM	Message-Oriented Middleware
MSOP	Mission-Specific Operating Picture
MX	Mail Exchange
NAS	Network Attached Storage
NFS	Network File System
NIC	Network Interface Cards
NIST	National Institute of Standards and Technology
NNTP	Network News Transport Protocol
NOS	Network Operating System
NSA	National Security Agency
NSSE	National Security Special Event
OCR	Optical Character Recognition
ODBC	Open Database Connectivity
OGC	Open GIS Consortium
OLAP	On-Line Analytical Processing
OLTP	On-Line Transaction Processing
OMB	Office of Management and Budget
OS	Operating System
OSE	Open Systems Environment
OSI	Open Systems Interconnection
P2P	Peer to Peer
PBX	Private Branch Exchange
PCI/ISA	Peripheral Component Interconnect/Industry Standard Architecture
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PDF	Portable Document Format
PKI	Public Key Infrastructure
PNG	Portable Network Graphics
POI	Point of Interest
POP3	Post Office Protocol version 3
POSIX	Portable Operating System Interface
PSTN	Public Switch Telephone Network
RA	Remote Access
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RFID	Radio Frequency ID
RIM	Registry Information Model
RVM	Research Virtual Machine
SAD	Server Attached Disk
SAE	Society of Automotive Engineers
SAML	Security Assertion Markup Language
SAN	Storage Area Network

SAR	Synthetic Aperture Radar
SAS	Sensor Alert Service
SBP	Semantic Business Profile
SBU	Sensitive But Unclassified
SCS	Sensor Collection Service
SCSI	Small Computer System Interface
SDP	Semantic Data Profile
SensorML	Sensor Model Language
SHA1	Secure Hash Algorithm
SIM	Service Information Model
SLA	Service Level Agreement
SLD	Style Layer Descriptors
SMS	Symbol Management Service
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SPS	Sensor Planning Service
SQL	Structured Query Language
SRM	Service Component Reference Model
SSH-2	Secure Shell
SSL	Secure Socket Layer
SSO	Single Sign-On
SSP	Semantic Service Profile
SWS	Sensor Web Services
TCP/IP	Transmission Control Protocol/Internet Protocol
TIFF	Tagged Image File Format
TLS	Transaction Layer Security
TP	Transaction Processing
TRM	Technical Reference Model
TSA	Transportation Security Agency
TXT	Text File
UDDI	Universal Description, Discovery and Integration
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
USCG	United States Coast Guard
USSS	United States Secret Service
VMS	Virtual Memory System
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRU	Voice Response Unit
VRU	Voice Response Unit
WAN	Wide Area Network
WAP	Wireless Application Protocol
WCS	Web Coverage Service
WEP	Wired Equivalent Privacy
WFS	Web Feature Service

WLAN	Wireless Local Area Network
WMS	Web Map Service
WNS	Web Notification Service
WPAN	Wireless Personal Area Network
WRS	Web Registry Service
WSDL	Web Services Description Language
WTS	Web Terrain Service
XBRL	eXtensible Business Reporting Language
XIMA	XML for Image and Map Annotation
XML	eXtensible Markup Language
XSLT	eXtensible Stylesheet Language Translation
Z/OS	Z series Operating System

Attachment C

Glossary

Key geospatial terms are defined in: "HLS Geospatial Business Language: Key Terms", Appendix G.Bus.1. This *Geospatial Business Language* consists of the key terminology used to define the role of geospatial in the HLS enterprise. The geospatial semantics of the HLS mission are embodied in these terms.

Business Logic	The portion of an application that is concerned with the encoding of business rules. Applications also contain housekeeping and other, non-business specific logic.
Channel	A mode of application access and delivery consisting of an end-point device, interface software, and a communications path to the application logic. An example is a Web browser executing on a PDA using a wireless protocol to access an application on the Internet.
Data Store	A logical data "container." An implementation of a data store may be a relational DBMS, a geographic information system (GIS), an indexed file system, a flat file system, an associative data store, or any other viable storage approach.
End-point Device	Any device, and associated operating system or other run-time software that is used to connect an end-user with an application. Examples are PDAs, cellular phones, printers, plotters and desktop and laptop computers.
End-user	A human interacting with a computer-based application.
Infrastructure Services	Technical components that provide common-use functionality to applications and/or to other services and are application-neutral; that is the services can and are expected to be used by any arbitrary application. Examples are a relational database management system and a directory service.
Service Component	As defined by the FEA Service Component Reference Model a *service component* is most granular level of the SRM framework. Service components are combined to provide specific business services organized by *service type* and *service layer* in the SRM.
Service Framework	A specific configuration of technical services, protocols and interfaces grouped by similar functionality into conceptual layers.
Service Platforms	Application-neutral computing, storage and communications mechanisms that provide the technical environment for a Services Framework.
Technical Component	In contrast to the functional capability provided by a *service component*, a technical component is the software or hardware implementation of a specific technical function. A technical component may be custom developed or acquired from a vendor, through open source channels, or from other appropriate sources.
Technical Service	In this document, a technical service is a technical component that provides functionality to applications and other technical services through well-defined and published interfaces.

Attachment D

References

1. Immigration and Naturalization Service Technical Reference Model Overview (Draft), February 2003.

2. Transportation Security Administration Technical Reference Model (Draft), data unknown.

3. United States Coast Guard Technical Reference Model (Draft), March 2003.

4. Federal Enterprise Architecture Service Component Reference Model (SRM) v1.0 June 12, 2003.

5. Federal Enterprise Architecture Technical Reference Model (TRM) v1.0 June 12, 2003.