FAA-HDBK-003
JUNE 27, 1997

DEPARTMENT OF TRANSPORTATION

FEDERAL AVIATION ADMINISTRATION

INTERFACE HANDBOOK
NATIONAL AIRSPACE SYSTEM (NAS)
OPEN SYSTEM ENVIRONMENT (OSE)
APPLICATION SERVICES

AREA DCPS

DISTRIBUTION STATEMENT A Approved for public release; distribution is unlimited

FOREWORD

This handbook is approved for use by all organizations of the Federal Aviation Administration (FAA). It provides a general description of the applications and services, within an Open System Environment (OSE), that are available to users. It begins by discussing the OSE and the types of applications it supports. Section 3 introduces the OSE reference model and its elements and discusses them in detail along with the applications and services that perform the information processing for software applications. Section 4 discusses the conformance recommendations and validation procedures necessary for establishing an OSE. In addition, a section describing the Internet Protocol Suite (IPS) is provided in Appendix A. Reference documents for each of the applications and services are mentioned in the respective discussion sections. A listing of all referenced material is provided in the Applicable Documents section of this handbook.

This handbook is for guidance only. The handbook cannot be cited as a requirement. If it is, the contractor does not have to comply.

CONTENTS

CONTENTS

1. SCOPE

1.1 Scope. This handbook provides the Federal Aviation Administration (FAA) with information necessary for developing and establishing an organizational Open System Environment (OSE). An OSE is a computing environment that supports portable, scaleable, and interoperable applications. It produces a standards-based environment for heterogeneous, distributed systems and integrates these standards to provide the functionality needed to address a broad range of information processing requirements. The recommendations listed within this handbook comply with International Civil Aviation Organization/Standards and Recommended Procedures (ICAO/SARPs) specifications.
This handbook is for guidance only. It cannot be cited as a requirement. If it is, the contractor does not have to comply.

1.2 Purpose. This handbook describes the application services within the OSE that are available to FAA users. It is designed to assist FAA project personnel in determining which standards to use when acquiring, developing, or maintaining information systems supported by heterogeneous application platform environments.

2. APPLICABLE DOCUMENTS

2.1 General. The documents listed below are not necessarily all the documents referenced herein, but are the ones that are needed in order to fully understand the information provided by this handbook.

2.2 Government documents.

Military Specifications

MIL-D-28003:1988	Digital Representation for Communication of Illustration Data: Computer Graphics Metafile (CGM) Application Profile

Federal Information Processing Standards (FIPS)

FIPS PUB 46 2:1993	Data Encryption Standard
FIPS PUB 113:1993	Computer Data Authentication
FIPS PUB 127-2:1993	Database Language SQL
FIPS PUB 128:1993	Computer Graphics Metafile (CGM)
FIPS PUB 140 1:1994	General Security Requirements for Equipment Using the Data Encryption Standard
FIPS PUB 151-2:1993	Portable Operating System Interface (POSIX) - System Application Program Interface
FIPS PUB 152:1988	Standard Generalized Mark-up Language (SGML)
FIPS PUB 158-1:1993	User Interface Component Of The Applications Portability Profile
FIPS PUB 171: 1992	Key Management
FIPS PUB 177:1992	Initial Graphics Exchange Specification (IGES)
FIPS PUB 179:1995	Government Network Management Profile (GNMP)
FIPS PUB 182:1993	Integrated Services Digital Network (ISDN)

2.3 Non-government documents.

National Institute of Standards and Technology (NIST)

NIST 500-210:1995	Application Portability Profile (APP) The U.S. Government's Open System Environment Profile V. 3.0
NIST 500-220:1994	Guide on Open System Environment (OSE) Procurements

Open Software Foundation

OSF/1	Distributed Computing Environment (DCE)--Remote Procedure Call

International Organization for Standardization/International Electrotechnical Committee (ISO/IEC)

ISO/IEC 2014:1995	Information Technology - Character Encoding
ISO/IEC 9579:1993	Information Technology - Open Systems Interconnection - Remote Database Access (RDA) - Part 1: Generic Model, Service and Protocol; Part 2: SQL Specialization
ISO/IEC 9995:1995	Information Technology - Keyboard Layouts for Text and Office Systems

ISO/IEC 10646-1:1993	Information Technology - Universal Multiple-Octet Coded Character Set (UCS)-Part 1: Architecture and Multilingual Plane

Institute of Electrical and Electronic Engineers (IEEE)

IEEE 1003.2:1992	Information Technology - Portable Operating System Interface (POSIX) - Part 1: Shell and Utilities, 1992
IEEE 1003.4:1993	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface, Amendment 1. Real Time Extension [C Language].
IEEE P1003.6	Information Technology - Portable Operating System Interface (POSIX) - Part 1: Security Interface for POSIX.
IEEE P1003.8	Information Technology - Portable Operating System Interface (POSIX) - Part 1: Network Transparent File Access.
IEEE P1003.12	Information Technology - Portable Operating System Interface (POSIX) - Part 1: Protocol Independent Network.
IEEE P1224.1:1993	IEEE Standard for Information Technology - X.400 Based Electronics Messaging Application Program Interface (API).
IEEE P1224.2:1993	IEEE Standard for Information Technology - Directory Services Application Program Interface (API).
IEEE P1238:1993	IEEE Standard for Information Technology - X.400 Based Electronics Messaging Application Program Interface (API).
IEEE 1295.1:1993	IEEE Standard for Information Technology - X Window System Graphical User Interface - Modular Toolkit Environment.

3. SYSTEM DESCRIPTIONS OF AN OPEN SYSTEMS ENVIRONMENT

3.1 Open System Environment (OSE). The OSE is a computing environment that supports portable, scaleable, and interoperable applications through standard services, interfaces, data formats, and protocols. Applications in an OSE are portable since they are written in a standardized programming language. In addition, they are wrapped in standard interfaces that connect them to the computing environment. Applications are scaleable among a variety of platform and network configurations, from stand-alone microcomputers to large distributed systems such as mainframes and supercomputers. Applications interoperate by using standard communication protocols, data interchange formats, and distributed system interfaces to transmit, receive, understand, and use information.

3.1.1 Application-process. Application-processes are abstract representations of a set of resources (i.e., a human being, application program, or physical process) that are used to perform a particular information processing activity. Application-processes use portable Application Programming Interfaces (API), which allow the specific characteristics of the platform to be transparent to application programs, to interface with the Application Layer.

3.1.2 Application layer. The Application Layer of the Open Systems Interconnection (OSI) Basic Reference Model (see FIGURE 1) is the seventh and highest layer and is the only layer that directly provides services to the application process. Its purpose is to serve as the window between corespondent application-processes which are using the OSI to exchange information. The Application Layer exchanges information by means of application-entities, which are the communication components of an application process pertinent to OSI. An application-entity, i.e., an entity in the application layer, consists of one user-element and a set of application-service-elements (ASEs).

3.1.2.1 User-element. The user-element represents a part of the application-process which uses those ASEs necessary for accomplishing the communications objectives of the application-process. The sole means by which user-elements in different systems can communicate is through the exchange of application-protocol-data-units. These application-protocol-data-units are generated by ASEs.

3.1.2.2 ASE. The ASE is the part of an application-entity which provides OSI environment capability using underlying services when appropriate. Two categories of ASEs are recognized: 1) common-application-service-elements, which provide capabilities to a variety of applications, and 2) specific-application-service-elements, which provide capabilities necessary for satisfying the particular needs of specific applications (e.g. file transfer, database access, job transfer, banking, message handling, etc.)

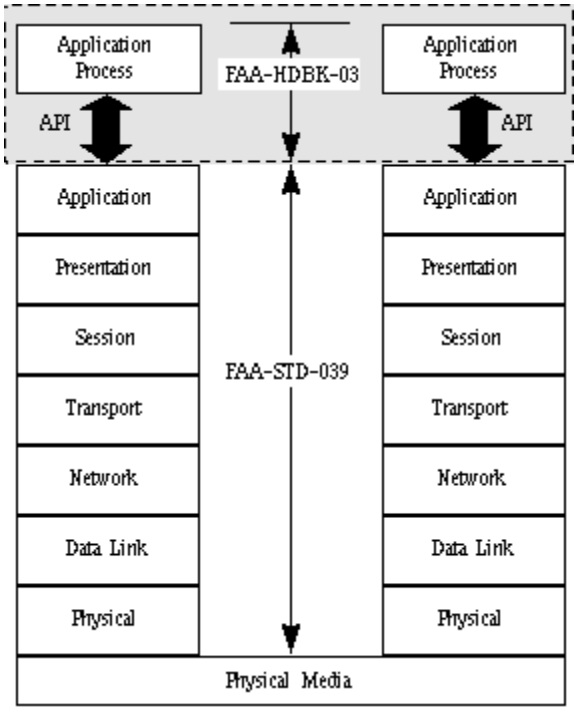


FIGURE 1. OSI reference model

3.1.3 NAS OSE Reference Model. The OSE Reference Model (OSE/RM) provides a framework for describing the functions of an automated information system (see FIGURE 2). It identifies the principal interfaces through which users and applications request data and services from computers and networks. The OSE reference model described is an adaptation of the POSIX.0 reference model, the NIST model in the APP guide, and the Department of Defense Technical Architectural Framework for Information Management (TAFIM) model. The OSE model resembles the TAFIM model which is an elaboration of the POSIX and NIST models. Two types of elements are used in the model:

a. Entities - Entities are the communication components of an application process. There are three types of entities:

(1) Application software - which includes data, documentation, training, as well as programs.

(2) Application platform - which is the collection of hardware and software components that provide the generic application and system services used by the application software.

(3) Platform external environment - which consists of those systems external to the application software and the application platform.

b. Interfaces - Interfaces are the common boundaries between independent systems where communication takes place. There are two classes of interfaces:

(1) Application Program Interfaces (API) - are the interfaces between the application software and the application platform. Their function is to support portability of application software and external environment interfaces. The OSE/RM consists of four types of API services:

(a) Human/Computer Interface

(b) Information Interchange

(c) Communication

(d) Internal System

(2) External Environment Interface (EEI) is the interface that supports information transfer between the application platform and the external environment. It consists of protocols and supporting data formats that enable the information transfer between the application platform and external environment. There are three types of information transfer services:

(a) Human users

(b) External data stores

(c) Other application platforms

The OSE/RM illustrates a straightforward user-supplier relationship where the application software is the user of services and the application platform/external environment entities are the suppliers. The API and EEI define the services that are provided.

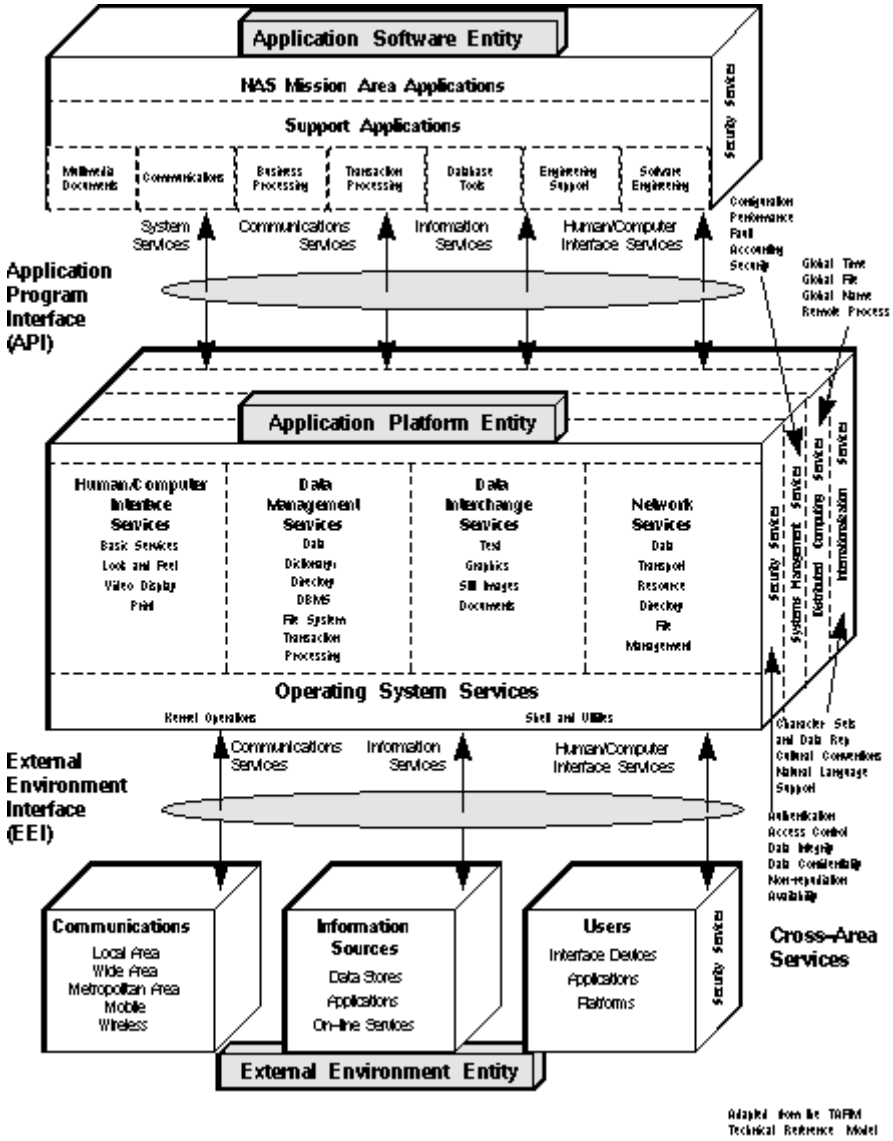


FIGURE 2. NAS OSE reference model

3.1.3.1 Entities. The following sections describe the three types of entities of the OSE Reference Model.

3.1.3.1.1 Application software entity. The application software entity is divided into two layers of applications:

1) Mission area software applications are applications that are most likely to require custom development and support applications, and are not available as commercial off-the-shelf (COTS).
2) Support applications are applications such as file utilities, database utilities, spreadsheets, and similar general purpose software that can be purchased off the shelf.

These applications can be standardized across one or more mission areas. Support applications services are used to develop or support mission applications with high level-communications or data management functions. These services include:

Multimedia Documents. Multimedia services may be used directly by mission area applications and by other support applications to satisfy a common requirement. These services include compressing, storing, retrieving, sorting, modifying, searching and printing information. Multimedia services make it possible to manage and manipulate documents of information content, presentation medium, and storage medium.

Communications. Communications applications support commonplace services such as electronic and voice message handling, electronic conferencing, video teleconferencing, facsimile transmission, and enhanced telephone services such as conference calls and call forwarding.

Business Processing. These services provide common day-to-day office functions including word processing, spreadsheet, calender, project management, and other applications for managing and administering office resources.

Transaction Processing. Characterized as a predefined sequence of data management actions that must be carried out as a complete sequence or not at all. Services may include support for distributing transactions to local and remote processors.

DatabaseTools. Include facilities to query, structure, graph, display, and report data maintained by a database management system. These tools provide an interface to the users while providing access to a variety of databases.

Engineering Support. These services include tools for analysis, design, modeling, simulation and development for a variety of users and environments. It also includes services provided by decision support development tools and expert system shells.

Software Engineering. This includes computer-aided software engineering (CASE) tools for designing applications, generating code modules, and managing software versions and configurations. It includes facilities for managing design specifications and code modules.

3.1.3.1.2 Application platform entity. The application platform entity consists of hardware and software components that provide system services used by application software. These components are proprietary commercial products and need only offer their services through standard APIs and EEIs in order to be OSE-compatible.

Hardware
Hardware components include memory, processors, input/output channels, network interface boards, and disk drives. Memory, processors, and input/output channels are offered as an integrated product with proprietary internal interfaces that are part of a vendor's architecture. Network and storage device interfaces are more likely to be based on standards.

The reference model is not directly concerned with hardware. It is the software for operating systems and Database Management Systems (DBMSs) that are required to show a standard interface to applications.

Software
Software components include the operating system, database management system, file management system, communications software, and language compilers. The following subsections describe the services and conformance requirements of the functions associated with the platform software components shown in FIGURE 2.

The service descriptions and definitions listed in the following subsections were extracted from the Application Portability Profile (APP) document, NIST 500-210. The APP is an OSE profile created for use by the U.S. government. The APP integrates industry, Federal, national, international and other specifications into a Federal application profile to provide the functionality necessary to accommodate a broad range of application software domains and Federal information technology requirements. The APP standards and specifications define protocols, interfaces, data formats, or a mix of these elements.

Operating system services. Operating system services are those services required to operate and administer the application platform and provide an interface between application software and the platform. These services consist of the following:

a. Kernel operations provide low-level services necessary to create and manage processes, execute programs, define and communicate signals, define and process system clock operations, manage files and directories, and control input-output processing to and from peripheral devices.

b. Commands and utilities include mechanisms for operations at the operator level, such as comparing, printing, and displaying file contents; editing files; pattern searching; evaluating expressions; logging messages; moving files between directories; sorting data; executing command scripts; and accessing environment information.

c. Real-time extension includes the application and operating system interfaces needed to support those application domains requiring deterministic execution, processing, and responsiveness. The extension defines the applications interface to basic system services for input/output, file system access, and process management.

d. System management includes capabilities to define and manage user resource allocation access (i.e., what resources are managed and the classes of access defined), configuration and performance management of devices, file systems, administrative processes (job accounting), queues, machine/platform profiles, an authorization of resource usage, and system back-up.

e. Operating system security services specify the control of access to system data, functions, hardware, and software resources by users and user processes.

The FIPS PUB 151-2 promotes the portability of computer application programs at the source code level. It references the ISO/IEC 9945-1 document which describes a set of fundamental services needed for the efficient construction of application programs. Access to these services is provided by defining an interface that establishes standard semantics and syntax. Since this interface enables application writers to write portable applications, it is referred to as the Portable Operating System Interface (POSIX). POSIX.1, the basis of the standard, is a vendor-independent definition for a standard interface between an application and the underlying operating system. POSIX.1 compliance represents the single most important development in the movement toward open systems and thus has caught the attention of many operating system vendors. Originally, POSIX.1 was based on UNIX System V and Berkeley UNIX,

however, it is now apparent that this standard is capable of unifying a wide range of UNIX-based and other major operating systems, not just UNIX. Other UNIX-based, NIST-certified POSIX-compliant operating systems include IBM's AIX, Digital's ULTRIX, Data General's DG/UX, Apple Computer's A/UX, Santa Cruz Operation's UNIX System V/386, Unisys CTOS, and Control Data's EP/IX. The list of vendor's and products pursuing and gaining POSIX-compliant certification grows daily and is not limited to only UNIX-based systems. Non-UNIX-based operating systems gaining POSIX compliance include IBM's MVS and OS/400, Digital's VMS, and Hewlett-Packard's MPE just to name a few.
The FIPS PUB 189 promotes portability of computer application programs at the source code level. It references the ISO/IEC 9945-2, which defines a command language interpreter (shell) and a set of utility programs. This handbook addresses the application portability profile functional area that deals with methods by which a person interacts with the operating system.

Human/computer interface services. Human/computer interface (HCI) services define the methods by which people may interact with an application. Depending on the capabilities required by users and the applications, these applications may include the following:

a. Client-server operations define the relationships between client and server processes operating within a network, in particular, graphical user interface display processes. In this case, the program that controls each display unit is a server process, whereas independent user programs are client processes that request display services from the server.

b. Object definition and management includes specifications that define characteristics of display elements: color, shape, size, movement, graphics context, user preferences, interactions among display elements, etc.

c. Window management specifications define how windows are created, moved, stored, retrieved, removed, and related to each other.

d. Dialogue support includes specifications that define the relationships between what is displayed on the screen (e.g. cursor movements, keyboard data entry, external data entry devices) and how the display changes depending on the data entered.

e. Multimedia specifications include API specifications, service definitions, and data formats that support the manipulation of multiple forms of digital and analog audiovisual data within a single application.

f. Human/computer interface security services include the definition and execution of types of user access to objects within the scope of human/computer interface systems, such as access to windows, menus, etc.; the functions that provide human/computer interface services such as human/computer management systems; and the security labeling of information on displays and other output devices.

The FIPS PUB 158-1 promotes the portability of computer application programs at the source code level. It references the X Protocol, Xlib Interface, Xt Intrinsics and Bitmap distribution format specifications of the X Window System. These specifications define a C language source code level interface to a network-based bit-mapped graphic system.

Data management services. Central to most systems is the management of data that can be defined independent of the processes that create or use it, can be maintained indefinitely, and can be shared among many processes. Data management services include the following:

a. Data dictionary/directory services allow users and programmers to access and modify data (i.e., metadata). Such data may include internal and external formats, integrity and security rules, and be located within a distributed system.

b. Database management systems (DBMS) services provide controlled access and modification of structured data. To manage the data, the DBMS provides concurrency control and facilities to combine data from different schemes. DBMS services are accessible through a programming language interface or an interactive/fourth-generation language interface. For efficiency, database management systems generally provide specific services to create, populate, move, back up, restore, and archive databases, although some of these services could be provided by general file management capabilities described in operating system services.

c. Distributed data services provide access to, and modification of, data in a remote database.

d. Data management security service include control of, access to, and integrity of data stored in a system through the use of specific mechanisms such as privileges, database views, assertions, user profiles, verification of data content, and data labels.

The FIPS PUB 127-2 promotes the probability and interoperability of database application programs. It references ANSI X3.135 which facilitates maintenance of database systems among heterogeneous data processing environments and allows for the efficient exchange of programs among different data management projects.

The FIPS PUB 156 promotes the portability of valuable information resources within and among Federal agencies. It references ANSI X3.138 which specifies a computer software system that provides facilities for recording, storing, and processing resources.

The FIPS PUB 193 specifies general purpose, SQL external repository interface (SQL/ERI) server profiles for non-SQL data repositories. This specification defines a new minimal level of the SQL language that can be supported by various non-SQL implementations.

Data interchange services. Data interchange service provide specialized support for the exchange of information, including format and semantics of data entities between applications on the same or different (heterogeneous) platforms. Data interchange services include the following:

a. Document services include specifications for encoding the data (e.g., text, pictures, numerics, special characters, etc.), and both the logical and visual structures of electronic documents.

b. Graphics data services include specifications for encoding vector graphics information (e.g., polylines, ellipses, and text) and raster graphics information.

c. Product data interchange services encompass those specifications that describe technical drawings, documentation, and other data required for product designed manufacturing, including geometric and nongeometric data such as form features, tolerances, material properties, and surfaces.

d. Data interchange security services are used to verify and validate the integrity of specific types of data interchange. Examples of such services include nonrepudiation, encryption, access, data security labeling, etc.

Network services. Network services provide the capabilities and mechanisms to support distributed applications requiring data access and applications interoperability in heterogeneous, networked environments. These services include the following:

a. Data communication includes API and protocol specifications for reliable, transparent, end-to-end data transmission across communications networks.

b. Transparent file access to available files located anywhere in a heterogeneous network.

c. Personal/microcomputer support for interoperability with systems based on other operating systems, particularly microcomputer operating systems, that may not be formally specified in a national or international standard.

d. Remote procedure call services include specifications for extending the local procedure call to a distributed environment.

e. Network security services include access, authentication, confidentiality, integrity, and nonrepudiation controls and management of communications between senders and receivers of information in a network.

3.1.3.1.3 External environment entity. The external environment platform consists of information system elements that use or are used by the application platform and the application software but are not part of those entities. They are categorized under the following:

Users. Include human users and the devices through which they exchange information with the application platform entity. This category includes display screens, keyboards, pointing devices, and printers. In addition, applications and other platforms that access the application platform entity or applications that it hosts act as clients or users and are considered to be in the external environment. Information Sources and Remote Services. Includes application platforms, data repositories, and applications that are not within the scope of the reference model applications entity and platform entity but are accessed from them.

Communications. Includes switches, routers, communication lines and other network devices and software that are not part of the reference model application platform entity but are used by it to transport information to and from components of the external environment.

3.1.3.2 Interfaces. The following sections describe the two types of interfaces used in the OSE Reference Model:

3.1.3.2.1 Application Program Interface (API). As previously mentioned, the API is the interface between the application software and the application platform. Its main function is to support portability of application software. The following sections describe the four main classes of service accessible through the API:

Human/computer interface services. These services represent the methods by which applications interoperate with platform services to use interface devices in the external environment to exchange information with human users. Typical services required at the API include prompt/answer message exchange, window functions such as open, close, display object, check cursor location, move cursor, get status of object or location, and process user interrupt message. At the API, the application is concerned with exchanging data with and issuing commands to user interface services using agreed-upon protocols

and formats. Software engineering products, such as Graphical User Interface (GUI) builders, are among the applications concerned with human/computer interface services at the API.

Information services. Information services consist of data management and data interchange services. However, through the API only data management services are carried out. Data management is concerned with the storage and retrieval of data. Data management services include the following services:

a. Data dictionary/directory services - which allow users and programmers to access and modify data about metadata. This includes data such as internal and external formats, integrity and security rules, and storage locations.

b. Database management system (DBMS) services - which provide controlled access and modification of structured data. DBMSs generally provide services to create, populate, move, back up, restore, and archive databases.

c. Distributed data services - provide access to, and modification of, data in a remote database.

In addition to DBMS services, other common forms of data management include:

d. File management - which includes normal maintenance of catalogues, directories, folder, files, data sets, and documents. Also included are facilities for managing distributed files in such a way that they appear to be local to an application or a user.

e. Transaction processing - refers to a data management scheme in which updates are contingent upon the successful completion of a unit of processing consisting of many steps rather than the execution of a single update command.

f. Information discovery - is analogous to the processes of traditional libraries, in which a card catalogue serves as a directory to various kinds of documents

Communications services. This class of services is referred to as network services by the NIST APP Guide. However, it is desirable and plausible to avoid direct access to network services in modern applications. It is desirable because an information environment in which data location is transparent to users and applications parallels the way humans use information. It is plausible because data location can be hidden from users and applications in many of todays DBMSs and distributed file systems.
The following services may be available for applications having to access network services directly through the API:

a. Directory services - the directory maintains the associations between names and locations. The directory services allow information resources to be referred to by name without regard to location.

b. Network connectivity - which is the physical and bit transmission layers of the protocol stack.

c. Data transport - is the service layer that guarantees reliable end-to-end delivery of data units.

d. Application-to-platform services - which are used to transfer files and messages and to establish user sessions.

e. Application-to-application services - which are used for cooperative exchanges of requests, status, and data between applications.

System services. System services are referred to as operating system services in the NIST APP Guide. Operating system services are the services necessary to operate and administer the application platform and provide an interface between application software and platform facilities. These services consist of the following:

a. Kernel operations - which provide the low-level services needed to create and manage processes, define and communicate signals, execute programs, manage files and directories, define and process system clock operations, and control input-output processing to and from peripheral devices.

b. Commands and Utilities - which include mechanisms for operations at the operator level, such as comparing, printing, and displaying file contents; editing files; pattern searching; moving files between directories; logging messages; evaluating expressions; executing command scripts; sorting data; and accessing environment information.

c. Real-time extensions - which include the application and operating system interfaces required to support those application domains requiring deterministic execution, processing and responsiveness. The extensions define the applications interface to basic system services for input/output, file system access, and process management.

3.1.3.2.2 External Environment Interface (EEI). The EEI interface supports the transfer of information between the application platform and the external environment and between distinct applications operating on the same platform. The EEI consists mainly of protocols and data formats and supports interoperability between applications, platforms, and users and applications. An EEI is categorized by the type of information transfer services provided. The following are the three types of information transfer services represented in the EEI:

Human/computer interface services. These interfaces define the methods by which people may interact with an application. In the OSE reference model, the structure of this interaction is that human users in the external environment read display devices and manipulate input devices, which are also in the external environment. Through the EEI, display and input devices interoperate with user interface system functions in the application platform. The user interface system functions, in turn, interoperate through the API with applications in the application software entity. Standardization at the EEI facilitates workstation portability across platforms, and user portability across platforms and applications. Human/computer interface services include the transmission of commands and queries through user interface devices such as keyboards and printing devices and the transmission of information for display on screens and paper.

Information services. As mentioned in the API section, information services are divided into data management services and data interchange services. Unlike the API where only the data management service can be accessed, the EEI allows access to both of these services. This section expands on these EEI services.

Data management services. These services at the EEI are basically the same as those described under the API. The main difference is in EEI access, where data is delivered through a communications network rather than from an application through the API, and the data and status messages must be returned through the network to the requesting process.

Data interchange services. These services take place only at the EEI. Their function is to ensure that data from one platform is represented in a way that can be processed meaningfully on another platform. Data interchange services include the following:

a. Document services - which include specifications for encoding the data; and both the logical and visual structures of electronic documents.

b. Graphics data services - which include device independent definition of picture elements.

c. Product data interchange services - which include those specifications that describe technical drawings, and other data required for product design and manufacturing.

Communications services. As discussed in section 3.4.2.1.3, communication services API, the communication services apply to both the API and the EEI. In addition communication services at the EEI for which standards can improve interoperability among platform entities include the following:

a. Data communications protocol specifications for reliable, transparent, end-to- end data transmission across communications network

b. Directory services for locating network resources such as files, other data stores, and applications; this includes interoperability between local and remote directory services

c. Remote procedure call services for extending the local procedure call to a distributed environment

d. Object request broker services for flexible configuration and reconfiguration of interoperating distributed applications

3.1.3.2.3 Cross-area services. Cross-area services are not considered as stand-alone components, although they do have a direct effect on the operation of other system components. There are times when these services affect each of the functional service areas and at other times these services have an influence that is unique to a particular service area. As the reference model evolves, the cross-area services category will be re-examined for additional components. Presently, cross-area services include the following services:

Internationalization services. Include those services and interfaces that allow users to define, select, and change between culturally different application environments. These services facilitate interoperability between commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) products. Internationalization falls into the following categories:

a. Character sets and data representation services - which include the capability to input, store, manipulate, retrieve, communicate, and present data independent of the coding scheme used.

b. Cultural convention services - which provide the capability to store and access rules and conventions for cultural entities maintained in a cultural convention repository.

c. Natural language support services - which provide the capability to support more than one language simultaneously.

Security services. These services protect information in an automation system, where the appropriate level of protection is determined according to the value of the information to the organization and the

perceived threats to it. Security services are imperitive in environments where data must not be corrupted and where management orders are issued only by authorized sources and must arrive at their destinations uncorrupted. Security services include the following:

a. Authentication service - which confirms the identities of requestors before use of system resources.

b. Access control service - which prevents the unauthorized use of system resources.

c. Data integrity service - which ensures that data are not altered or destroyed in an unauthorized manner.

d. Data confidentiality service - which ensures that data are not made available or disclosed to unauthorized individuals or computer processes.

e. Non-repudiation service - which ensures that entities engaging in an information exchange cannot deny being involved in it.

f. Availability service - which ensures that timely and regular communication services are available.

To achieve the goals of an open system environment (OSE), information systems must be managed effectively. Information systems are composed of diverse resources (such as printers, software, users, processors) which may differ widely, but are treated uniformly as managed objects. The basic concepts of management are then applied to the full suite of OSE components and their services.

System management services. Systems management functionality is divided according to the aspects of management that generically apply to all functional resources. The OSI system management framework consists of the following aspects:

a. Configuration management services - which address the identification, control, status accounting, and verification functions.

b. Performance management services - which provide the ability to establish targets for performance and to measure performance against those targets.

c. Fault management services - which allow a system to react to the loss or incorrect operation of system components at various levels.

d. Accounting management services - which provide the ability to identify and/or negotiate mechanisms for collecting, and associating charges with information regarding communications resource usage.

e. Security management services - which monitor and control the security services.

Distributed computing services. These services provide specialized support for applications that may be physically or logically dispersed among computer systems in a network, yet wish to maintain a cooperative processing environment. Distributed computing services include the following services:

a. Global time services - which include synchronizing computer clocks to ensure consistent time reference among distributed processes.

b. Global data services - which provide access to, and modification of, data and metadata in remote or local databases.

c. Global file services - which provide for a level of abstraction for file systems.

d. Global name services - which provide a means for unique, location-transparent identification of resources within a distributed computing environment.

e. Remote process services - which provide the means for dispersed applications to interoperate across a computer network.

f. Thread services - which provide an underlying service used for multiple current executions within a single computer process.

3.2 Definitions. Terms used in this document are defined below.

Acquisition: The process for obtaining systems, equipment, or modifications to existing inventory items.

Application:
1) A logical grouping of activities, and their related data and technology, which constitutes a cohesive unit;
2) A logical grouping of programs, data, and technology with which an end-user interacts to perform a specific function or class of functions.

Application Entity: Is a communication component of an application process.

Application Layer: Layer seven of the OSI reference model. It is concerned with providing communication support for system-independent application service.

Application Portability Profile (APP): Is the U.S. Government's Open System Environment profile that identifies specifications which address a broad range of federal applications and systems.

Application Process (AP): Is an element (a human being or an application program) within an open system that performs the information processing for a particular application.

Application Program Interface (API): An interface that allows the specific characteristics of the platform to be transparent to application programs.

Application Service Element (ASE): An atomic subobject of an application entity. It defines a set of capabilities of an application entity.

Application Software: All computer programs of a given system that directly support the process of a functional application.

Client/Server: The client/server model states that a client (user), whether a person or a computer program, may access authorized services from a server (host) connected anywhere on the ADP system.

Commercial Off-The-Shelf (COTS): A fully developed product that is available on the commercial market.

Context Management: Service that supports addressing requirements for Air Traffic Services Communication (ATSC).

Contractor: An entity in private industry which enters into contracts with the Government.

Entity: Is the communication component of an application process.

Functional Information Processing Standard (FIPS): Publications, organized into major service categories, that define the Government's Federal Information Processing Standards as issued by NIST.

Government Open Systems Interconnection Profile (GOSIP): Defines and describes a set of protocols that enable systems developed by different vendors to interoperate and enable users of different applications to exchange information.

Information System (IS): The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures.

Interface: The common boundary between independent systems or modules where communication takes place.

International Organization for Standardization (ISO): An organization established to develop and define data processing standards to be used throughout participating countries.

Interoperability: The capability of systems to communicate with one another and to exchange and use information including content, format, and semantics.

Local Area Network (LAN): A user owned, user operated, high volume data transmission facility connecting a number of communicating devices within a single building or several buildings within a physical area.

Maintainability: Ability of an item to be retained in or restored to a specified condition when maintenance is performed.

Network: A composition of a communications media and components attached to that medium whose responsibility is the transfer of information.

Network Architecture: The philosophy and organizational concept for enabling communication among data processing equipment at multiple locations.

Network Security: The protection of networks and their services from all natural and human-made hazards including protection against unauthorized access, modification or destruction of data; denial of service; or theft.

National Institute of Standards and Technology (NIST): An organization of the U.S. Department of Commerce that develops standards and guidelines for Federal computer systems.

Offeror: Contractor submitting a proposal in response to a Government acquisition effort.

Open System: Is an abstract representation of that part of a real system (equipment and resources) that provides those system functions that are addressed within the OSI reference model and may be fully described within the OSI framework.

Open System Environment (OSE): A computing framework including software, hardware, and communications services, interfaces, data formats, and protocols that are based on evolving, available, consensus standards, and provides a significant degree of portability, scalability, and interoperability of applications and data.

Open Systems Interconnection (OSI): A seven-layer network architecture used for the definition of network protocol standards to enable any OSI-compliant system or device to communicate with any other OSI-compliant system or device for a meaningful exchange of information.

Operating System (OS): The central control program that governs a computer's operations.

Organizational Profile: A suite of specifications chosen by an organization for implementing an open system environment based on that organization's particular requirements.

OSI Reference Model: The generic model by which OSI communication services are structured.

Platform: The hardware, software, and communications required to provide the processing environment to support one or more application software systems.

Portability: The ability of application software source code and data to be transported without significant modification to more than one type of computer platform or more than one type of operating system.

Portable Operating System Interface (POSIX): Is an operating system interface, based on the UNIX operating system, that enables application writers to write portable software. It provides access to a set of fundamental services needed for the efficient construction of application programs.

Profile: A set of one or more base standards necessary for accomplishing a particular function.

Protocol: A set of procedures for establishing and controlling communications transmissions.

Requirement: The need or demand for personnel, equipment, facilities, other resources or services, by specific quantitative for specific periods of time or at a specified time.

Scalability: The ability to move application software source code and data into systems and environments that have a variety of performance characteristics and capabilities without significant modification.

Software Interface: The languages, codes and messages that programs use to communicate with each other.

System Software: A major category of programs used to control the computer and process application programs.

User: That organization or person which will be the recipient of the production item for use in accomplishing a designated mission.

Validation: The process of testing a computer program or automated system for correct implementation of requirements.

3.3 Acronyms and abbreviations. The following are definitions of acronyms and abbreviations used in this handbook.

ACSE	Association Control Service Element
ADS	Automatic Dependent Surveillance
ANSI	American National Standards Institute
API	Application Program Interface
APP	Application Portability Profile
ASE	Application Service Elements
ASI	Application Software Interface
ATC	Air Traffic Control
ATIS	Automatic Terminal Information Services
ATN	Aeronautical Telecommunication Network
ATSC	Air Traffic Services Communication
CAS	Commercially Available Software
CM	Context Management
COTS	Commercial Off-The-Shelf
CPDLC	Controller Pilot Data Link Communications
CSL	Computer Systems Laboratory
DBMS	Database Management System
DI	Data Interchange
DM	Data Management
EEI	External Environment Interface
ERI	External Repository Interface
FAA	Federal Aviation Administration
FAT	Factory Acceptance Test
FIPS PUB	Federal Information Processing Standard Publication

FIS	Flight Information Service
GOTS	Government Off-The-Shelf
GS	Graphics Services
HCI	Human/Computer Interface
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Committee
IEEE	Institute of Electrical and Electronic Engineers
ISDN	Integrated Services Digital Network
ISEE	Integrated Software Engineering Environments
ISO	International Organization for Standardization
NAS	National Airspace System
NDI	Non-Developmental Item
NIST	National Institute of Standards and Technology
NOTAM	Notice to Airmen
NS	Network Services
NVLAP	National Voluntary Laboratory Accreditation Program
OS	Operating System
OSE	Open Systems Environment
OSE/RM	Open Systems Environment/Reference Model
OSF	Open Software Foundation
OSI	Open Systems Interconnection
PII	Protocol Independent Interfaces
PIREP	Pilot Report Service
POSIX	Portable Operating System Interface
RCP	Required Communications Performance
RDA	Remote Database Access

RPC	Remote Procedure Call
RVR	Runway Visual Range
SARP	Standards and Recommended Practices
SGML	Standard Generalized Markup Language
SQL	Structured Query Logic
SWE	Software Engineering
TEMP	Test and Evaluation Master Plan
TWS	Terminal Weather Service
VPL	Validated Products List

4. GENERAL RECOMMENDATIONS

4.1 OSE application software conformance recommendations. All information technology products and services offered in an OSE should operate in and execute upon platforms that provide an open system environment as described in the NIST Special Publication 500-210.

4.1.1 Portability. Portability refers to the ease with which application software and data shall be transported from one operating system to another.

4.1.1.1 CAS and NDI software portability. Portability of commercially available software (CAS) and non-developmental item (NDI) components incorporated into FAA applications should be demonstrated using one of the following methods:

a. The compilation and execution of source code should be performed on two heterogeneous platforms. A detailed report of the modifications should be submitted.

b. The current Validated Products List (VPL) of NIST should have two or more references that indicate the same implementation of the proposed software has been validated on at least two different vendors' platforms.

c. The CAS vendor or an industry-recognized trademarking or branding organization should provide a certificate that indicates the same implementation of the proposed software has been validated on at least two different vendors' platforms.

d. The test method deviation, demonstration type, and schedule should be documented in the Program Test and Evaluation Master Plan (TEMP).

4.1.2 Scalability. Scalability refers to the ability of application software and data to move into systems and environments that have a variety of performance characteristics and capabilities without significant modification. The Program TEMP should document the demonstration.

4.1.3 Interoperability. Interoperability refers to the capability of systems to communicate with one another and to exchange and use information including content, format, and semantics. Demonstration of interoperability should occur using one of the following methods:

a. Execution of software components (developed software, CAS, or NDI software) communicating by means of interfaces (Service provider or OSI protocols selected by the FAA), should occur on two heterogeneous platforms with input data transmitted bidirectionally from one platform to the other. Output data should be analyzed to verify correct operation.

b. Execution of software components (developed software, CAS, or NDI software) communicating by means of files or pipes, selected by the FAA, should occur on two heterogeneous platforms with the data files produced by the source application on one platform transferred to the destination application residing on the second platform. Output data should be analyzed to verify correct operation.

c. The current Validated Products List (VPL) of NIST should have two or more references that should indicate that the same implementation of the proposed software has been registered on the interoperability registers for at least two platforms.

d. The CAS vendor should provide proof that indicates that the same implementation of the proposed software has been tested for interoperability on at least two platforms.

4.1.4 Validation and conformance demonstration recommendations. These procedures and guidelines are derived from the NIST document "Guide to Open Systems Environment Procurement," NIST 500-220: 1994.

4.1.4.1 Applicability of validation and conformance. Only validated implementations should be used when a Federal Information Processing Standard (FIPS) is specified, and a validation test suite is available, and NIST validation testing procedures are in place, and one or more NIST-recognized testing laboratories are available.

The contractor should perform a conformance demonstration when a FIPS is not the required specification, or where a FIPS is required and a validation test suite is not available or NIST validation testing procedure has not been established, or where official NIST-recognized test laboratories do not exist.

Validation should be in accordance with CSL validation procedures for the individual FIPS concerned. The results shall be used to confirm that the requirements are satisfied.

4.2 System software conformance recommendations.

4.2.1 Operating system services standards. The following standards and conformance recommendations should apply to Operating System Services:

a. A POSIX compliant operating system should be used for kernel operations and conform to FIPS PUB 151-2, as a minimum, be validated.

b. Commands and utilities offered in support of FIPS PUB 151-2 should implement IEEE 1003.2, as a minimum.

c. Operating system security services offered in support of FIPS PUB 151-2 should implement the functionality defined in IEEE P1003.6, Security Interface for the POSIX.

d. Real-time operating system services offered in support of FIPS PUB 151-2 should implement the functionality defined in IEEE 1003.4-1993, Amendment 1.

4.2.2 Human/computer interface services standards. The following standards and conformance recommendations should apply to human/computer interface services:

All X Windows client-server implementations should comply with FIPS PUB 158-1. Object definition and management services, window management services, and dialogue support services offered as a result of this and other requirements should implement the IEEE P1295.1 interface.

4.2.3 Data management services standards. The following standards and conformance recommendations should apply to data management services:

a. SQL language processors offered should conform to FIPS PUB 127-2 Data Language SQL. These processors should implement all of the required language elements options, and special procurement considerations. Validation is required.

b. Distributed database services offered should implement "Remote Database Access (RDA)", ISO/IEC 9579.

c. The DBMS/data dictionary should maintain and store database descriptions separate from, but available to, applications through an appropriate API.

d. The DBMS should provide database integrity checking; allocating, initializing, and deallocating physical storage; loading, unloading, reorganizing, and reloading files and parts of files; repairing damaged information; and logging all transactions selectively before or after the data is updated.

4.2.4 Data interchange services standards. The following standards and conformance recommendations should apply to data interchange services:

a. All of the language elements of SGML should be implemented in accordance with FIPS PUB 152, SGML.

b. All graphical information in vector format among different devices, systems and installations should conform to FIPS PUB 128 CGM.

c. All generators of computer graphics metafiles acquired should conform to FIPS PUB 128, CGM, and MIL-D-28003.

d. Product data interchange services encompassing technical drawings, documentation, and other data required for product design and manufacturing, including geometric and non-geometric data should implement FIPS PUB 177.

4.2.5 Network services standards. The following standards and conformance recommendations should apply to Network Services:

a. Network management and functionality offered as a result of these and other recommendations should conform to FIPS PUB 179, and have a capability demonstration.

b. Transparent file access services offered as a result of these and other requirements should conform to IEEE P1003.8, and should have a conformance demonstration.

c. Process communication interfaces proposed should provide the functionality defined in Protocol Independent Interfaces (PII) IEEE P1003.12 and should have a capability demonstration.

d. OSI ACSE/presentation application program interfaces proposed should provide the functionality defined in IEEE P1238 and have a capability demonstration.

e. Software interfaces for accessing and administering Integrated Services Digital Network (ISDN) services proposed should provide the functionality defined in Application Software Interface (ASI) Version 1.

f. Integrated video, voice, and data communications proposed should implement the protocols defined in FIPS 182.

g. Electronic mail/message handling programming interfaces proposed should implement the functionality defined in X.400 Based Electronic Messaging Application Program Interface (API) IEEE P1224.1 and should have a capability demonstration.

h. Directory services programming interfaces proposed should implement the functionality defined in Directory Services Application Program Interface (API) IEEE P1224.2 and have a capability demonstration.

4.2.6 Security services standards. The following standards and conformance recommendations should apply to Security Services:

a. Data encryption provided by the system should be accomplished in accordance with FIPS PUB 46-1 data encryption standard.

b. Data/message authentication provided by the system should be accomplished using message authentication codes as defined by FIPS PUB 113.

c. The electronic signature capability provided by the system should be accomplished in accordance with FIPS PUB 113.

d. The key management provided by the system should be accomplished in accordance with FIPS PUB 171.

e. The design, implementation, and use of the cryptographic module provided by the system should be in conformance with FIPS 140-2.

4.2.7 System management services standards. The following standards and conformance recommendations should apply to system management services:

a. System management services offered in support of FIPS 151-2 implementations should implement the functionality defined in IEEE P1003.2-1993.

b. Telecommunications infrastructure administration should be provided and implement the functions and capabilities defined in FIPS 187.

c. A system administration facility should be provided and implement system administration functions to allocate the use of system resources by individual user, by class of users, and by application.

4.2.8 Distributed computing services standards. The following standards and conformance recommendations should apply to Distributed computing services:

a. Distributed computing functionality offered as a result of these recommendations should conform to OSF/1, and should have a capability demonstration.

b. Products offered should interoperate with and support FIPS PUB 151-2 POSIX, and should require capability demonstration of this interoperability.

c. Communications should execute transparently to the users and provide programming interfaces at the application layer where appropriate.

4.2.9 Internationalization services standards. The following standards and conformance recommendations should apply to internationalization services:

a. Character encoding provided by the system should be in conformance with ISO 10646, ASN.1.

b. Cultural conventions provided by the system should be in conformance with ISO 2014, ISO 3307.

c. Natural language support provided by the system should be in accordance with ISO 9995.

5. NOTES

5.1 References.

Department of Defense 5200.28 STD, "Department of Defense Trusted Computer System Evaluation Criteria," December 1985.

Department of Defense, Draft "Technical Architecture Framework for Information Management," Volume 7, Information Technology Standards Guidance Open Systems Environment (ITSG-OSE), Release 1.1.

DMR Group, Inc., "Strategies for Open Systems," Boston, 1990.

Draft ISO 10303, "Standard for the Exchange of Product Model Data (STEP)."
Emerging Technologies Group, Inc., "An Analysis of Application Environments,"
Dix Hills, New York 19890.

FIPS 21 3, "COBOL," U.S. Department of Commerce (DOC). January 12, 1990.

FIPS 29 3, "Interpretation Procedures for Federal Information Processing Standards for Software," DOC, October 29, 1992.

FIPS 46 2, "Data Encryption Standard," DOC, December 30, 1993.

FIPS 69 1, "Fortran," DOC, December 24, 1985.

FIPS 101, "Guideline for Life Cycle Validation, Verification, and Testing of Computer Software," DOC, June 6, 1983.

FIPS 119, "Ada," U.S. Department of Defense, November 8, 1985.

FIPS 113, "Computer Data Authentication," DOC, May 30, 1985.

FIPS 120 1, "Graphical Kernel System," DOC, January 8, 1991.

FIPS 132, "Guideline for Software Verification and Validation Plans,"
DOC, November 19, 1987.

FIPS 140 1, "General Security Requirements for Equipment Using the Data Encryption Standard," DOC, January 11, 1994.

FIPS 146 1, "Government Open Systems Interconnection Profile (GOSIP) Version 2," DOC, April 3, 1991. (See entry for planned FIPS 146 2.)

FIPS 153, "Programmer's Hierarchical Interactive Graphics System (PHIGS)," DOC.
}}}
}}

FIPS 156, "Information Resource Dictionary System (IRDS)," DOC, 1989.

FIPS 160, "C," DOC, March 13, 1991.

FIPS 161, "Electronic Data Interchange (EDI)," DOC.

FIPS 171, "Key Management Using ANSI X9.17," DOC, April 27, 1992.

FIPS 186, "Digital Signature Standard (DSS)," DOC.

FIPS 189, "Portable Operating System Interface (POSIX); Part 2: Shell and Utilities," DOC, 1994.

FIPS 192, "Government Information Locator Service (GILS)," DOC.

FIPS 193, "SQL Environments," DOC, 1995.
Galitz, Wilbert O., User lnterface Screen Design, QED Publishing, Wellesley, Massachusetts, 1993.

IEEE Working Group P1003.1f, Draft "Security Interface for the Portable Operating System Interface for Computer Environments."

IEEE Working Group P1003.1f, Draft "Transparent File Access (TFA)."

ISO 8613:1989, "Office Document Architecture (ODA)."

ISO/IEC 9945-1:1990, "Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) [C Language]."

ISO/IEC 9945-2:1993, "Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utiltities."

National Computer Security Center (NCSC) Technical Guide NCSC TG 024, "A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work- An Aid to Procurement Initiators" June 30, 1993.

NBS Special Publication 500 117, "Selection and Use of General Purpose Programming Languages, Volumes 1 and 2," DOC, October 1984.

NBS Special Publication 500 131, "Guide for Selecting Microcomputer Data Management Software." DOC, October 1985.

NIST Special Publication 500 184, "Functional Benchmarks for Fourth Generation Languages," DOC, March 1991.

NIST Special Publication 500 192, "Government Open Systems Interconnection Profile Users' Guide, Version 2." October 1991.

NIST Special Publication 500 201, "Reference Model for Frameworks of Software Engineering Environments," DOC, December 1991.

NIST Special Publication 500 211, "Framework for Software Engineering Environments Reference Model," DOC, August 1993.

NIST Special Publication 500 213, "Project Support Environment (PSE) Reference Model," DOC, November 1993

NIST Special Publication 500 217, "IGOSS Industry/Government Open Systems Specification," Gerard Mulvenna, Editor. DOC, May 1994. (See entry for planned FIPS 146 2.)

NIST Special Publication 800 4, "Computer Security Considerations in Federal Procurements." DOC, March 1992.

Office of Management and Budget (OMB) Circular A 130, "Management of Federal Information Resources."

OSF/1, "Distributed Computing Environment (DCE)-Remote Procedure Call (RPC)," Open Software Foundation.

Planned FIPS 146 2, "Profiles for Open Systems Internetworking Technologies," DOC, undated.

ANSI X3.135:1992, " SQL," DOC.

ANSI X3.138:1988, " Information Systems - Information Resource Dictionary System (IRDS)," DOC.

RFC 768, "User Datagram Protocol."

RFC 788 and RFC 821, "Simple Mail Transfer Protocol."

RFC 791, "Internet Protocol."

RFC 792, "Internet Control Message Protocol."

RFC 793, "Transmission Control Protocol."

RFC 821 and RFC 788, "Simple Mail Transfer Protocol."

RFC 822, "Standard for the Format of ARPA Internet Text Messages."

RFC 854, "TELNET Protocol Specification."

RFC 855, "TELNET Option Specifications."

RFC 904, "Exterior Gateway Protocol."

RFC 919, "Broadcasting IP Datagrams."

RFC 922, "Broadcasting Internet Datagrams in the Presence of Subnets."

RFC 950, "Internet Standard Subnetting Procedure."

RFC 959, "File Transfer Protocol."

RFC 974, "Mail Routing and the Domain System."

RFC 1034, "Domain Names-Concepts and Facilities."

RFC 1035, "Domain Name-Implementation and Specification."

RFC 1049, "Content Type Header Field."

RFC 1112, "Host Extensions for IP Multicasting."

RFC 1119, "Network Time Protocol (Version 2)."

RFC 1155, "Structure and Identification of Management Information for TCP/IP based Internets."

RFC 1157, "A Simple Network Management Protocol (SNMP)."

RFC 1212, "Concise MIB Definitions."

RFC 1213, "Management Information Base II (MIB)."

Technical Report ECMA TR/55, 3rd Edition, "Reference Model for Frameworks of Software Engineering Environments," European Computer Manufacturers' Association, 1993.

U.S. General Services Administration (GSA),"Federal ADP and Telecommunications Standards Index," GSA, April 1993.

U.S. General Services Administration (GSA), "Standard Solicitation Documents for Federal Information Processing (FIP) Resources" (software, equipment, maintenance, systems, and modifications based on changes in Federal regulations).

5.2 Document sources. The following organizations are responsible for distributing standards for various standards making organizations. Ordering and fee information for specific standards may be obtained directly from the following standards organizations:

ANSI
American National Standards Institute
1430 Broadway
New York, NY 10018
Phone: (212) 354 3300

ANSI International Publications
Information on standards from ISO and its member bodies (e.g., DIN, BSI, JISC), IEC, and CEN/CENELEC
Phone: (212) 642 4995

ANSI General Sales (National Standards)
Phone: (212) 642 4900

Department of Defense
Defense Printing Service Detachment
Standardization Documents Order Desk
700 Robbins Avenue

Philadelphia, PA 19111 5094
Phone: (215) 697 1187
Any Federal organization or DoD contractor can order numerous types of standards, including FIPS PUBs and MIL STDs from the Defense Printing Service.

Data Interchange Standards Association
ASC X12 and PAEB Secretariat
1800 Diagonal Road, Suite 355
Alexandria, VA 22314
Phone: (703) 548 7005
FAX: (703) 548 5738

ECMA
European Computer Manufacturers Association
Rue du Rhone 114
CH 1204 Geneva
Switzerland
Phone: 011 41 22 735 36 34

Federal Information Processing Standards (FIPS PUB)
U. S. Department of Commerce National Technical Information Service (NTIS)
Springfield, VA 22161
Phone: (703) 487 4650
FAX: (703) 321 8547
NIST publishes an index of FIPS PUB that is available through NIST. Request "NIST Publications List 58."

GPO
Government Printing Office
Superintendent of Documents
U. S. Government Printing Office
Washington, DC 20402
Phone: (202) 783 3238

IEC
International Electrotechnical Commission
3 Rue de Varembe
P. O. Box 131
CH 1211 Geneva 20
Switzerland
Phone: 011 41 22 34 01 50

IEEE (for accepted standards)
The Institute of Electrical and Electronics Engineers, Inc.
445 Hoes Lane
P. O. Box 1331
Piscataway, NJ 08855 1331
Phone: (201) 562 3800

IEEE (for draft standards)
1730 Massachusetts Avenue, N. W.

Washington, DC 20036 1903
Phone: (202) 371 0101
Ask for the name and address of the editor of the draft standard for specific working groups.

ISO
International Organization for Standardization
Central Secretariat
1 Rue de Varembe
P. O. Box 56
CH 1211 Geneva 20
Switzerland
Phone: 011 41 22 34 12 4()

National Computer Security Center
INFOSEC Awareness Division
ATTN: IAOC (X711 Ms. Keller)
Ft. George G. Meade, MD 20755 6000

National Technical Information Service (NTIS)
U. S. Department of Commerce
National Technical Information Service (NTIS)
Springfield, VA 22161
Phone: (703) 487 4650
FAX: (703) 321 8547

SQL Access
SQL Access Group c/o Robert Crutchfield
Fransen and Associates, Inc.
2171 Campus Drive, Suite 260
Irvine, CA 92715
Phone: (714) 752 5942

T1 Standards
Standards Committee T1 Telecommunications
1200 G Street, N.W. Suite 500
Washington, DC 20005
Phone: (202) 434 8845
FAX: (202) 393 5453

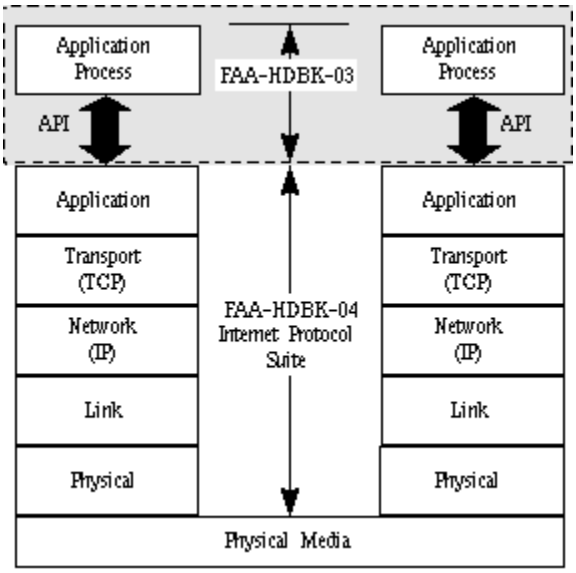
X3
American Standards Committee X3 -- Information Processing Systems
Computer and Business Equipment Manufacturers Association (CBEMA)
Director, X3 Secretariat
1250 Eye Street NW, Suite 200
Washington, DC 20005 3922
Phone: (202) 737 8888 (Press 1 twice.)
FAX: (202) 638 4922 or (202) 628 2829

APPENDIX A

IPS SERVICES

A.1 INTERNET PROTOCOL SUITE

The Internet Protocol Suite (IPS) Reference Model (see FIGURE A-1) depicts the interface between the application process and the TCP/IP communication protocols. The Application Programming Interface (API) that provides this interface is called a socket (see RFC 147). A socket is a 4.x BSD UNIX operating system abstraction, provided by Berkeley UNIX, that allows an application program to access the TCP/IP communication protocols. An interface is achieved when an application opens a socket, specifies the service desired, binds the socket to a specific destination, and then sends or receives data. Other common operating systems for sockets include vendor implementations such as SunOS 4.x, SVR4, and AIX 3.2 that were originally developed from the Berkley sources.



FLGURE A-1. IPS reference model

A.1.1 Internet services. When an interface is achieved, application programs can use the following most popular and wide spread internet services provided at the application level:

Electronic Mail. Allows a user to compose memos and send them to individuals or groups. It also allows users to read memos that they have received.

File Transfer. Allows users to send or receive files of programs or data.

Remote Login. Allows a user sitting at one computer to connect to a remote machine and establish an interactive login session.