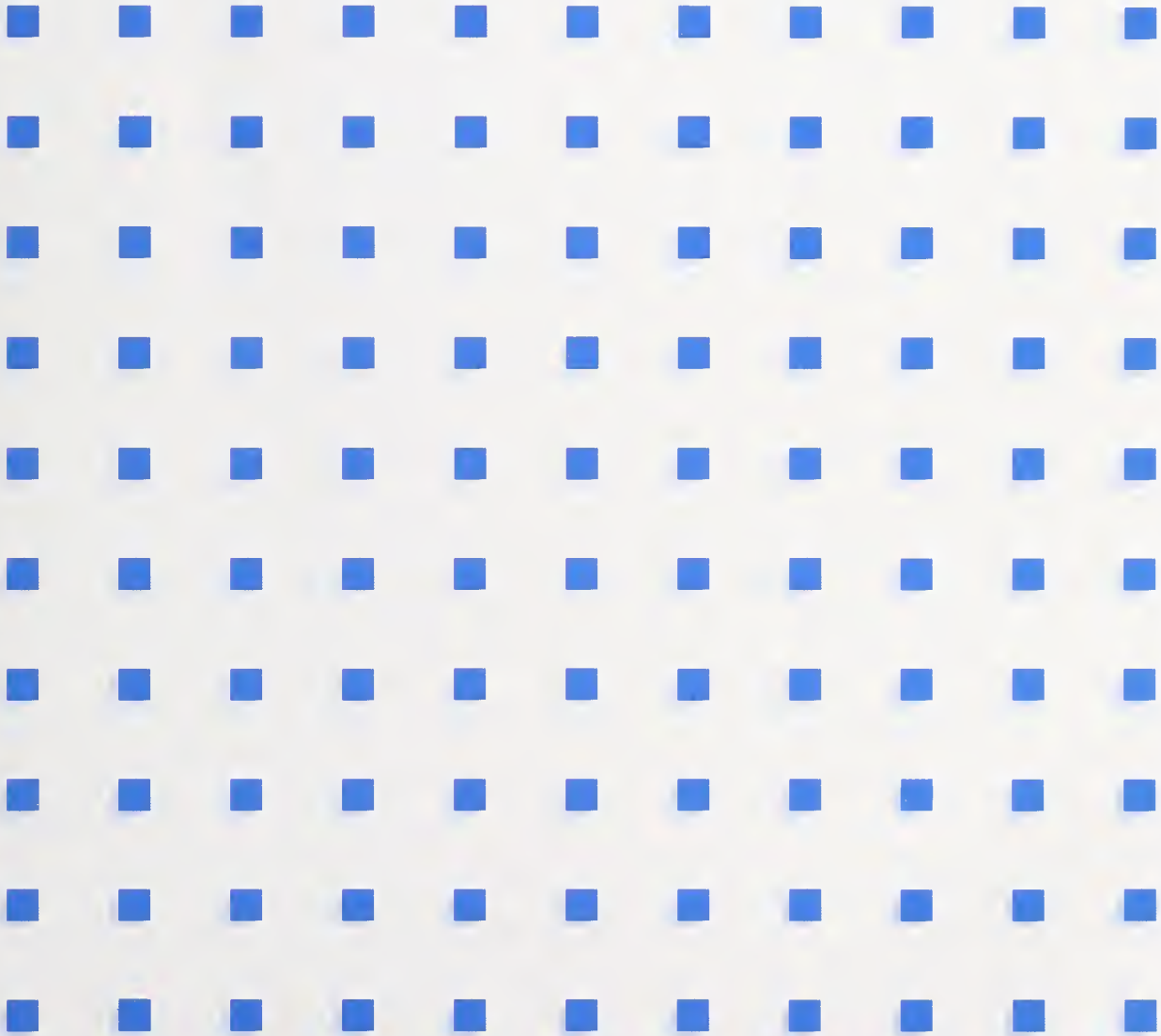
NIST Special Publication 500–230

Computer Systems Technology

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology

NIST

Application Portability Profile (APP) The U.S. Government's Open System Environment Profile Version 3.0



The National Institute of Standards and Technology was established in 1988 by Congress to "assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries."

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency's basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department's Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering, and develops measurement techniques, test methods, standards, and related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST's research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Public Inquiries Desk, 301-975-3058.

Office of the Director
- Advanced Technology Program
- Quality Programs
- International and Academic Affairs

Technology Services
- Manufacturing Extension Partnership
- Standards Services
- Technology Commercialization
- Measurement Services
- Technology Evaluation and Assessment
- Information Services

Materials Science and Engineering Laboratory
- Intelligent Processing of Materials
- Ceramics
- Materials Reliability[1]
- Polymers
- Metallurgy
- Reactor Radiation

Chemical Science and Technology Laboratory
- Biotechnology
- Chemical Kinetics and Thermodynamics
- Analytical Chemical Research
- Process Measurements
- Surface and Microanalysis Science
- Thermophysics[2]

Physics Laboratory
- Electron and Optical Physics
- Atomic Physics
- Molecular Physics
- Radiometric Physics
- Quantum Metrology
- Ionizing Radiation
- Time and Frequency[1]
- Quantum Physics[1]

Manufacturing Engineering Laboratory
- Precision Engineering
- Automated Production Technology
- Intelligent Systems
- Manufacturing Systems Integration
- Fabrication Technology

Electronics and Electrical Engineering Laboratory
- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Electromagnetic Fields[1]
- Electromagnetic Technology[1]
- Optoelectronics[1]

Building and Fire Research Laboratory
- Structures
- Building Materials
- Building Environment
- Fire Safety
- Fire Science

Computer Systems Laboratory
- Office of Enterprise Integration
- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

Computing and Applied Mathematics Laboratory
- Applied and Computational Mathematics[2]
- Statistical Engineering[2]
- Scientific Computing Environments[2]
- Computer Services
- Computer Systems and Communications[2]
- Information Systems

[1] At Boulder, CO 80303.
[2] Some elements at Boulder, CO 80303.

NIST Special Publication 500–230

Application Portability Profile (APP) The U.S. Government's Open System Environment Profile Version 3.0

Systems and Software Technology Division
Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-0001

(Supersedes NIST SP 500-210)

February 1996

U.S. Department of Commerce
Ronald H. Brown, Secretary

Technology Administration
Mary L. Good, Under Secretary for Technology

National Institute of Standards and Technology
Arati Prabhakar, Director

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) has a unique responsibility for computer systems technology within the Federal government. NIST's Computer Systems Laboratory (CSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. CSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. CSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 500 series reports CSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

National Institute of Standards and Technology Special Publication 500-230
Natl. Inst. Stand. Technol. Spec. Publ. 500-230, 108 pages (Feb. 1996)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1996

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

Executive Summary

An Open System Environment (OSE) encompasses the functionality needed to provide interoperability, portability, and scalability of computerized applications distributed across networks of heterogeneous, multivendor hardware/software/communications platforms. The OSE forms an extensible framework that allows services, interfaces, protocols, and supporting data formats to be defined in terms of nonproprietary specifications that evolve through open (public), consensus-based forums.

A selected suite of specifications that defines the interfaces, services, protocols, and data formats for a particular class or domain of applications is called a profile. The Application Portability Profile (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 Federal information technology requirements.

This report is designed to provide recommendations on a variety of specifications that will generally fit the requirements of U.S. Government information systems. A specific organization will not necessarily require all of the recommended specifications in the APP. As the U.S. Government's OSE profile, this guidance is provided to assist Federal agencies in making informed choices regarding the selection and use of OSE specifications, and in the development of more selective application profiles based on the APP. It is directed toward managers and project leaders who have the responsibilities of acquiring, developing, and maintaining information systems supported by heterogeneous application platform environments.

The APP is <u>not</u> a standard and is not designed to cover every case. In some instances, the selection of one specification recommended in the APP will obviate the need for other specifications that are also recommended (i.e., select one or the other, but not both). There is some overlap in functionality covered in different specifications. There are also gaps in functionality. In areas where the APP does not meet all of a user's requirements, the user must augment the recommended specifications to ensure that proposed systems built on these specifications meet organizational requirements. This report is designed to help users determine which specifications to use.

Not only is the U.S. Government involved in the development of profiles, but industry, national, and international organizations are preparing specifications that encompass numerous types of profiles. Corporations such as American Airlines, Boeing, DuPont, General Electric, Kodak, McDonnell Douglas, Merck, Motorola, Northrop, and Unilever are developing profiles for use within their own organizations and in many cases have based these profiles on the APP. The Institute of Electrical and Electronics Engineers, the International Organization for Standardization, and other standards-making organizations are in the process of developing profiles for specific types of application domains. U.S. Government organizations that are engaging the concepts of organizational profiles include the U.S. Army Sustaining Base Information Services, the U.S. Bureau of the Census, the Internal Revenue Service, the Defense Information Systems Agency, and many others.

Many specifications were reviewed and evaluated before the final recommended specifications were selected. If there are other specifications that should be considered in the APP and that meet a broad range of U.S. government application requirements, users, vendors, and other interested

parties should formally recommend them for evaluation using the same evaluation criteria applied to the selected specifications. This is one of the ways in which the APP will continue to evolve as technology evolves.

This report is one in a family of reports concerning the open system environment. These reports cover various aspects of the OSE and include the following:

- NIST Special Publication 500-220 "Guide on Open System Environment (OSE) Procurement"

- NIST Special Publication 800-7 "Security in Open Systems"

- Forthcoming publication of NIST Interim Report (NISTIR) "Operations and Administrations Requirements"

- Forthcoming publication of NIST Interim Report (NISTIR) "Open System Environment (OSE) Architectural Framework for Services and Specifications"

These reports, and other planned reports, provide the context for the APP and the impact of future developments and evolution on open systems.

The initial version of the APP was published by the National Institute of Standards and Technology (NIST) in April 1991 as Special Publication 500-187. Version 2 of the APP Guide, NIST Special Publication 500-210, was published in June 1993. The changes in this third revision reflect the evolutionary developments that have occurred in the standards arena. Examples of the types of changes in this version include the following:

a) The introductory material incorporates work done by the Institute of Electrical and Electronics Engineers (IEEE) POSIX Working Group 1003.0 on the Open System Environment Reference Model (OSE/RM).

b) The evaluation criterion, *de facto usage*, has been removed and others have been reworded to provide more usable definitions.

c) A new *bindings* information item has been added to individual specifications where appropriate.

d) All of the recommended specifications have been updated and many new ones have been added. Areas that have seen the most change are those that encompass data interchange and communications where numerous new specifications have been added.

Specific changes between Version 2 and Version 3 recommended specifications include the following:

a) Operating System Services
IEEE 1003.2-1992 POSIX Shell is now FIPS 189.
IEEE 1003.4 Realtime is now IEEE 1003.1b.

IEEE 1003.6 Security is now IEEE 1003.1e and IEEE 1003.2c.
IEEE P1387.2, .3, and .4 are new.

b) Human/computer Interface Services
Proposed FIPS 158-1 X Window System is now officially FIPS 158-1.
IEEE P1295 X Window Toolkit is now IEEE 1295.1.

c) Software Engineering Services
FIPS 119 Ada is now FIPS 119-1 Ada.
FIPS 21-3 COBOL is now FIPS 21-4 COBOL.
FIPS 119 Pascal has been deleted due to very limited interest in this specification.
ECMA PCTE has been replaced by ISEE Repository ISO/IEC 13719-1.

d) Data Management Services
FIPS 127-1 SQL is now FIPS 127-2.
FIPS 193 SQL Environments is new.

e) Data Interchange Services
ODA/ODIF/ODL ISO 8613 has been deleted due to lack of implementations.
Draft Portable Document Delivery Format (PDDF) is new.
SPDL ISO 10180 has been deleted and replaced by PDDF.
Standard Data Elements ISO 11179 Parts 3, 4, and 5 are new.
FIPS 194 Raster is new.
JPEG is new.
MPEG is new.
ISO 9660 is new.
STEP ISO 10303 has been replaced by the planned FIPS on STEP.
FIPS 173 SDTS is now FIPS 173-1.

f) Graphics Services
FIPS 153 PHIGS is now FIPS 153-1.

g) Network Services
PII API P1003.12 has been renamed P1003.1g.
IEEE 1238.1 FTAM has been deleted. (This specification is included as part of FIPS 146-2.)
FIPS 146-1 GOSIP is now FIPS 146-2 POSIT.
ISDN is now FIPS 182 ISDN.
IEEE 1003.8 TFA has been deleted. (This specification is included as part of FIPS 146-2.)
CORBA is new.
FIPS 179 GNMP has been deleted and replaced with OMNI*Point*.
FIPS 192 GILS is new.
NISO Z39.50 is new.
FIPS 46-2 DES is new.
FIPS 186 DSS is new.

The universe of OSE is continually evolving and the APP Guide will strive to reflect this evolution. The Computer Systems Laboratory (CSL) welcomes any recommendations for changes to the APP. Such recommendations may be sent to the following:

Via postal mail: National Institute of Standards and Technology
Editor, APP Guide
Building 225, Room B266
Gaithersburg, MD 20899

Via FAX: Editor, APP Guide
(301) 926-3696

How to Use this Report

A warning must be given to users of this report. Wholesale inclusion of sections in this report in procurement documents through statements such as "Products shall conform to the APP," or similar wording, is a misuse of this information. Such actions will not guarantee that the acquiring organization has adequately addressed organizational and technical requirements. As a matter of fact, such actions will probably ensure that an organization will not move in the intended direction. Some specifications overlap others, and the selection of one specification may conflict with or prevent the use of another. For these reasons, it is incumbent on users to be aware of the choices that must be made in using any particular set of standards and other specifications. This normally requires expert knowledge in applying each of the individual specifications, the pertinent options to be used, appropriate values for parameters, and the interactions among different specifications.

The intended use of this report is as a catalog from which thoughtful selections can be made in response to clearly defined user requirements. Individual recommendations and specifications in this report must be reviewed by the acquiring agencies to determine if they are applicable to a specific acquisition and whether or not the specifications are adequate to describe the organization's requirements. In addition, inasmuch as there is overlap among some of the specifications recommended, the acquiring agencies must ensure that requirements do not conflict with one another, nor with internal organizational policy.

A suggested means of gathering information and lessons-learned in using this report is the "Guide on Open System Environment (OSE) Procurements," NIST Special Publication 500-220. It describes many of the decisions that have to be made in developing the requirements for an OSE based on the APP and provides text that can be used in statements of work for acquisition and transition to the OSE.

Contents

CLAUSE PAGE

1. INTRODUCTION 1
   1.1 Scope 1
   1.2 Purpose 2

2. ACRONYMS 3

3. OPEN SYSTEM ENVIRONMENT 7
   3.1 OSE Reference Model 8
   3.2 OSE Profile and the APP 10
   3.3 APP Service Areas 11
      3.3.1 Operating System Services 12
      3.3.2 Human/Computer Interface Services 13
      3.3.3 Software Engineering Services 14
      3.3.4 Data Management Services 15
      3.3.5 Data Interchange Services 15
      3.3.6 Graphics Services 16
      3.3.7 Network Services 16

4. APP SPECIFICATIONS 17
   4.1 Publicly Available Specifications 17
   4.2 Specification Evaluation 17
   4.3 Evaluation Criteria 18
   4.4 Additional Information on Specifications 19
   4.5 Federal Information Processing Standards 20
   4.6 FIPS Testing 20
   4.7 Validated Products List 21
   4.8 Operating System Services 22
      4.8.1 Kernel Operations API 22
      4.8.2 Operating System Commands and Utilities 23
      4.8.3 Operating System Realtime Services 25
      4.8.4 Operating System Security API 26
      4.8.5 Operating System Security Commands 27
      4.8.6 System Management 28
   4.9 Human/Computer Interface Services 29
      4.9.1 Graphical User Interface 30
      4.9.2 Graphical User Interface Toolkit 31
   4.10 Software Engineering Services 33
      4.10.1 Programming Language Ada 33
      4.10.2 Programming Language C 34
      4.10.3 Programming Language COBOL 35
      4.10.4 Programming Language Fortran 36

4.10.5 Integrated Software Engineering Environment Repository 37
4.11 Data Management Services 39
4.11.1 Relational Database Management System 39
4.11.2 Data Dictionary/Directory System 41
4.11.3 Distributed Data Access 42
4.11.4 Database Environment 44
4.12 Data Interchange Services 45
4.12.1 Document Markup Language 46
4.12.2 Document Distribution Format 47
4.12.3 Manuscript Markup Tag Set 48
4.12.4 Data Element Specification 49
4.12.5 Graphics Data Interchange 50
4.12.6 Raster Image Interchange 51
4.12.7 Image Compression 53
4.12.8 Video Compression 55
4.12.9 Compact Disk File and Directory System 56
4.12.10 Graphical Product Data Interchange 57
4.12.11 Product Lifecycle Data Interchange 59
4.12.12 Electronic Data Interchange 60
4.12.13 Spatial Data Interchange 61
4.13 Graphics Services 62
4.13.1 Two-Dimensional Graphics 63
4.13.2 Interactive and Three-dimensional Graphics 64
4.14 Network Services 65
4.14.1 Communication API for Protocol Independent Interfaces 65
4.14.2 Communication API for OSI Services 67
4.14.3 Communication Protocols 68
4.14.4 Communication API for Integrated Digital, Video, and Voice 69
4.14.5 Communication Protocols for Integrated Digital, Video, and Voice 70
4.14.6 Remote Procedure Call 71
4.14.7 Object Request Broker 72
4.14.8 Electronic Messaging API 75
4.14.9 Directory Services API 76
4.14.10 Network Management 77
4.14.11 Network Information Locator 78
4.14.12 Distributed Information Service 79
4.14.13 Data Encryption 80
4.14.14 Digital Signatures 82

5. STRATEGIC EVALUATIONS 83

6. CONCLUSION 86

ANNEX A — DOCUMENT SOURCES: CONTACT INFORMATION 87

ANNEX B — BIBLIOGRAPHY 93

INDEX 94

Figures

Figure 1. Open System Environment Reference Model (OSE/RM). 9
Figure 2. APP Service Areas and the OSE/RM. 11
Figure 3. Example Summary Status Report. 18

Tables

Table 1. Strategic Value of APP Specifications 84

1. INTRODUCTION

Federal agencies are under increasing pressure to use information technology to improve efficiency and delivery of services to the public. Key aspects of the reality with which Federal agencies have to deal are the following:

a) Agencies recognize that they no longer can create de jure standards and enforce them on the commercial market as they were able to do with early standards.

b) Agencies must rely on the commercial market for information technology products and services. Commercial-off-the-shelf (COTS) products are the preferred choice rather than custom-built systems.

c) Agencies must establish strategies and plans for acquiring information technology products and services based upon open system standards that support application software interoperability, portability, and scalability.

Systems within Federal agencies typically were developed in an environment of isolated islands of computing. Now there is interdependence of users and systems across the entire organization. This interdependence has served to highlight enterprise-wide needs for common application architectures, communication networks, databases, security, and management capabilities. It also has raised concerns about the need to address those issues from policy, management, and technical perspectives.

One of the most significant factors underlying the changing technology is that Federal and nonfederal users now recognize that no single vendor can supply all of their needs for information technology systems and services. Since very large homogeneous environments are no longer practical in many cases, users need open systems that provide interoperability of products and portability of people, data, and applications that are distributed throughout heterogenous computing environments.

The need to improve portability and interoperability has resulted in widespread interest in standards such as the Portable Operating System Interface (POSIX) and communications standards. Whereas development of these standards are important milestones in the effort to achieve portability and interoperability, operating system and communications standards are not sufficient to address the full spectrum of needs, even within their stated scopes of concern.

1.1 Scope

The focus of this guide is on open system environments (OSE) which integrate standards and other specifications to provide the functionality necessary to address a broad range of Federal information technology requirements. The usefulness of the APP is in the eye of the beholder. If it is applicable in the minds of those who are using it, and implementations work and provide the intended functionality, then the recommended specifications are applicable in reality. The APP does not define an open system, nor does it guarantee that an open system environment will result from its

use. The APP does, however, provide a common starting point for deciding what is required in building open systems based on standards and common infrastructure.

The guidance is intended to assist Federal agencies in making informed choices regarding the selection and use of OSE specifications and in the development of OSE profiles. This guidance is directed toward managers and project leaders who have the responsibilities of acquiring, developing, and maintaining information systems supported by heterogeneous hardware, software, and communications environments. Applications in an OSE may include management information systems, embedded systems, realtime systems, transaction processing systems, database systems, geographical information systems, or other systems in which the recommended specifications might apply and provide utility. Since the specifications described are highly technical in nature, users of this guidance should consult with subject area experts to determine the applicability of each specification to a particular organizational objective.

Ideally, specifications would be expressed in terms of international standards. There are some areas of OSE functionality that do not have formal standards, much less international standards. Although this situation will improve over time, users who have requirements for those functions are faced with the question, "What specifications should I use now?"

1.2 Purpose

The Application Portability Profile (APP) is directed toward assisting managers, project leaders, and users in making an informed judgment regarding the choice of specifications to meet current requirements. There are two dimensions of the assistance provided. First, specifications are provided for each service area described in the APP. The specifications represent the collective judgment of the National Institute of Standards and Technology (NIST) Computer System Laboratory's (CSL) staff regarding the most appropriate specification for each functional area. Second, and equally as important, evaluation criteria to assist in making qualitative assessments of the recommended specifications are defined and applied. Application of these evaluation criteria resulted in the NIST assessments of the suitability of the specifications recommended.

Users of the APP should use the evaluation criteria to make their own assessments of the recommended specifications. Further, users should consider assigning weighted values to elements of the criteria based on their judgments of the relative importance to be given to each element. Users should also consider requiring vendors to use the evaluation criteria to assess specifications that the vendors choose to propose as an alternative to the specifications recommended in this document.

The following sections briefly describe the meaning of open system environment, the OSE Reference Model, and specific components of the Application Portability Profile. Later sections provide recommended specifications for each APP component. References for further information and addresses of organizations that distribute documents on the recommended specifications are included toward the end of this report.

2. ACRONYMS

The acronyms used throughout this report are defined in this section.

AAP: Association of American Publishers
ACSE: Association Control Service Element
ADL: Assertion Definition Language
AJPO: Ada Joint Program Office
ANS: American National Standard
ANSI: American National Standards Institute
AOW: Asiatic Oceania Workshop
API: Application Program Interface
APP: Application Portability Profile
APTL: Accredited POSIX Testing Laboratory
ASI: Application Software Interface
ASME: American Society of Mechanical Engineers
ASN.1: Abstract Syntax Notation One
BRI: Basic Rate Interface
BSD: Berkeley Systems Development
CAD/CAM: Computer-Aided Design and Manufacturing
CADETC: CAD/CAM Data Exchange Technical Centre
CAE: Computer Application Environment
CASE: Computer-Aided Software Engineering (See ISEE)
CCITT: International Telegraph and Telephone Consultative Committee (renamed International Telecommunication Union—Telecommuncations Standardization Sector [ITU-T])
CD: compact disk
CD-ROM: compact disk read-only memory
CGM: Computer Graphics Metafile
CMP: Completeness
CNIDR: Clearinghouse for Networked Information Discovery and Retrieval
COBOL: Common Business Oriented Language
CORBA: Common Object Request Broker Architecture
COS: Corporation for Open Systems
COSMIC: Computer Software Management and Information Center
CSL: Computer Systems Laboratory (part of NIST)
DAC: Discretionary Access Control
DBMS: Database Management System
DCE: Distributed Computing Environment
DIA: Defense Intelligence Agency
DIS: Draft International Standard
DISA: Defense Information Systems Agency
DNI: Detailed Network Interface
DPANS: Draft Proposed American National Standard
DoD: Department of Defense
DTD: Document Type Definition
ECMA: European Computer Manufacturers Association (name changed to "ECMA: Standardizing Information and Communications Systems"; ECMA is no longer an acronym in this context)

ECMA/TC33: ECMA: Standardizing Information and Communications Systems/Technical Committee 33
EDI: Electronic Data Interchange
EDIFACT: Electronic Data Interchange For Administration, Commerce, and Transport
EEI: External Environment Interface
EMPM: Electronic Manuscript Preparation and Markup
EPRI: Electric Power Research Institute
EWOS: European Workshop on Open Systems
FDDI: Fiber Distributed Data Interface
FIPS: Federal Information Processing Standard
GCA: Graphics Communication Association
GIS: Geographic Information System
GKS: Graphical Kernel System
GORD: GOSIP Register Database
GOSIP: Government Open System Interconnection Profile
GUI: Graphical User Interface
HCI: Human/Computer Interface
ICCCM: Inter-Client Communications Conventions Manual
IDRP: Inter-Domain Routing Protocol
IEC: International Electrotechnical Commission
IEEE: Institute of Electrical and Electronics Engineers
IGES: Initial Graphics Exchange Specification
IGOSS: Industry/Government Open Systems Specification
INTAP: Interoperability Technology Association for Information Processing
IRDS: Information Resource Dictionary System
IS-IS: Intermediate System-Intermediate System
ISDN: Integrated Services Digital Network
ISEE: Integrated Software Engineering Environment
ISO: International Organization for Standardization
ISO/IEC: International Organization for Standardization/International Electrotechnical Commission
ITI: Information Technology Industry Council (formerly Computer Business Equipment Manufacturers Association [CBEMA])
ITU: International Telecommunication Union
ITU-T: International Telecommunication Union—Telecommuncations Standardization Sector [ITU-T] (formerly CCITT)
JITC: Joint Interoperability Test Command
JTC1: Joint Technical Committee One
JPEG: Joint Photographic Experts Group
LAN: Local Area Network
LAPD: Link Access Procedure on the D channel
LIS: Language Independent Specification
LOC: Level of Consensus
M: Programming language (previously known as MUMPS)
MAC: Mandatory Access Control
MAN: Metropolitan Area Network
MAP/TOP: Manufacturing Automation Protocol/Technical and Office Protocols
MAT: Maturity

MHS: Message Handling Service
MIME: Multipurpose Internet Mail Extensions
MPEG: Motion Pictures Expert Group
NASA: National Aeronautics and Space Administration
NBSIR: National Bureau of Standards Interim Report
NCC: National Computing Centre
NCGA: National Computer Graphics Association
NCSC: National Computer Security Center
NI-X: Bellcore National ISDN-X
NISO: National Information Standards Organization
NIST: National Institute of Standards and Technology
NISTIR: National Institute of Standards and Technology Interim Report
NIU-Forum: North American ISDN Users' Forum
NIUF: North American ISDN Users' Forum
NTIS: National Technical Information Service
NVLAP: National Voluntary Laboratory Accreditation Program (NIST-sponsored program)
OIW: OSE Implementor's Workshop
OMG: Object Management Group
OSE: Open System Environment
OSE/RM: Open System Environment Reference Model
OSF: Open Software Foundation
OSI: Open System Interconnection
PAV: Product Availability
PCTE: Portable Common Tools Environment
PDES: Product Data Exchange using STEP
PDDF: Portable Document Delivery Format
PDF: Page Description Format
PHIGS: Programmer's Hierarchical Interactive Graphics System
PII: Protocol Independent Interfaces
POSIT: Profiles for Open Systems Internetworking Technologies
POSIX: Portable Operating System Interface (POSIX)—System Application Program Interface [C Language]
PRI: Primary Rate Interface
PRL: Problems/Limitations
RDA: Remote Database Access
RPC: Remote Procedure Call
SDIF: Standard Document Interchange Format
SDTS: Spatial Data Transfer Specification
SGML: Standard Generalized Markup Language
SHA: Secure Hash Algorithm
SNI: Simple Network Interface
SPDL: Standard Page Description Language
SQL: Structured Query Language
STB: Stability
STEP: Standard for the Exchange of Product Model Data
SVID: System V Interface Definition
TEI: Text Encoding Initiative

TET: Test Environment Toolkit
TFA: Transparent File Access
UAC: User Advisory Council
UI: UNIX International
UN/ECE/WP.4: United Nations Economic Commission for Europe, Working Party Four on Trade Facilitation
USGS: U.S. Geological Survey
VAN: Value-Added Network
VPL: Validated Products List
WAN: Wide Area Network
WYSIWYG: What You See Is What You Get
X3: Standards Committee X3 - Information Technology
XTI: X/Open Transport Interface

3. OPEN SYSTEM ENVIRONMENT

From the perspective of users and technologists alike, an open system environment (OSE) consists of a computing support infrastructure which facilitates the acquisition of applications that—

a) execute on any vendor's platform;
b) use any vendor's operating system;
c) access any vendor's database;
d) communicate and interoperate over any vendor's networks;
e) are secure and manageable; and
f) interact with users through a common human/computer interface.

In more technical terms, an OSE is a computing environment that supports interoperable, portable, and scalable applications through standard services, interfaces, data formats, and protocols. The standards defining these elements may consist of international, national, industry, or other open (public) specifications. These specifications are available to any user or vendor for use in building systems and products that meet OSE criteria.

The three major concepts of open systems are interoperability, portability, and scalability of applications. These terms are defined as follows:

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

- 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. An indirect effect of portability combined with interoperability provides a basis for user portability, i.e., that users are able to move among applications and transfer skills learned in one operating environment to another.

- 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. The concept extends portability to various scales of operating environments, such as local area networks versus wide area networks, distributed databases versus centralized databases, etc.

An application is 1) a logical grouping of activities, and their related data and technology, which constitutes a cohesive unit; an application is part of an information system; it is comprised of a group of programs (i.e., software) or information resources designed to process data into desired information; 2) a logical grouping of programs, data, and technology with which an end-user interacts to perform a specific function or class of functions.

There is a continuum in the relationship between an application and its environment. The degree to which an application is tied to a particular environment determines its portability, scalability, and interoperability. The following illustrates:

The hardware driver is inextricably tied to the hardware for which it is written and is very difficult, if not impossible, to port to other environments. The payroll update, on the other hand, should lend itself well to the aspects of portability, scalability, and interoperability, if it is written in a manner fitting the OSE.

Applications in an OSE are portable insofar as they are written in a standardized programming language. Additionally, they are wrapped in standard interfaces that connect them to the computing environment. They produce and accept standard data formats, and communicate using standardized protocols when executing in any computing environment.

Applications are scalable among a variety of platform and network configurations, from standalone microcomputers, to large distributed systems that may include microcomputers, workstations, minicomputers, mainframes, and supercomputers, or any configuration in between. The existence of greater or fewer computing resources on any platform will be apparent to users only in the context that they affect the application's speed of execution, for example in how fast screens are refreshed or data is retrieved, or the capacity of each platform to process data (i.e., 16-bit data bus versus a 32-bit bus).

Applications interoperate by using standard communication protocols, data interchange formats, and distributed system interfaces to transmit, receive, understand, and use information. The process of moving information from one platform, through a local area network, wide area network, or combination of networks to other platforms should be transparent to the application and the user. Locations of other platforms, users, databases, and programs should also be transparent.

In short, an OSE supports applications through the use of well-defined components: a plug-compatible technology or building-block approach for developing systems.

Unfortunately, not enough standards are in place to define an OSE completely. Standards organizations are working on this problem, but much effort is still needed. As technology changes, some standards will become obsolete and other new ones will be required. Organizations can still accomplish a great deal in moving toward an OSE by selecting specifications that will provide greater openness over time.

3.1 OSE Reference Model

The Institute of Electrical and Electronics Engineers (IEEE) POSIX Working Group 1003.0 defines an OSE Reference Model (OSE/RM) that provides a framework for describing open system concepts and defining a lexicon of terms that can be agreed upon generally by all interested parties.

The OSE/RM is also identified at the international level in Joint Technical Committee 1 (JTC1) Technical Report (TR) 14252. Figure 1 illustrates the OSE/RM.

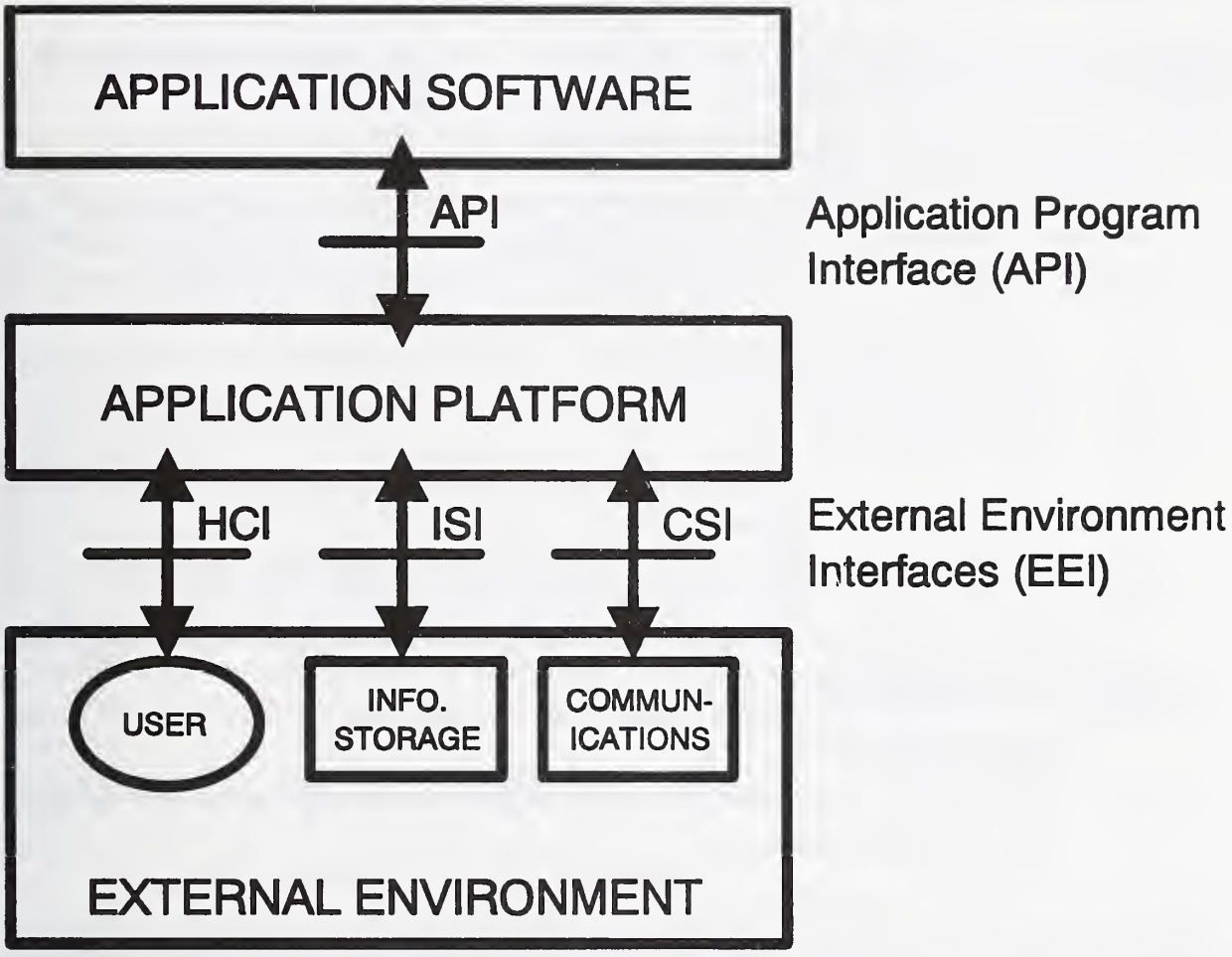


Figure 1. Open System Environment Reference Model (OSE/RM).

Two types of elements are used in the model: entities consisting of the application software, application platform, and platform external environment; and interfaces including the application program interface and external environment interface.

The three classes of OSE reference model entities are described as follows:

a) **Application Software** — Within the context of the OSE Reference Model, the application software includes data, documentation, and training, as well as programs.

b) **Application Platform** — The application platform is composed of the collection of hardware and software components that provide the generic application and system services.

c) **Platform External Environment** — The platform external environment consists of those system elements that are external to the application software and the application platform (e.g., services provided by other platforms or peripheral devices).

There are two classes of interfaees in the OSE reference model: the application program interface and the external environment interface.

a) **Application Program Interface (API)** — The API is the interface between the application software and the application platform. Its primary function is to support portability of application software. An API is categorized in accordance with the types of service accessible via that API. There are four types of API services in the OSE/RM:

   1) Human/computer interface services
   2) Information interchange services
   3) Communication services
   4) Internal system services

b) **External Environment Interface (EEI)** — The EEI is the interface that supports information transfer between the application platform and the external environment, and between applications executing on the same platform. Consisting chiefly of protocols and supporting data formats, the EEI supports interoperability to a large extent. An EEI is categorized in accordance with the type of information transfer services provided. There are three types of information transfer services. These are transfer services to and from:

   1) Human users
   2) External data stores
   3) Other application platforms

In its simplest form, the OSE/RM illustrates a straightforward user-supplier relationship: 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.

3.2 OSE Profile and the APP

A profile consists of a selected list of standards and other specifications that define a complement of services made available to applications in a specific domain. Examples of domains might include a workstation environment, an embedded process control environment, a distributed environment, a transaction processing environment, or an office automation environment, to name a few. Each of these environments has a different cross-section of service requirements that can be specified independently from the others. Each service, however, is defined in a standard form across all environments.

An OSE profile is composed of a selected list of open (public), consensus-based standards and specifications that define services in the OSE/RM. Restricting a profile to a specific domain or group of domains that are of interest to an individual organization results in the definition of an organizational profile. The Application Portability Profile (APP) is an OSE profile designed for use by the U.S. Government. It covers a broad range of application software domains of interest to

many Federal agencies, but it does not include every domain within the U.S. Government's application inventory. The individual standards and specifications in the APP define data formats, interfaces, protocols, or a mix of these elements.

3.3 APP Service Areas

The services defined in the APP tend to fall into broad *service areas*. These service areas are:

a) operating system services (OS)
b) human/computer interface services (HCI)
c) data management services (DM)
d) data interchange services (DI)
e) software engineering services (SWE)
f) graphics services (GS)
g) network services (NS)

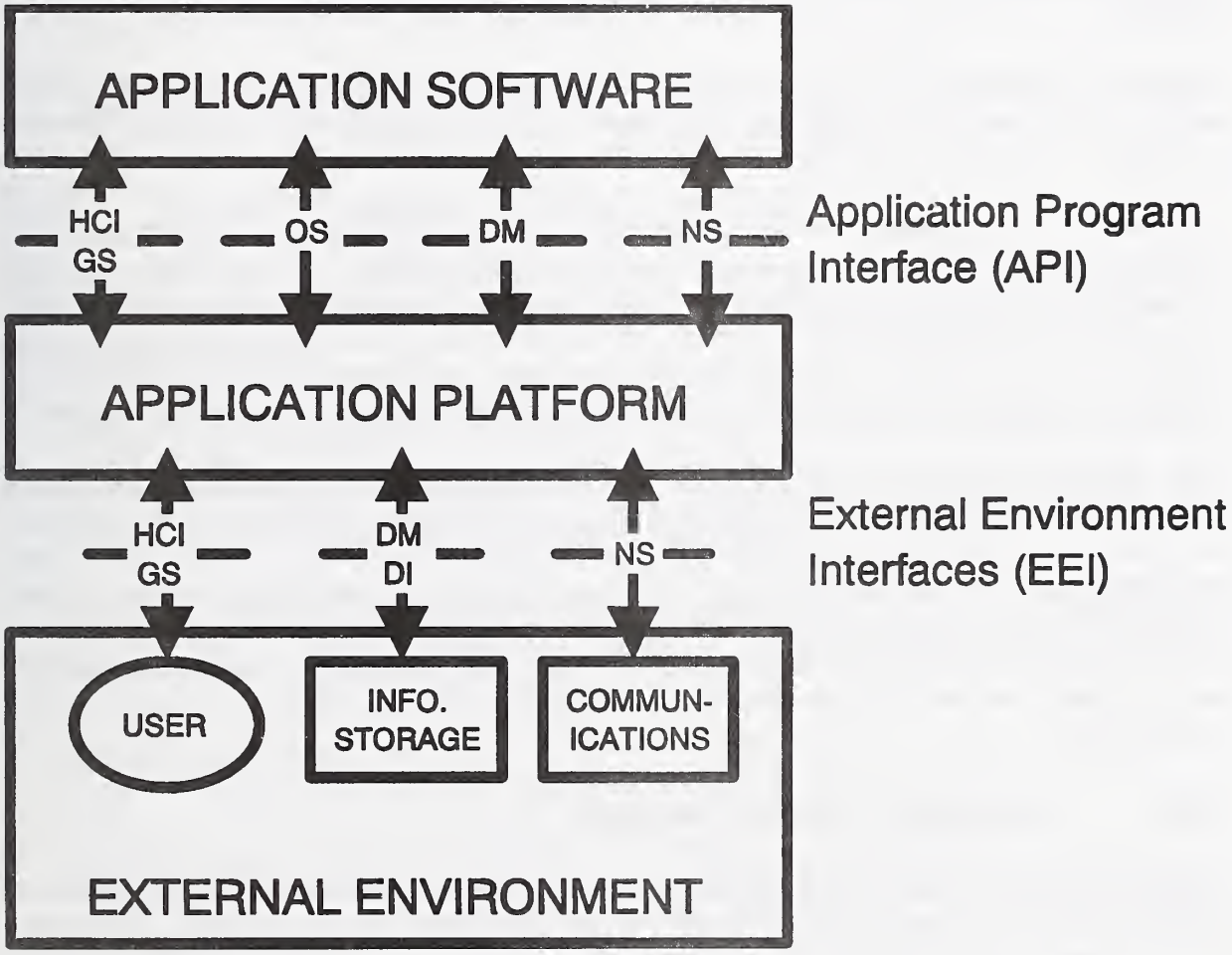


Figure 2. APP Service Areas and the OSE/RM.

Each service area is defined in the following sections. Figure 2 illustrates where each of these services areas relates to the OSE/RM. (Assume that software engineering services are applicable in all areas.)

Each of the APP service areas addresses specific components around which interface, data format, or protocol specifications have been or will be defined. Security and management services are common to all of the service areas and pervade these areas in one or more forms.

Security as applied to both stand-alone and distributed systems takes a holistic approach. Each component provides different elements of functionality and security service. Security services are provided to support the secure distribution and integrity of information and to protect the computing infrastructure from unauthorized access. Security policy, authority, domains, and interactions among these domains are specifically defined in IEEE P1003.22 *Draft Guide for POSIX Open Systems Environment—A Security Framework.* Security is a cross-category service and part of the overall context in which information systems must operate. It is of relevance within all system functions, for example system services, communications services, and data management services.

Currently, specifications for security can be recommended in operating system services, network services, and access control and integrity constraints for data management services. Specifications for security in the other service areas are not sufficiently advanced to warrant inclusion at this time.

Distributed system management is coming to be regarded as the integration of distinct, supporting management areas. Among these areas are system administration, communication (network) management, information management, and human/computer interface management. Management services provide the mechanisms to monitor and control the operation of individual applications, databases, systems, platforms, networks, and user interactions with these components. Management services also enable users and systems to become more efficient in performing required work.

These services are just now being addressed by standards development organizations (SDO) and user consortia, particularly for heterogeneous systems. The disparate mechanisms necessary for competent management of distributed systems require an integrated approach to assure consistency. Standardization is being developed by many committees in various SDOs, workshops, and consortia. Recent attempts by these committees has led to closer coordination. True integration among them, however, requires significant additional effort. As specifications for management services mature and stabilize, they will be reviewed and appropriate ones may be selected for use in the APP.

3.3.1 Operating System Services

Operating system services are the core services needed to operate and administer the application platform and provide an interface between application software and the platform. These core 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 the external environment.

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) Realtime 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 and 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, authorization of resource usage, and system backup.

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

3.3.2 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 interfaces 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 interface management systems; and the security labeling of information on displays and other output devices.

User interfaces are often the most complex part of system development and maintenance. Within the past few years, significant advances have been made in user interface technology in both ease-of-use and in reducing the development effort required.

The principal components of a window system are a video interface that contains one or more windows or panels; a pointing device such as a mouse or touch screen; and a set of objects on the screen that can be directly manipulated by the user through the pointing device or through keyboard responses.

Multimedia, in the world of information processing, is a general term that describes the integration of different information representations, such as text, sound, and video, within a single presentation session, especially within a common user interface. In addition to the traditional text and line graphics, multimedia applications often include scanned images, part- or full-motion video with or without synchronized audio, and digitized sound or music. Some of the key challenges in identifying and defining standards associated with this area include: analog to digital conversions, compression and storage of large data sets, synchronization of time-dependent representations such as video with sound, and multi-channel input and output.

3.3.3 Software Engineering Services

The production and use of portable, scalable, interoperable software is the objective of open systems. Software engineering services provide the infrastructure to develop and maintain software that exhibits the required characteristics. Standard programming languages and software engineering tools and environments become central to keeping with this objective. The required capabilities are provided by software engineering services which include the following:

a) Programming languages and language bindings for COBOL, FORTRAN, Ada, and C.

b) Integrated software engineering environments (ISEE) and tools include systems and programs that assist in the automated development and maintenance of software. These include, but are not limited to, tools for requirements specification and analysis, for design work and analysis, for creating and testing program code, for documenting, for prototyping, and for group communication. The interfaces among these tools include services for storing and retrieving information about systems and exchanging this information among the various programs in the development environment.

c) Software Engineering security services provide the means to control access to and integrity of programming objects such as libraries, program code, etc., and the tools or information that provide the infrastructure for development of software.

While applications do not necessarily make direct use of software engineering services, without these services, much of the automating of processes would be much more difficult and error-prone. Without the use of programming languages, none of these capabilities would be possible. Software engineering services transform the capabilities of hardware and communications links into the automated processes that are available to system users.

3.3.4 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, maintained indefinitely, and shared among many processes. Data management services include the following:

a) Data dictionary/directory services allow users and programmers to access and modify metadata (i.e., data about data). Such data may include internal and external formats, integrity and security rules, and other characteristics and attributes. The data may be located within a stand-alone or distributed system.

b) Database management system (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 schemas. 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.

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

d) Data management security services 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.

3.3.5 Data Interchange Services

Data interchange services 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 design and 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.

There are various levels of complexity of data interchange. At the lowest level of complexity is the ability to define representations for the data to be interchanged. A representation might be defined as a language or a data format. The next higher level represents content. Text, raster images, and audio are examples of different content types. Above this level are object representations where different content types may be combined to form a complex data representation, such as a complex document. Above the object level is the language level. The language level is suitable for humans to understand what is being represented. The highest level of complexity is the application level. The application level uses any of the lower levels of representation to interchange data with another application, such as transmitting digitized video or sound through a teleconferencing center.

3.3.6 Graphics Services

Graphics services provide functions required for creating and manipulating displayed images. These services include—

a) Display element definition and management services provide mechanisms for defining, manipulating, and managing graphical drawing elements.

b) Image attribute definition services include the capabilities necessary to describe dimensions (i.e., 2- and 3-dimensional attributes), and interaction functions.

c) Graphics security services include those necessary to protect the integrity of and access to nontext data, such as graphical images (e.g., checksums on display bitmaps compared to file contents after encoding/decoding or compression/decompression techniques have been applied).

The services are defined in specifications for describing multidimensional graphic objects and images in a form that is independent of devices.

3.3.7 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/micro computer 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.

4. APP SPECIFICATIONS

Ideally, all specifications would be expressed in terms of international standards. There are areas of OSE functionality for which formal standards, much less international standards, do not exist. Although this situation will improve over time, users who have requirements for those functions are faced with the question, "What specifications should I use now?"

4.1 Publicly Available Specifications

In some cases, there are no publicly available *open* specifications that pertain directly to a specific service area component. In those cases, CSL has tried to recommend a specification that at least partly covers the required functionality. In other cases, CSL has recommended specifications that are not entirely open as stop-gap measures, recognizing the fact that users need guidance now.

Publicly available specifications that may not be Federal standards can be used in some instances to fill the gaps between existing standards. CSL does not advocate that organizations should use the specifications in these cases without knowledge of the associated risks and adverse effects of such use (e.g., difficulty in porting applications later in a system's life, justifying the use of non-open specifications, etc.). If another specification appears to meet an organization's requirements more fully, then CSL recommends that the organization choose the one that meets those requirements the best. For a broad range of Federal applications and organizations, however, CSL can offer some insight into minimizing problems and managing those that cannot be solved directly at this time.

4.2 Specification Evaluation

The following sections describe the recommended specifications for each of the APP services and summarize some of the pros and cons of selecting each specification. The information is provided to managers, technical project leaders, and users to assist them in evaluating these specifications for inclusion in application or organizational profiles. These evaluations may be used to compare specifications listed in this guide to other specifications that an organization may be considering.

Each service area is preceded by a summary status report of all specifications reviewed in this report for that particular service area. An example of an entry from one of the summary status

reports is presented in figure 3. Subsections of each service area describe specific evaluation criteria for the specification.

The summary status report relates the results of major evaluation criteria (e.g., level of consensus, completeness, etc.) to a graphic representation. With one view, all of the specifications in a particular service area can be compared to determine relative coverage of the area. Users may use this information to determine where they should concentrate their efforts in tailoring and augmenting application and organizational profiles.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	PRL
REALTIME IEEE 1003.1b-1993	O	O	O	●	O	O

Legend: ●-high evaluation O-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
PRL -- Problems/limitations

Figure 3. Example Summary Status Report.

4.3 Evaluation Criteria

Each of the specifications is evaluated according to how well it meets the requirements of a specific criterion. The criteria are defined as follows:

a) Level of consensus—A low evaluation is given to specifications that are proprietary or are used by a very limited or specialized group of users, such as vendor consortia; a high evaluation is given for a specification that has already become a national or international standard; average evaluations are assigned for public domain specifications that are not standard, or that may be in the process of becoming a standard (i.e., standards committee work-in-progress), or that are widely available across various hardware/software platforms.

b) Product availability—A low evaluation is given to specifications for which only a very few proprietary products are available; high evaluations are given to specifications for which there is a wide variety of products available from various vendors across different application platforms; average evaluations are assigned to specifications that may be proprietary but have many products available from a variety of vendors, or that are public domain specifications with products readily available.

c) Completeness—A specification is evaluated on the degree to which it defines and covers key features necessary in supporting a specific functional area or service. For example a network security specification that includes all of the components described would be evaluated higher than others that do not include all of the features.

d) Maturity—According to the underlying technology of a specification, a high evaluation indicates that it is well-understood (e.g., a reference model is well-defined, appropriate

concepts of the technology are in widespread use, the technology may have been in use for many years, a formal mathematical model is defined, etc.). A low evaluation indicates that it may be based on technology that has not been well-defined and may be relatively new.

e) Stability—A high evaluation means that the specification is very stable, that no changes are expected within the next 2 years. A low evaluation indicates that significant or many changes are expected within a relatively short time (1 to 2 years), or that incompatibilities exist between current and expected releases of the specification. An average evaluation is given to those specifications that may have known changes forthcoming to replace features in the existing specifications.

f) Problems/limitations—Lower evaluations are assigned to specifications with severe restrictions on use or capabilities (e.g., licensing restrictions) or known problems tend to be too difficult and too numerous to overcome (e.g., new releases of the specification are not compatible with previous releases, or not enough is covered in the standard to be useful). An average evaluation is given to those specifications that require some minor additional facility in order to be fully effective in their intended environment. This additional facility may be provided by a related standard or other specification.

4.4 Additional Information on Specifications

Additional informational items, including the following, are provided where appropriate:

a) Specification title—The full identifying title of the specification for purposes of ordering or reference.

b) Specification available from—Organization from which the specification can be ordered.

c) Publication date—Date on which the publication was released for general use (usually designated on the specification's title page.) For FIPS that will become mandatory, the publication date may be followed by an effective date indicating when it becomes mandatory. The effective date is generally 6, 12, or 18 months after the publication date.

d) Sponsoring organization—Organization responsible for developing or maintaining the specification. (In the case of certain Federal Information Processing Standards [FIPS] that adopt existing national or international standards, the organization responsible for the existing base standard is listed.)

e) Rationale—In a very few cases, a rationale section has been included to describe the reasoning behind a specific recommendation. The intent of this section is to show that a requirements validation process was undertaken before a recommendation was made.

f) Applicability—Description of the OSE service area that covers the recommended specification.

g) Conformance testing—Provides information about current and future plans for conformance testing of products based on the recommended specification. In the case of FIPS testing, each

FIPS publication describes the requirements for testing and the policies that affect such testing. For other specifications, testing may or may not be described in the specification recommended.

h) Bindings—Application program interfaces (API) that are applicable to the recommended specification, such as Graphical Kernel System's (GKS) bindings to Ada, C, and Fortran. These are the subroutine and function calls necessary to use the services of a standard implementation in a particular programming language. Bindings are not applicable to all specifications recommended, such as data interchange formats.

i) Future plans—Published or otherwise-announced directions and long-term plans (i.e., 3 years or more) for individual specifications.

j) Alternative specifications—In some instances, other specifications exist besides the recommended specification. Users may want to review these alternatives before selecting a specification on which to standardize.

4.5 Federal Information Processing Standards

Federal Information Processing Standards (FIPS) are adopted and promulgated under the provisions of Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987. FIPS include standards, guidelines, and technical methods that are developed by NIST, approved by the Secretary of Commerce, and issued for government-wide use.

FIPS frequently adopt standards that have been developed by national and international voluntary industry standards organizations with NIST assistance. This use of voluntary industry standards enables the Federal government to acquire commercially available off-the-shelf technology and to avoid the costs of developing its own standards.

NIST works with industry through voluntary standards committees and through sponsored activities such as the Open System Environment Implementors' Workshop (OIW) and the North American Integrated Services Digital Network Users' Forum (NIUF) to develop the technical agreements that are needed to implement standards in products.

The specific conditions under which standards are applicable to Federal government acquisitions are included in each FIPS. The extent to which each FIPS is compulsory and binding on Federal agencies is determined by the Secretary of Commerce when the FIPS is approved. Heads of agencies are authorized to waive the mandatory use of specific FIPS under certain conditions. Certain government systems are exempted from the use of certain FIPS. These include certain classified computer systems and those that support specialized military and intelligence missions.

4.6 FIPS Testing

Each FIPS specifies whether testing is necessary to validate conformance of implementations. If validation is required, a test policy is produced by CSL for implementing the testing described. The

testing policy is developed to define what requirements must be met for testing, what test suites will be used, what procedures will be followed, and how test failures will be treated.

The National Voluntary Laboratory Accreditation Program (NVLAP), an organization within NIST, accredits laboratories for performing testing for certain FIPS. The accreditation requirements are strict and differ for each standard. Accredited laboratories are generally reaccredited every 2 years.

4.7 Validated Products List

The *Validated Products List* (VPL) contains references to products that have been tested according to the conformance requirements of specific Federal Information Processing Standards (FIPS). Products are listed according to the applicable FIPS under which the product was tested. Listings are of two types: 1) certificate listings indicating that a product was tested according to the applicable FIPS, that test results contained no test failures, and that a Government-approved witness was present for the test; and 2) product registrations indicating that the manufacturer or a third party certifies that a product was tested using an approved test suite according to the applicable FIPS. Product registrations are essentially manufacturers' self-certification of product conformance.

The VPL is updated and published through CSL as a NISTIR several times a year. It is available by subscription through the National Technical Information Service (NTIS ordering number PB94-937304/AS). It is also available in WordPerfect 5.1 electronic form through anonymous FTP on speckle.ncsl.nist.gov (IP address 129.6.59.2) in the vpl directory, or as text files on the World Wide Web at URL "http://speckle.ncsl.nist.gov/~kailey/intro.htm". Note that products may be validated as conforming implementations, but may not be listed in the VPL due to restrictions placed on dissemination of this information by the vendor.

4.8 Operating System Services

Operating system (OS) services include kernel operations, commands and utilities, system management, realtime extension, and security.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	PRL
FIPS 151-2 POSIX	●	●	●	●	●	●
FIPS 189 Shell and Utilities	●	●	●	●	●	●
REALTIME IEEE 1003.1b-1993	O		O	●	O	
SECURITY IEEE 1003.1e				O		
SECURITY IEEE 1003.2c						
SYSTEM MANAGEMENT IEEE P1387.2, .3, and .4	O		●	O	●	O

Legend: ●-high evaluation O-average evaluation blank-low evaluation
LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
PRL -- Problems/limitations

4.8.1 Kernel Operations API

Specification title: FIPS 151-2 Portable Operating System Interface (POSIX)—System Application Program Interface [C Language]

Specification available from: National Technical Information Service (NTIS)

Publication date: April 1993

Sponsoring organization: The Institute of Electrical and Electronics Engineers, Inc. (IEEE)

Applicability: 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 external devices. The FIPS is mandatory for use where POSIX-like requirements are defined.

Level of consensus: The U.S. Government's Federal Information Processing Standard Publication (FIPS) is based on international standard ISO/IEC 9945-1:1990. The FIPS makes certain optional capabilities mandatory for Federal procurements.

Product availability: As of the date of this publication, there were over 100 products validated according to FIPS 151-2 validation requirements on numerous types and classes of platforms.

Completeness: FIPS 151 has undergone change to bring it in line with ISO/IEC 9945-1:1990. This standard does not, however, include other kernel operations that are widely understood as part of the operating system kernel, such as realtime operations or kernel security capabilities. These capabilities will become parts of related standards for augmenting the usability of FIPS 151-2 in the future. For kernel operations, FIPS 151-2 is complete as written.

Maturity: Antecedents of POSIX have existed for 20 years. The current standard was developed over a 12-year period. Much research based on POSIX antecedents has been pursued, which has led to various improvements in the POSIX specification.

Stability: FIPS 151-1 adopted the 1988 IEEE POSIX standard. FIPS 151-2 revised the previous FIPS to bring it into line with the current national (IEEE 1003.1-1990) and international (ISO/IEC 9945-1:1990) standards. No changes are expected within the next 2 to 3 years.

Known problems/limitations: POSIX consists of a family of related specifications, some of which are still in draft stages (e.g., IEEE P1003.1e Security). FIPS 151-2 is complete in itself. The other pieces mentioned here will augment FIPS 151-2 usability as additional FIPSes.

Conformance testing: NIST has developed a conformance test suite and offers testing services via Accredited POSIX Testing Laboratories (APTL). Certificates of validation are issued by NIST. Validated products are listed in CSL's quarterly "Validated Products List" (VPL), on a NIST/CSL-supported e-mail server, and the NIST Gopher system.

Bindings: The IEEE POSIX specification is the C language binding to the operating system application program interface (API). An additional binding is defined in IEEE 1003.5 Ada language binding.

Future plans: Existing kernel operations will not change, although additional operations are on the horizon (1003.1a). Related standards for other service area components, such as realtime extensions, system security, system administration, etc., will be developed over the next 1 to 2 years.

Alternative specifications: None (All other known specifications that provide these services are compatible with POSIX.)

4.8.2 Operating System Commands and Utilities

Specification title: FIPS 189 Portable Operating System Interface (POSIX); Part 2: Shell and Utilities

Specification available from: NTIS

Publication date: October 11, 1994 (effective date: April 3, 1995)

Sponsoring organization: IEEE

Applicability: 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, scheduling signal execution processes, and accessing environment information. The shell programming language allows the creation of portable, easily created scripts to perform actions that combine or tailor the functions performed by the individual utilities. Programming tools, such as AWK and GREP, and system/file management tools, such as TAR, are part of the specification.

Level of consensus: The IEEE standard, IEEE 1003.2-1992 (POSIX.2), was approved in October 1992. The FIPS adopts the international standard, ISO/IEC 9945-2:1993.

Product availability: Implementations of commands and utilities capabilities are available in proprietary operating systems that implement, or are very similar to requirements in the specification.

Completeness: The POSIX.2 Standard is currently complete.

Maturity: Antecedents and similarly specified implementations have existed for 10 to 20 years.

Stability: No new additions to the POSIX.2 base specification are planned. As implementations are processed through validation, however, changes may result through interpretation of the specification or through the standards correction process. New capabilities will be added as additional specifications (see future plans).

Known problems/limitations: None

Conformance testing: NIST plans to provide certification procedures and tests for demonstrating product conformance. No time schedule has been developed for these actions, although the test assertions for the POSIX.2 standard (IEEE POSIX 1003.2) are currently in ballot. Test technology is being reviewed for possible use in a future validation testing program.

Bindings: Language bindings for POSIX.2 are appropriate only indirectly. POSIX.2 defines a command language interface for users, shell scripts, and several systems level scripting and programming languages.

Future plans: Additional functionality is being developed in subgroups as follows: Shell and Utilities Extensions (P1003.2b), Security Extensions (P1003.2c), and Batch Extensions (P1003.2d). Each of these has its own schedule, but the expected completion dates are within the next 6 to 18 months.

Alternative specifications: None (All other known specifications that provide these services are compatible with POSIX.)

4.8.3 Operating System Realtime Services

Specification title: IEEE 1003.1b-1993 Portable Operating System Interface (POSIX) Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension [C Language]

Specification available from: IEEE

Publication date: April 1994

Sponsoring organization: IEEE

Applicability: Provides the POSIX operating system extensions needed to allow incorporation of realtime application domains into the OSE. The extensions define the applications interface to basic system services for input/output, file system access, and process management.

Level of consensus: IEEE 1003.1b-1993 was adopted as a national standard and is undergoing the process to make it an international standard.

Product availability: Implementations of some of these realtime extension capabilities are available in proprietary operating systems that are very similar to the specification.

Completeness: The specification is complete. Additional capabilities for realtime threads and additional extensions are included in other IEEE Working Group specifications.

Maturity: Commercially available operating systems contain much of the 1003.1b functionality.

Stability: Since becoming an IEEE standard, work has intensified on the extensions. Realtime operating system capabilities have been involved in the evolution of POSIX from the beginning. Specification of these capabilities has evolved over the last 7 years.

Known problems/limitations: The specification as it stands includes a C language binding (1003.1b) and realtime threads (P1003.1c).

Conformance testing: When a FIPS is adopted, NIST plans to provide certification procedures and tests for demonstrating product conformance. No time schedule has been developed for these actions.

Bindings: IEEE 1003.1b-1993 is defined as a C language binding.

Future plans: Still to come are Additional Extensions (1003.1d), Security Extensions (1003.1e), realtime profile (1003.13), and testing specifications. Other related subparts in addition to those mentioned previously include 1003.1f POSIX - Transparent File Access (TFA), 1003.12 POSIX--Protocol Independent Interface (PII), and 1003.13 POSIX Application Environment Profile--Realtime.

Alternative specifications: None.

4.8.4 Operating System Security API

Specification title: POSIX - Security Extensions IEEE 1003.1e

Specification available from: IEEE Working Group P1003.6

Publication date: Draft available

Sponsoring organization: IEEE

Applicability: Security considerations are specified in terms of data encryption mechanisms, access control, reliability control, system logging, fault tolerance, and audit facilities. (The security interface does not specify a secure operating system; only its interface.)

Level of consensus: This specification is still in a draft stage but is in ballot resolution.

Product availability: Implementations exist with the majority of defined features.

Completeness: This specification defines those security capabilities necessary to secure kernel operations. Another specification, 1003.2c, defines security capabilities at the user level.

Maturity: The basic technology is well understood and the specification is based on several underlying standards/criteria.

Stability: With the expected balloting process to complete in late 1994, consensus has evolved around the core document with minor exceptions. These exceptions may become options in the current document, or modifications in later versions. Resolution of ballots will determine the outcome.

Known problems/limitations: While not a problem, users should not mistake the capabilities provided through this interface specification as the implementation of secure operations. Users must define security policies separate from the implementation. The interface specification provides only the means for communicating these policies to the system.

Conformance testing: A method of measuring conformance has not been defined. Until this has occurred, no determination of where or when testing might take place will be made. A set of draft test assertions has been developed for use in test suite development.

Bindings: The 1003.1e specification is defined as the C language binding.

Future plans: Security specifications will expand to integrate interfaces for other service area components.

Alternative specifications: National Computer Security Center "Orange Book" security standards for access control (NCSC-STD-020-A) and password management (NCSC-STD-002-85); Defense Intelligence Agency (DIA) DRS-2600-5502-87: "Security Requirements for System High and Compartmented Mode Workstations (CMW)"; DIA DDS-2600-6216-91: "Compartmented Mode

Workstation Labeling: Encoding Format"; DIA DDS-2600-6215-91: "Compartmented Mode Workstation Labeling: Source Code and User Interface Guidelines".

4.8.5 Operating System Security Commands

Specification title: POSIX - Security Extensions IEEE 1003.2c

Specification available from: IEEE Working Group P1003.6

Publication date: Draft available

Sponsoring organization: IEEE

Applicability: This specification is the complement of 1003.1e. It defines the security interface for use by users and batch processing scripts that seek access to secure systems.

Level of consensus: This specification is still in a draft stage but is in ballot resolution.

Product availability: Implementations exist with the majority of defined features.

Completeness: This specification defines those security capabilities necessary to secure user and batch operations. Another specification, 1003.1e, defines security capabilities at the kernel level.

Maturity: The basic technology is well understood and the specification is based on several underlying standards/criteria.

Stability: With the expected balloting process to complete in 1995, consensus has evolved around the core document with minor exceptions. These exceptions may become options in the current document, or modifications in later versions. Resolution of ballots will determine the outcome.

Known problems/limitations: While not a problem, users should not mistake the capabilities provided through this interface specification as the implementation of secure operations. Users must define security policies separate from the implementation. The interface specification provides only the means for communicating these policies to the system.

Conformance testing: A method of measuring conformance has not been defined. Until this has occurred, no determination of where or when testing might take place will be made. A set of draft test assertions has been developed for use in test suite development.

Bindings: The 1003.2c specification does not require a language binding.

Future plans: Security specifications will expand to integrate interfaces for other service area components.

Alternative specifications: National Computer Security Center "Orange Book" security standards for access control (NCSC-STD-020-A) and password management (NCSC-STD-002-85); Defense Intelligence Agency (DIA) DRS-2600-5502-87: "Security Requirements for System High and

Compartmented Mode Workstations (CMW)"; DIA DDS-2600-6216-91: "Compartmented Mode Workstation Labeling: Encoding Format"; DIA DDS-2600-6215-91: "Compartmented Mode Workstation Labeling: Source Code and User Interface Guidelines."

4.8.6 System Management

Specification title: Standard for Information Technology - Portable Operating System Interface (POSIX) System Administration - Part 2: Software Administration IEEE P1387.2; Part 3: User and Group Account Management IEEE P1387.3; and Part 4: Printing Interfaces IEEE P1387.4

Specification available from: IEEE

Publication date: Second half of 1995.

Applicability: This specification applies to several aspects of system management: software administration, user and group account management, and printing interfaces. Part 2 defines a software packaging layout, and utilities that operate on that packaging layout, as well as software installed from that packaging layout. The scope of this standard is administration of software across distributed systems. This administration includes packaging of software for distribution, distribution of software to systems, installation and configuration of software on systems, and removal of software from systems, as a minimum.

User and Group Account administration, Part 3, includes tasks such as the creation and maintenance of user and group accounts on both single systems and within heterogeneous, distributed environments. P1387.3 provides the distributed management of a POSIX conformant system. POSIX.1 describes a user and a group database, but POSIX.2 does not describe utilities to manage these entities. P1387.3 provides a means of managing these entities. It also provides interfaces which may be used to manage extensions such as passwords for which there is widespread existing practice.

Part 4 of the specification defines interfaces for a printing system that can be used in both local and distributed environments. This includes a command line interface, an application programming interface, and a set of managed objects. The command line interface section of this standard provides common utility programs for use by application programs and humans. The application programming interface is meant to support printing application portability at the source code level. The managed objects provide a foundation for the definition and implementation of printing system functionality and interoperability, especially in a heterogeneous, distributed environment. The commands, operations, and managed objects in this standard specify interfaces for both the use and management of the printing system.

Level of consensus: This IEEE standard has developed a high level of consensus within the POSIX community. It is given an average evaluation only since it has not yet been published. Upon publication it will be given a high evaluation.

Product Availability: Almost all vendors supplying POSIX platform will implement this standard.

Completeness: This set of specifications provides a complete detailed approach to packaging, distribution, installation, configuration, and removal of software in distributed systems; a complete detailed approach to adding, modifying, and deleting user and group accounts, as well as an interface to manage passwords associated with accounts; and a complete detailed printer interface specification.

Maturity: The principal elements have been agreed for the last two years. In time, as the API is fully implemented, the standard will reach a high level of maturity.

Stability: This specification is stable. Fine tuning modifications can be expected until the final draft is accepted as an IEEE standard.

Known problems/limitations: None.

Conformance testing: Conformance requirements are defined. Test methods are being defined for measuring the conformance of implementations to this specifications.

Bindings: IEEE 1387 defines a C language binding.

Future plans: The committee will likely pursue standardization in other aspects of system administration.

Alternative specification: None.

4.9 Human/Computer Interface Services

The components of this service include the Graphical User Interface Service component, Planned FIPS 158-1, which refers to the X Window System, version 11, release 5, and the Graphical User Interface Toolkit component.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	PRL
FIPS 158-1 X Window System	●	○	○	●	●	
Draft Standard for Information Technology—X Window System Graphical User Interface—Part 1: Modular Toolkit Environment (IEEE 1295)	●	●	○	○	○	○

Legend: ●-high evaluation ○-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
PRL -- Problems/limitations

4.9.1 Graphical User Interface

Specification title: FIPS 158-1 User Interface Component of Applications Portability Profile (MIT X Window System)

Specification available from: NTIS

Publication date: October 20, 1992

Sponsoring organization: Massachusetts Institute of Technology X Consortium

Applicability: The MIT X Window System is the Federal standard for graphical user interfaces in the OSE. Its software, written in C, has proven to be highly portable between various hardware platforms and operating systems. Because of its client-server architecture, the X client application can run on one system while the X server can be running on another system on a network. As a result, networked PC's which run X server software can act as X terminals for X client applications running on OSE platforms.

Level of consensus: This specification forms the base standard for further work being done in various standards making organizations. Toolkits, libraries of standard controls, utilities, protocols, and dialogue management are some of the specific areas planned for future standards based on the X Window System specification.

Product availability: Virtually all major hardware vendors have produced implementations of the X Window System for their product lines. A copy of the software is available through World Wide Web (WWW), Gopher, or through the "ftp" command on Internet.

Completeness: The specification defines the primitives, intrinsic functions based on these primitives, and some of the lower level library specifications for human/computer interface services. It does not specify any of the "look and feel" or style services that will be accessible at higher levels of abstraction. It does not contain a full complement of utilities and services required to allow application programmers to easily program user interfaces.

The X Window System defines a C language source code level interface to a network-based bit-mapped graphic display system. The computer program source code contained in Version 11, Release 5, is not part of the specification for the FIPS. The specification for this FIPS includes the following documents from the X Consortium, X Window System, Version 11, Release 5:

1) X Window System Protocol, X Version 11
2) Xlib—C language X Interface
3) X Toolkit Intrinsics—C Language Interface
4) Bitmap Distribution Format 2.1.

Maturity: The X Window System has been in existence since 1983. It was one of the products to come out of Project Athena at MIT.

Stability: The Xlib, X Window System Protocol, and the Xt Intrinsics documents are stable. Further changes in these specifications are expected to include tuning modifications rather than major deletions or additions.

Known problems/limitations: Most of the functionality is available at a low level (i.e., too low for most application programming).

Conformance testing: The U.S. Government will accredit conformance testing services through the National Voluntary Laboratory Accreditation Program (NVLAP) when test suites and testing policy for FIPS 158-1 become available. Some testing technology is available through proprietary sources.

Bindings: The X Window System specification is defined as the C language binding.

Future plans: Revision of the FIPS will be considered and made where appropriate as national and international standards are approved.

Alternative specifications: None

4.9.2 Graphical User Interface Toolkit

Specification title: Draft Standard for Information Technology—X Window System Graphical User Interface—Part 1: Modular Toolkit Environment (1295)

Specification available from: IEEE Working Group P1295

Publication date: N/A

Sponsoring organization: IEEE

Applicability: This specification supports writing portable applications with graphical user interfaces based on the X Window System. It defines a source code level interface to an X Window System toolkit graphical user interface environment. It includes a C language application program interface that is consistent with the Graphical User Interface Drivability Recommended Practice developed by IEEE P1201.2.

Level of consensus: The IEEE P1295 Working Group has advanced the toolkit API originally based on the OSF MOTIF Application Environment Specification User Environment Volume. The technical credibility and maturity of the specification is reflected by the successful, large installed base of technology which complies with the specification. Due to the substantial consensus already achieved in the industry, NIST expects this specification to move from a de facto to a de jure status in a relatively short time.

Product availability: Virtually all POSIX platform vendors and users are already using variant implementations of MOTIF from which the 1295 specification was derived.

Completeness: The 1295 specification provides a toolkit of functions and objects for developing application interfaces for GUI. Use of the 1295 specification in conjunction with FIPS 158-1

implementations of the X Window System will provide a complete GUI, but without management capabilities that can be provided in dialogue and presentation tools such as user interface management systems (UIMS).

Maturity: Existing applications that are written to comply with the OSF MOTIF API specification should port with reasonable ease to the 1295 specification.

Stability: Due to industry commitment to a substantial installed base, the specification should remain stable. Extensions to the Graphical User Interface Toolkit specification may be proposed within 1 to 2 years. Consensus is converging rapidly on the 1295 specification.

Known problems/limitations: The 1295 specification provides only the toolkit level interface. An underlying GUI system, such as the X Window System, must also be provided to complete the GUI.

Conformance testing: Proprietary validation tests exist. These are being considered in plans for a NIST testing service when the specification becomes a FIPS.

Bindings: The 1295 specification is defined as a C language binding.

Future plans: Presentation and dialogue management services will be defined after the toolkit specification is adopted.

Alternative specifications: None.

4.10 Software Engineering Services

Programming languages, Integrated Software Engineering Environments (ISEE), and software engineering tools are included as components of software engineering services. The programming languages included herein are broad-based FIPS programming languages. While other programming languages are developing or may be specified as FIPS, no attempt to include every programming language was made. As consensus develops and needs warrant, each language will be considered for inclusion as a recommended specification within the APP. (Alternative specifications are not included for programming languages.)

SPECIFICATION	LOC	PAV	CMP	MAT	STB	PRL
FIPS 119-1 Ada	●	●	●	●	●	●
FIPS 160 C	●	●	●	●	●	●
FIPS 21-4 COBOL	●	●	●	●	●	●
FIPS 69-1 FORTRAN	●	●	●	●	●	●
ISEE Repository ISO/IEC 13719-1	●	O	O	O	O	O

Legend: ●-high evaluation O-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
PRL -- Problems/limitations

4.10.1 Programming Language Ada

Specification title: FIPS 119-1 Ada

Specification available from: NTIS

Publication date: March 13, 1995

Sponsoring organization: Ada Joint Program Office

Applicability: Ada is a general-purpose, high-level programming language. In addition, it provides strong data-typing, concurrence, and significant code-structuring capabilities. Although it can be used for any type of system, it is particularly suited to embedded realtime systems, distributed systems, highly reliable software development, and reuse of proven code.

Level of consensus: Ada is an international standard (ISO 8652:1995) and a FIPS. The Department of Defense has directed that Ada be used in all DoD systems development.

Product availability: Numerous DoD-validated compilers and Ada environments are available commercially.

Completeness: Ada is complete for use as a general-purpose programming language.

Maturity: Ada was developed as a DoD-sponsored language and is based on well-defined predecessor languages such as Pascal.

Stability: Ada has the backing of the Department of Defense, the U.S. Government, the American National Standards Institute (ANSI), and the International Organization for Standardization (ISO).

Known problems/limitations: Insofar as the majority of POSIX bindings are written in C, specialized standards groups are working on Ada bindings. Generally, there are fewer standardized bindings for Ada.

Conformance testing: Ada conformance and validation testing are carried out under the auspices of DoD's Ada Joint Program Office (AJPO). A monthly list of validated compilers is published by AJPO. NIST publishes a quarterly Validated Products List (VPL) of FIPS-validated implementations. An additional compiler performance measurement testing service is available through AJPO.

Bindings: Ada bindings have been defined for various OSE services. Most prominent are those for POSIX (IEEE 1003.5) and SQL (FIPS 127-2). Additional specifications are in process for other OSE services, such as realtime (IEEE 1003.5a and 1003.5b).

Future plans: A test suite for the revised Ada should be available within a year.

4.10.2 Programming Language C

Specification title: FIPS 160 C

Specification available from: NTIS

Publication date: March 13, 1991

Sponsoring organization: Standards Committee X3J11

Applicability: C is a general purpose high-level programming language designed for use in various levels of software including operating systems, system level software (e.g., special purpose processors), and business and scientific application software.

Level of consensus: FIPS 160 and the ANSI standard are based on the International Standard, ANSI/ISO 9899:1992. FIPS 160 specifies certain options and minimum capabilities that are left as options or variables within the ANSI standard.

Product availability: Numerous ANSI C compilers, interpreters, and associated products are commercially available and supported. Many of the compilers are also FIPS-validated and are commercially available.

Completeness: C includes facilities for every level of programming, from low-level (hardware control) operations to high-level abstract functions and procedures. Data structuring, reusable library support, and memory management are included.

Maturity: Development of C has progressed from a family tree of similar languages developed in academia, to a well-defined, widely supported language over a period of 15 years.

Stability: Standards Committee X3J11 is considering changes to fine-tune the standard based on usage experience.

Known problems/limitations: C does not provide direct support for data abstraction, information hiding, inheritance, or operator overloading. A new standard is developing to incorporate these capabilities within the C programming environment (see Future Plans below.) There are also some idiosyncracies within implementations due to environmentally defined or implementor-defined components allowed by the standard.

Conformance testing: The U.S. Government established testing procedures and a testing service in August 1992 for formal validation using the FIPS. NIST publishes a quarterly Validated Products List (VPL) of FIPS-validated implementations. The POSIX operating system interface standard, FIPS 151-2, requires a C compiler for validation of POSIX implementations. Validation of the POSIX interface does not qualify as validation of the C compiler. A separate validation for the compiler is required.

Bindings: Most of the POSIX application program interfaces are defined in terms of C language bindings.

Future plans: Standards Committee X3J16 is developing the C++ language standard, which will provide the tools for object-oriented software development. The current schedule includes proposing a draft standard in 1995.

4.10.3 Programming Language COBOL

Specification title: FIPS 21-4 COBOL

Specification available from: NTIS

Publication date: July 17, 1995

Sponsoring organization: Standards Committee X3J4

Applicability: COBOL is designed for use in programming self-documenting business oriented applications.

Level of consensus: The FIPS and international standards (ISO 1989:1985) are based on ANSI Standard X3.23-1985 and Addendum X3.23A-1989. The latest revision (21-4) provides corrections to various parts of the standard.

Product availability: COBOL is the most widespread programming language. An overwhelming percentage of all existing Federal applications are written and maintained in COBOL. All major vendors offer FIPS COBOL.

Completeness: The current standard does not include realtime, operating system, and communications components. It is most complete in the areas of data manipulation, and business/financial applications, which is its intended domain.

Maturity: COBOL is one of the oldest standard general-purpose programming languages, having been established in the early 1960s by DoD initiative.

Stability: The X3J4 Standards Committee is in the process of adding new functionality for communications interfaces and screen management. Compatibility with previous versions of the standard will be maintained. This has historically been one of COBOL's stronger points.

Known problems/limitations: COBOL has always been specialized toward the development of general-purpose business and financial applications. It is limited in other types of application domains, such as in realtime and communications, although this may change with functionality introduced by proposed revisions.

Conformance testing: FIPS conformance test suites are available from Federal sources. Testing services are also available from NIST. NIST publishes a quarterly Validated Products List (VPL) of FIPS-validated implementations.

Bindings:

Future plans: The addition of new functionality over the next 3 to 5 years will greatly expand the capabilities of COBOL to other application areas. An example of expansion includes object-oriented capabilities which are under development.

4.10.4 Programming Language Fortran

Specification title: FIPS 69-1 Fortran

Specification available from: NTIS

Publication date: December 24, 1985

Sponsoring organization: Standards Committee X3J3

Applicability: Fortran is a high-level programming language used largely in scientific and engineering applications where large amounts of data are analyzed and processed in computationally intensive environments.

Level of consensus: The FIPS and the international standard (ISO 1539:1980) are based on the national standard (ANSI Standard X3.9-1978).

Product availability: Every major hardware vendor markets a Fortran compiler based on the standard. Additional compilers are available from a multitude of software vendors.

Completeness: It is a general-purpose programming language with capabilities for performing virtually any type of application function. It was originally developed to assist in the development of scientific calculation applications, but it has since been extended to cover other types of applications.

Maturity: Fortran is one of the oldest programming languages and was also the first one to be standardized.

Stability: Although it has undergone several major revisions over its lifespan, Fortran contains virtually all of the same capabilities that were available when it was new. In addition, it contains elements for assisting in the development of information systems, realtime and process control systems, structured programming constructs, etc.

Known problems/limitations: Due to loose data-typing and some idiosyncracies of various compilers, some debugging problems are very difficult to locate and fix.

Conformance testing: Conformance test suites are available from Federal sources. Testing services are also available from NIST. NIST publishes a quarterly Validated Products List (VPL) of FIPS-validated implementations.

Bindings:

Future plans: An IEEE Working Group is defining a POSIX/Fortran 77 binding (IEEE 1003.9).

4.10.5 Integrated Software Engineering Environment Repository

Specification title: Portable Common Tool Environment (PCTE) Application Programmer's Interface ISO/IEC 13719-1

Specification available from: ECMA, ISO

Publication date:

Sponsoring organization: ISO/IEC JTC1/SC22 Working Group 22 and ECMA Technical Committee 33

Rationale: NIST is working to develop a suite of ISEE standards. A cornerstone for the interoperability of software engineering tools within ISEE environments is the existence of a framework which provides a consistent set of services to allow for the integration of data, control, and presentation attributes among the various tools in the environment. PCTE is one such open standard that provides for some of these framework services, principally object management services.

Applicability: Integrated software engineering environments (ISEE) and tools include systems and programs that assist in the automated development and maintenance of software. These include, but are not limited to, tools for requirements specification and analysis, for design work and analysis, for creating and testing program code, for documenting, for prototyping, and for group communication. The interfaces among these tools include services for storing and retrieving information about systems and exchanging this information among the various programs in the development environment.

PCTE provides a set of well-integrated services as the foundation for Integrated Software Engineering Environment (ISEE) frameworks. It provides portability of applications with object management services (OMS) for distributing the PCTE repository, and other operating system-like services for messages, processes, etc. The OMS provides schema definition sets (SDS) using the Entity-Relationship-Attribute (ERA) data model, dynamic access to schemas, multiple inheritance, support for version control and configuration management, all within a heterogeneous environment.

Level of consensus: Major European manufacturers, and U.S. software developers and integrators have announced products that implement the ISO standard. The base standard stems from the ECMA standard ECMA-149. Additional standards provide the bindings for several programming languages.

Product availability: There are two implementations of PCTE available with several products built using these frameworks.

Completeness: The current specification includes the capability of documenting large-grained system components, such as modules, programs, and subsystems. Full object-oriented capabilities are now being considered in proposals for extending PCTE into fine-grained development areas.

Maturity: PCTE has been under development since 1982, and under ECMA sponsorship since 1988. The basis entity-relationship (ER) data repository model used by PCTE is fairly stable and unlikely to undergo major changes in the future. Enhancements to address object-oriented design and further developments to aid data, control, and presentation integration have been incorporated in the base repository and framework.

Stability: Additions or modifications are planned in the evolution of PCTE to enhance its object-oriented capabilities, client-server support, and management functions.

Known problems/limitations: The current PCTE specification can accommodate the representation of large data objects, such as documents, modules, programs, etc. but does not provide an efficient mechanism for representing small objects, such as data elements and the associated actions.

Conformance testing: No organizations are currently planning to develop a test suite for PCTE.

Bindings: ISO/IEC 13719-2 C language binding, ISO/IEC 13719-3 Ada language binding, draft specification for C++ language binding.

Future plans: CSL is one of the participants in the Object Management Group's PCTE Special Interest Group (SIG). This group intends to promote Common Object Request Broker Architecture

(CORBA) PCTE compatibility through the development of a PCTE Interface Definition Language (IDL) binding and definition of a PCTE subset.

Standards Committee X3H4 for Open Repository (see IRDS) is now also responsible for U.S. participation in the new ISO Working Group for PCTE (SC22 WG22). This will hopefully lead to a tying together of standards for data related aspects of software engineering with standards for data management services.

Internet information: FTP specifications, documents, and general information from omg.org

4.11 Data Management Services

Data management services include the data dictionary/directory component for accessing and modifying data about data (i.e., metadata), the database management system component for accessing and modifying structured data, and the distributed data component for accessing and modifying data from a remote database.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	PRL
FIPS 127-2 SQL	●	●	●	●	●	●
FIPS 156 IRDS	O		●	●	O	
RDA	O		O		O	O
FIPS 193 SQL Environments	O		O	O	O	O

Legend: ●-high evaluation O-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
PRL -- Problems/limitations

4.11.1 Relational Database Management System

Specification title: FIPS 127-2 Database Language SQL

Specification available from: NTIS

Publication date: June 1993

Sponsoring organization: Standards Committee X3H2

Applicability: FIPS SQL provides data management services for definition, query, update, administration, and security of structured data stored in a relational database. A relational database is appropriate for general purpose data management, especially applications requiring flexibility in data structures and access paths; it is particularly desirable where there is a substantial need for *ad*

hoc data manipulation or data restructuring. The seeurity interfaee for granting and revoking privileges does not specify a seeure DBMS; only its interface.

Level of consensus: FIPS 127-2 adopts ANSI Standard X3.135-1992 (SQL), which is identical to ISO/IEC Standard 9075:1992. SQL has been adopted as the database managemcnt component by X/Open, OSF, SQL Access Group, and other vendor consortia.

Product availability: Numerous implementations of the original ANSI SQL exist on all classes and brands of platforms. The NIST SQL Validated Products List maintains a long list of validatcd products and environments that conform to this and earlier FIPS. Vendors are vigorously implementing the additional optional, intermediate, and full features as speeified in FIPS 127-2. In addition, vendors provide proprietary extensions to the standard as a mechanism for adding value. These extensions may not be compatible with future directions that the standard may take.

Completeness: The 1992 SQL standard specifies data definition, view definition, access control, integrity constraints, schema manipulation, data manipulation (Select, Insert, Update, Delete), Dynamic SQL, transaction management, connection management, scssion management, diagnostics management, information schema tables, and two methods of programming language bindings (Module and Embedded) for seven different programming languages (Ada, C, COBOL, Fortran, MUMPS [now known as M], Pascal, and PL/I). FIPS SQL requires ANSI Standard X3.135-1992 Entry SQL conformance to one or more FIPS programming languages and requires a FIPS Flagger to flag extensions in an implementation. FIPS SQL provides options for three other levels of conformance (Transitional, Intermediate, and Full), specifies charaeter sets and a documentation schema required to be supported in FIPS Intermediate SQL and above, and specifies default SQL sizing requirements. The FIPS provides options for SQL interoperability using the Remote Database Aecess (RDA) SQL Specialization. The FIPS also contains specifications for some Diseretionary Access Control (DAC) meehanisms, but not Mandatory Aceess Control (MAC) nor the assoeiated seeurity labels. For a definition of DAC or MAC, refer to "Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria" (NCSC-TG-021 Version 1, "Lavender Book"), National Computer Security Center, April 1991.

Maturity: The SQL data model is based on the relational model first published in 1969. The first commercial systems were available in 1979, and the first SQL standard was published in 1986. All subsequent standards have been upward compatiblc enhancements to add new facilities and features.

Stability: The SQL language has firm mathematical foundations in the first-order predieate calculus. Standards groups and vendors are firmly eommitted to upward compatibility in revisions and future extensions to the standard. Existing features are expected to remain stable for the foreseeable future.

Known problems/limitations: The existing standard is a nonprocedural data definition and manipulation language. It applies to stand-alone, single-environment database arehiteetures. It also applies to client-server architectures with proprietary internal interfaees and protocols. When combined with the RDA standard in Section 4.11.3, SQL is suitable for heterogeneous distributed database processing. Enhancements are under development to provide a call-level interface (CLI),

user-defined data types, triggers, assertions, flow of control statements, and other capabilities associated with object data management.

Conformance testing: A formal SQL test service was instituted by NIST in April 1990. Version 4.0 of the SQL test suite, which tests FIPS entry SQL, has been available publicly since January 1994; version 5.0, to test FIPS transitional SQL, is expected in April 1995. The SQL test suite measures conformance to both required and optional features of FIPS 127-2. NIST publishes a quarterly list of FIPS-validated processors. Certificates of validation are issued for products tested that show fully conforming test results. Validation summary reports (VSR) are issued for each test conducted, regardless of whether products have nonconformities.

Bindings: Bindings of SQL are available for seven different programming languages (Ada, C, COBOL, Fortran, MUMPS [now known as M], Pascal, and PL/I).

Future plans: Specifications for SQL interoperability with remote heterogeneous sites are under development in an emerging ISO/IEC Remote Database Access (RDA) standard (see sec. 4.11.3). An SQL Call Level Interface (SQL/CLI), to provide a services interface for third-party software vendors, and a specification for Persistent SQL Modules, to allow interchange of complete SQL stored procedures, are both under development with completion expected in 1995 and 1996, respectively. An emerging SQL3 specification, with features for managing complex objects in heterogeneous environments, is under development in ANSI and ISO standardization committees, with completion expected in the 1997 time frame. The SQL3 specification will include triggers, assertions, user-defined data types, object hierarchies, inheritance, and other features for management of complex objects. A new project for development of SQL Multimedia and other Application Packages (SQL/MM) is under ballot with completion of initial parts for Full-Text, Images, and Spatial Data projected for completion in 1998. Revised FIPS SQL standards that adopt the new SQL enhancements are expected as appropriate.

Alternative specifications: None.

4.11.2 Data Dictionary/Directory System

Specification title: FIPS 156 Information Resource Dictionary System (IRDS)

Specification available from: NTIS

Publication date: April 5, 1989

Sponsoring organization: Standards Committee X3H4

Applicability: Data dictionary/directory services consist of utilities and systems necessary to catalog, document, manage, and use metadata (information about data).

Level of consensus: ANSI Standard X3.138-1988 and the FIPS are the same document.

Product availability: Commercial implementations have been developed, but their quality has not yet been determined. A prototype implementation is available from CSL which contains a large subset of IRDS functionality.

Completeness: The FIPS specification includes human/computer interfaces only. ANSI Standard X3.185-1992, IRDS Services Interface, provides an application program interface to the IRDS. It is appropriate for metadata interchange with a database management system, and between an IRDS and application programs. ANSI Standard X3.195-1991, IRDS Export-Import File Format, supports schema and metadata interchange among IRDS-compliant databases, among IRDS and CASE tools with repositories or dictionaries, between IRDSes and application programs, and between other systems that wish to employ the exchange mechanism that it specifies.

Maturity: Antecedents of the IRDS have been in existence for 15 years. The current specification has been in development during the major part of this time.

Stability: The next 2 to 3 years may see significant changes in the current standard. Related standards efforts are specifying additional and upwardly compatible functionality.

Known problems/limitations: Virtually all procurements that specify a data dictionary/repository require it to be active. In such cases, the FIPS 156 IRDS would need to be augmented by the ANSI standard, X3.185-1992, discussed above.

Conformance testing: NIST has developed an automated conformance test system for the FIPS 156 IRDS Command Language. Version 1 of the test system was released in November 1993 and has since been revised. The test system provides the basis for FIPS 156 validation testing performed by NIST. For each individual implementation tested, NIST issues a Validated Summary Report detailing the results of the testing. These reports are then listed in the Validated Products List which is published quarterly by NIST.

Bindings:

Future Plans: Related standards work will provide additional functionality and capability to manage object-oriented data structures and provide for enhanced communication of information between applications and other data management tools. A major revision to the standard is envisioned in about 3 years to include this new functionality.

Alternative specifications: None.

4.11.3 Distributed Data Access

Specification title: Remote Database Access (RDA) ISO/IEC 9579:1993

Specification available from: ANSI

Publication date: 1993

Sponsoring organization: ISO/IEC JTC1

Applicability: RDA is used to establish a remote connection between an RDA client, acting on behalf of an application program or a client data manager, and an RDA server, interfacing to a process that controls data transfers to and from a database. The goal is to promote the interconnection of applications and the interoperability of database management systems among heterogeneous environments.

Level of consensus: The ISO/IEC RDA specification became a standard in 1993. The specification is in two parts: Part 1 -- Generic Model, Service, and Protocol, and Part 2 -- SQL Specialization. RDA is a working task group of the NIST Open System Environment Implementor's Workshop (OIW) and RDA agreements for the Basic Application Context of the SQL Specialization are part of the Stable Agreements. Agreements for the Transaction Processing (TP) Application Context are under development in OIW.

Product availability: Vendor consortia such as the SQL Access Group have demonstrated interoperability with working prototypes among different SQL servers. Various SQL vendors are planning to have conforming client and server products available.

Completeness: RDA services consist of dialogue management, association control, resource handling, and data language services between a single client and a single server. Association control includes making a connection to a specific database at the server site. SQL statements are sent as character strings with a separate list of input parameters, and resulting data or exception conditions are returned. Transaction management services are also included for both one-phase and two-phase commit protocols. Different application contexts are negotiable to determine whether one-phase (Basic context) or two-phase commit (TP context) are available. The existing specification does not consider integrated concurrency control mechanisms, so distributed database management is the concern of the client process. Extensions for true distributed database management among different SQL implementations are under consideration.

Maturity: Methods for establishing communications links between client and server sites are well known, but agreements on nonproprietary communications protocols are very new.

Stability: The client-server architecture is just one of several architectures used for implementing distributed systems and there is no final conclusion as to which is best. The stability of RDA depends on the stability of the client-server architecture.

Known problems/limitations: The RDA SQL Specialization only supports Entry SQL from the SQL-1992 standard. Support for features in Intermediate SQL and Full SQL are under development with approval expected in 1996. Although distributed extensions are under consideration, RDA does not currently specify distributed database access, except what is achievable by the client using two-phase commit protocols among different servers.

Conformance testing: At the present time, RDA can be tested indirectly using the NIST SQL test suite, with application programs at the client site and data at the server site. NIST plans a complete RDA test service for Fall 1995.

Future plans: Enhancement projects for distributed database and stored database procedures have already been proposed to ISO. Extensions to support new features in the recently adopted SQL-

1992 standard are under development. Vendor agreements reached by various consortia are finding their way into the RDA standard.

Alternative specifications: None.

4.11.4 Database Environment

Specification title: FIPS 193 SQL Environments

Specification available from: NTIS

Publication date: February 1995

Sponsoring organization: NIST

Applicability: The FIPS for SQL Environments is applicable in any situation where it is desirable to integrate user productivity tools and heterogeneous data repositories into an SQL environment. It is particularly suitable for specifying limited SQL interfaces to legacy databases or to specialized data repositories such as geographic information systems, full-text document management systems, or object database management systems.

Level of consensus: This standard leverages the consensus already achieved by FIPS SQL.

Product availability: Numerous user productivity tools claim to be able to access data stored in SQL databases, and numerous data repositories claim to support limited SQL interfaces. The profiles defined in FIPS 193 make it possible for the customer to specify exactly the style of interface and the level of SQL support required for each of these types of products.

Completeness: The emphasis in this first FIPS for SQL Environments is on profiles for limited SQL interfaces to non-SQL data repositories. Subsequent versions of this FIPS may specify more complete profiles for other products in an SQL environment.

Maturity: This standard leverages the maturity already achieved by FIPS SQL.

Stability: This standard leverages the stability already achieved by FIPS SQL.

Known problems/limitations: The profiles defined by this standard are not complete in and of themselves. The user is required to add information before this standard can be successfully used in a procurement.

Conformance testing: Conformance testing for products claiming conformance to one of the profiles specified by FIPS 193 will be achieved by a suitable modification of the existing NIST SQL test suite.

Bindings: This standard requires the customer to choose from among the different binding styles already defined by the SQL standards. Two of these styles (CLI and RDA) are expected to be more

popular than the others. If a programming language binding style is chosen, then FIPS SQL specifies the parameter passing requirements for each of seven different programming languages.

Future plans: The FIPS for SQL Environments will continue to evolve to capture any SQL extensions or alternatives specified by FIPS SQL.

Alternative specifications: None.

4.12 Data Interchange Services

Data interchange services provide support for the exchange of information, including format and semantics of data between applications on homogeneous platforms.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	PRL
FIPS 152 SGML	●	●	●	●	●	○
PDDF						
EMPM ANSI/NISO Z39.59	●	○	●	●	●	○
Std. Data Elements ISO 11179, Parts 3, 4, and 5	●	○	○	●	●	●
FIPS 161-1 EDI	●	●	●	●	○	○
FIPS 128-1 CGM	●	●	●	●	●	●
FIPS 194 Raster	●		●	○	●	●
FIPS 177 IGES	●	●	●	●	●	●
JPEG	●	●	●	●	●	●
MPEG	●	●	●	○	○	○
Compact Disk Read-only Memory (CD-ROM) ISO 9660	●	●	●	●	○	○
Planned FIPS on STEP (ISO 10303)	●		○	○		
FIPS 173-1 SDTS	○	○	●	●	●	●

Legend: ●-high evaluation ○-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
PRL -- Problems/limitations

4.12.1 Document Markup Language

Specification title: FIPS 152 Standard Generalized Markup Language (SGML)

Specification available from: NTIS, ANSI, GCA

Publication date: September 26, 1988

Sponsoring organization: ISO/IEC JTC1

Applicability: Interchange of documents — SGML is intended to formally define the grammar of languages for document markup. It provides a means to specify what markup is allowed, what markup is required, and how markup is distinguished from text. Tag sets, such as Electronic Manuscript Preparation and Markup (EMPM) are defined in terms of SGML grammar. The tag set is then used to markup documents (i.e., to define paragraphs, section headings, etc.). A CALS (Continuous Acquisition and Life-Cycle Support) SGML library (CSL) containing an SGML Tagset Registry (STR) and an SGML Reuse Library is being developed to standardize on common tagsets and data type definitions (DTD).

Level of consensus: SGML is defined by international standard ANSI/ISO 8879:1986. The FIPS specifies a profile of capabilities that are defined in the ANSI/ISO standard and sets minimum options for use in Federal systems.

Product availability: SGML is in widespread use within government and industry. Currently, it is gaining particular momentum within the Internet community via Hypertext Markup Language (HTML), an SGML application. Major word processing software implementors have produced SGML add-on tools to assist users in the development of SGML-based documents.

Completeness: A high percentage of SGML features are available in current implementations. SGML does not deal with the meaning of the markup. (Markup consists of the common sets of document formatting codes used in classes of document types. For example, technical manuals may use a different markup from management guideline documents due to the audience and content of the respective document types, and the types of publishing layouts that are commonly used for each.) Through the use of tags, SGML enables retrieval and intelligent markup of the information so that other processes can exploit the information.

Maturity: Precursors of SGML include Backus Naur Form, Regular, Context Free, Left-to-Right scanning with k-token lookahead (LR[k]), and Context Sensitive grammars. These are well understood and have a rich mathematical basis. SGML recently passed its ISO 5-year review.

Stability: The position as a grammar representation standard makes SGML a very stable specification. It is generalized to the extent that various other representations and models can be included and represented within the SGML framework. The market is having difficulty, however, adopting any of the many possible SGML-encoded markup architectures as a basis for interchange. See Known problems/limitations.

Known problems/limitations: The CALS program has defined a specification and guidance for using SGML in an interchangeable and uniform way (i.e., MIL-HDBK-28001 "CALS SGML Handbook"). The adoption of a common CALS tagset and DTD repository will also standardize common SGML practice.

Conformance testing: NIST is in the process of developing formal testing procedures and policy to implement an SGML validation service. The service should be available in 1995.

Future plans: SGML is currently being reviewed by ISO and proposals for enhancements may be put forward over the next 1 to 3 years. The standards developers have agreed that any future changes will not affect existing conforming SGML documents. A recommendation to add all of ISO 8879 to the FIPS is under review.

Alternative specifications: None.

4.12.2 Document Distribution Format

Specification Title: Portable Document Delivery Format (PDDF)

Specification Available From: National Institute of Standards and Technology (NIST)

Publication Date: Draft available (planned publication in 1996)

Sponsoring Organization: NIST

Applicability: PDDF provides for the final form delivery of information in a standardized platform-independent electronic format. A proposed specification is currently being developed for a final form standard Portable Document Delivery Format (PDDF) which retains the page layout and pictorial information needed for the delivery of complex documents. The portable final form document is created from the revisable form document using conversion applications.

Level of Consensus: A group of Federal Government users from a large constituency of Federal agencies provided requirements to CSL for improving the interchange of final form electronic documents. The panel recommended that CSL consider existing specifications as the basis for a FIPS that will benefit the government user community in improving the interchangeability of final form electronic documents.

Product Availability: Products exist on the marketplace that use the proposed PDDF.

Completeness: The specification is both extensive and complete. The specification is open, published, and available for public use.

Maturity: Since the PDDF is to be based on existing public specifications, a significant level of maturity is built into the standard. Implementations have been available for several years. A de jure standard does not exist at this time.

Stability: A public specification is planned by 1997. Its current state is that of a draft in evolution.

Known Problems/Limitations: PDDF is a final form format specification. Documents specified in PDDF cannot be edited directly such as is the case with revisable form documents (i.e., non-PDDF documents), such as those found in word processor applications.

Conformance Testing: Plans will not be in place until a standard or stable public specification can be referenced.

Future Plans: A PDDF Users Forum may organize and meet on a regular basis to discuss directions for the PDDF specification and how to handle problem areas within the specification.

Alternative Specifications: There are several alternative format specifications, most of which are proprietary and not openly published. Some of these format specifications can be interchanged within proprietary environments only. The exception is SGML coupled with a set of standardized style semantics. Such a set of specifications based on SGML could form the basis for a PDDF specification, but the problem has been the lack of consensus on what constitutes a standardized set of style semantics.

4.12.3 Manuscript Markup Tag Set

Specification title: Electronic Manuscript Preparation and Markup (EMPM) ANSI/NISO Z39.59-1988

Specification available from: ANSI, AAP

Publication date: 1988

Sponsoring organization: ISO/IEC JTC1

Applicability: Electronic Manuscript Preparation and Markup is a specialized Document Type Definition (DTD) that includes an architecture encoded in SGML (see sec. 4.12.1) suitable for the interchange of the logical structure of books, articles, and serials. It provides a high-level language for describing these logical structures.

Level of consensus: EMPM is a national standard initially developed by the Association of American Publishers (AAP) and available as ANSI/NISO Z39.59-1988.

Product availability: Implementations are available generally within products that also implement SGML document interchange, such as SGML editors and conversion utilities.

Completeness: The standard offers a complete set of markup for logical structure of specific document types. The standard offers little assistance with layout and presentation style issues.

Maturity: The logical structure of documents is well known and captured in such documents as the Chicago Manual of Style.

Stability: The position as standard for the markup of logical structure makes this a very stable standard. No changes are expected within the next 2 years.

Known problems/limitations: The physical appearance of documents is not covered.

Conformance testing: None is specified directly for EMPM. The base standard for the formulation of EMPM, SGML, does, however, specify conformance testing.

Bindings: Bindings are not defined for data interchange formats.

Future plans: None.

Alternative specifications: None.

4.12.4 Data Element Specification

Specification title: Specification and Standardization of Data Elements, ISO 11179, Parts 3, 4, and 5.

Specification available from: ISO SC 14 Secretariat

Publication date: Part 3, July 1994; Part 4, January 1995; Part 5, May 1995

Sponsoring organization: ISO

Applicability: Standardization of data elements is essential to data sharing among organizations. This standard prescribes the methods of deriving and describing standard data elements which will insure ease of transfer by Electronic Data Interchange (EDI) and survivability of meaning over time. Each of the six parts of the standard may be used independently from the others, or in combination for best effect. The parts and expected publication dates for the full set of specifications are listed as follows:

11179-1 Framework for the Specification and Standardization of Data Elements, June 1996
11179-2 Classification of Concepts for the Identification of Domains, June 1996
11179-3 Basic Attributes of Data Elements, July 1994
11179-4 Rules and Guidelines for the Formulation of Data Definitions, January 1995
11179-5 Naming and Identification Principles for Data Elements, May 1995
11179-6 Registration of Data Elements, December 1995

Level of consensus: The United Nations EDIFACT developers and the Basic Semantic Repository (BSR) Project have expressed intent to apply the standards as they are developed. The majority of the development effort has been done in the United States by the X3L8 Committee, Data Representations. Five of the six editors are members of X3L8.

Product availability: Several commercial and noncommercial products implement parts of the standard; no product will conform to all parts as they are not all at a sufficient level of development.

Completeness: When used together, the six parts of the standard should result in a set of standardized data elements. Parts 3, 4, and 5 make up a significant part of the full capabilities of the specification.

Maturity: All parts of the standard are based on existing techniques and working systems.

Stability: All parts will remain stable from their publication dates for at least 2 years. X3L8 is developing follow-on projects assuming ISO 11179 as the base for further development.

Known problems/limitations: As of the publication date of this report, only parts 3 and 4 have been completed. Additional work is necessary on the other parts, each of which is in a different state of completeness. The standard does not address identification of data values or data concepts. These topics are under consideration as new work items.

Conformance testing: Data elements proposed for the register (Part 6) will be inspected for compliance by the Registrar. No product conformance tests are available at this time.

Future plans: In addition to the identification of data concepts and values, a metamodel for data representation is under development by X3L8.

4.12.5 Graphics Data Interchange

Specification title: FIPS 128-1 Computer Graphics Metafile (CGM)

Specification available from: NTIS, ANSI, ISO

Publication date: 1992 (Revised FIPS expected to be approved by end of 1995)

Sponsoring organization: Standards Committee X3H3, ISO/IEC JTC1

Applicability: Graphics data interchange is specified in terms of a file format that can be created independently of device requirements and translated into the formats needed by specific output devices, graphics systems, and computer systems. The standard specifies the content of graphic data interchange.

Level of consensus: The FIPS is based on national and international standard ANSI/ISO 8632:1992 for neutral (implementation and machine independent) graphics file formats. Vendors commonly use CGM as an exchange format for the storage, interchange, or output of a wide range of graphical pictures (from slides for presentation graphics or business charts to diagrams generated by scientific applications). Several application communities have defined CGM application profiles. These profiles specify the implementation requirements and subsets of CGM required for conforming implementations. The ANSI/ISO CGM standard requires the use of profiles for conformance. The revised FIPS will adopt revised industry specifications and will also require the use of profiles for conformance.

Product availability: Numerous CGM implementations exist for use in Federal procurements. Virtually all major microcomputer software products that utilize graphics can generate or interpret CGM files.

Completeness: CGM capabilities include the application of symbol libraries, application structuring within metafile pictures, advanced vector graphics, representation of tiled compressed raster data, engineering drawings, and cartography.

Maturity: CGM research and development has been performed since 1984.

Stability: The CGM standard defines metafiles of three upwardly compatible versions. Version 1 metafiles are defined by the original 1987 CGM standard; versions 2 and 3 define additional capabilities and provide increased graphical expressive power. There are two amendments to the 1992 version; Amendment 1 defines rules for profiles and Amendment 2 defines an application structuring capability.

Known problems/limitations: If an image is not completely specified in the CGM file (e.g., whether or not text fonts are solid or outline) an application may invoke default values for interpreting the image.

Conformance testing: NIST is currently operating a CGM test service to test for conformance of CGM metafiles, generators, and interpreters. The test service determines the degree to which the metafile, generator, or interpreter conforms to the FIPS 128-1 and the CALS CGM profile. Currently, the test service addresses only CGM version 1. The test service is being expanded to test for other profiles and CGM versions. A certificate of validation will be issued for metafiles passing the tests with no failures. Certificates of validation will be issued for generators (i.e., software that produces CGM metafiles) and interpreters (i.e., software that reads metafiles) that pass the tests with no failures. Generators and interpreters that undergo validation testing that results in test failures will be issued a registered report listing the failures. All certificates and registered reports are published in the NIST VPL.

Future plans: Work on two amendments to the CGM standard has been completed. Amendment 1, "Rules for Profiles" specifies a definition of conforming generators and interpreters, rules for writing profiles, and a complete and valid profile called the Model Profile. Amendment 2, "Application Structures," addresses the need for application-related structuring of metafiles. The FIPS currently includes the DoD CALS CGM profile and is being revised to include several other profiles.

Alternative specifications: None.

4.12.6 Raster Image Interchange

Specification title: FIPS 194 Open Document Architecture (ODA) Raster Document Application Profile (DAP)

Specification available from: NTIS

Publication date: March 13, 1995

Sponsoring organization: ISO/IEC JTC1

Applicability: The ODA Raster DAP is available for use by Federal Government agencies when acquiring and developing raster graphics applications. It applies to systems processing, generating, and receiving raster graphics images utilizing a structured document environment. It specifies the structure and parameters for describing and interchanging bi-level untiled compressed images as well as tiled raster images.

Level of consensus: The FIPS adopts the ISO/IEC 12064-1 International Standardized Profile (ISP). The ISP specifies a profile of capabilities that are defined in the ISO/IEC 8613 | ITU-T Rec. T.410 Series ODA standard. The FIPS defines three levels of conformance:

1. ANSI/AIIM MS-53 (Untiled) - This level supports the ANSI/AIIM MS-53 standard developed by the Association for Information and Image Management (AIIM).

2. Intermediate ODA Raster DAP - This level supports the tiled/untiled requirements that were jointly specified by the Department of Defense, Defense industry, and Open Systems Environment Implementors Workshop (OIW).

3. Full ODA Raster DAP - This level fully supports all aspects of the ODA Raster DAP.

Product availability: There is at least one current implementation that supports the ODA Raster DAP. Additional implementations are in development.

Completeness: A high percentage of the features necessary for implementing bi-level raster graphics applications are available in the ODA Raster DAP. Additional features to specify the grey scale/color formats and compression algorithms are being addressed.

Maturity: The basic technology upon which the ODA Raster DAP is based has existed for a few years. The process of scanning, storing, and displaying raster graphics images has been available for a similar period. The definition of a standard for structuring and interchanging raster graphics in a structured compound document has existed for 6 years. The definition of profiles to use the standard have only been published in the last year.

Stability: The basic standard to support raster graphics is very stable. There are, however, actions in process to add other compression algorithms, i.e., JPEG.

Known problems/limitations: The ODA standard was selected to support tiled raster graphics images because it was visualized as the primary specification for implementations supporting applications containing compound documents consisting of text (character), geometric graphics, and raster graphics content. Implementing the ODA standard has not advanced or been as widespread as was envisioned. In fact, there appears to be very little support for ODA. The known exception is the requirement to support raster graphics applications in a data repository environment for the Department of Defense. ODA is not required for implementation of the raster specification.

Conformance testing: NIST has developed formal testing procedures and policy to implement an ODA Raster DAP validation service. The testing service is capable of fully testing the "Intermediate ODA Raster DAP" level of the specifications. The "ANSI/AIIM MS-53 (Untiled)" level of the specifications can be tested to a limited extent, i.e., capable of testing ITU-T Rec. T.6 (Group 4) compressed data, but not ITU-T Rec. T.4 (Group 3) compressed data. Testing for the "Full ODA Raster DAP" level is not yet available.

Future plans: There are proposals within ISO/IEC to add the JPEG compression algorithm to the base ODA standard. Upon completion, it can then be added to the ODA Raster DAP.

Alternative specifications: CGM supports raster graphics images as well as geometric (vector) graphics.

4.12.7 Image Compression

Specification Title: Joint Photographic Experts Group Compression Specification - JPEG (IS10918:1992) Standard: Digital Compression and Coding of Continuous-tone Still Images.

Specification Available From: ANSI

Publication Date: 1992

Sponsoring Organization: ISO/IEC JTC 1/SC2 Working Group 10

Applicability: This standard is applicable to continuous-tone (grayscale or color) digital still image data. It is applicable to a wide range of applications which require use of compressed images. It is not applicable to bi-level image data. The primary use is as a standardized way of compressing and storing both 24-bit color and gray scale images. With this specification, compressed formatted image files are more efficiently transmitted across networks.

Level of Consensus: JPEG is defined by international standard ANSI/ISO IS10918:1992, and is widely used by the graphics and image community for both storage and transmission of digital imagery.

Product Availability: There are numerous applications using the JPEG specification both to create compressed image files and to decompress and view them. Freeware and Shareware applications abound on the Internet as well as all the leading on-line computer services.

Completeness: There are three elements specified in this standard:

1) An *encoder*, which is an embodiment of an *encoding process*. An encoder takes as input digital source image data and table specifications, and by means of a specified set of procedures generates compressed image data as output.

2) A *decoder*, which is an embodiment of a *decoding process*. A decoder takes as input compressed image data and table specifications, and by means of a specified set of procedures generates digital reconstructed image data as output.

3) An *interchange format*, which is a compressed image data representation that includes all table specifications used in the encoding process. The interchange format is for exchange between application environments.

Maturity: The underlying technology of compression via the use of discrete cosine transformation functions has existed for several years. The JPEG standard is now accepted universally, and embedded in numerous applications. It is also one of the preferred ways of downloading and uploading photographic images to the World Wide Web.

Stability: The standard is considered to be very stable. New variations, however, are being developed constantly. The shell format is interoperable across platforms and is considered to be platform independent.

Known Problems/Limitations: A parameter matrix is used within the specification that is tailored to various imagery compression requirements. The resultant resolution of the image may vary depending upon the amount of compression that is obtained. This specification is considered to be a *lossy* compression technology whereby image information is lost in the compression process. If one needs to have the original digital image representation intact, then a *lossless* compression technology, such as Lempel-Ziv-Welsh (LZW), would be better suited for that particular case. Note that LZW is a patented algorithm and requires licensing for use. In general, most of the color spectrum that is lost in the compression process is not missed by the normal optics of human vision.

Conformance Testing: There are no standard conformance tests for the standard. The format is very specific in nature with no variations of the shell structure. This makes it an interoperable format specification.

Future Plans: Refinement of the JPEG parameter matrix is a continuing developmental process being carried out by ISO/IEC/JTC1/SC2/WG10.

Alternative Specifications: Proprietary technologies are the only alternatives to the standard. Licensing is an issue with respect to implementations based on those technologies. Fractal compression formats for moving imagery as well as still imagery are being developed by industry. This technology promises to deliver very high compression ratios (e.g., 800 to 1) with resolution independence. It is also a lossy compression technology with the added problem of introducing false artifacts that are not part of the original image. Fractal compression technology is also considered to involve an asymmetric process where enormous amounts of processing power is needed on the compression side, but very little is needed on the decompression side (or the viewing side). Other standards using this specification include SGML, and MPEG.

4.12.8 Video Compression

Specification Title: Motion Pictures Expert Group MPEG-1 - Coding of Moving Pictures and Associated Audio for Digital Storage Media up to about 1.5 Mb/s - part 2 Video and part 3 Audio, ISO 11172

Specification Available From: ANSI

Publication Date: 1992

Sponsoring Organization: ISO/IEC JTC 1/SC2 WG11

Applicability: MPEG-1 addresses the compression of video signals at about 1.5 megabits/second. MPEG Audio addresses the compression of a digital audio signal at the rates of 64, 128, and 192 kilobits/second per channel.

Level of Consensus: MPEG-1 is defined by international standard ANSI/ISO IS11172:1992, and is widely used by the digital video, graphics and moving image communities for both storage and transmission of digital moving imagery.

Product Availability: There are a number of applications using the MPEG specification both to create compressed image files and to decompress and view them. Freeware and Shareware applications are obtainable on the Internet as well as all the leading on-line computer services.

Completeness: The MPEG video compression algorithm relies on two basic techniques: block-based motion compression for the reduction of temporal redundancy, and transform domain-based compression for the reduction of spatial redundancy. Motion-compensated techniques are applied with both casual (pure predictive coding) and non-casual predictors (interpolative coding). The remaining signal (prediction error) is further compressed with spatial redundancy reduction (DCT). The information relative to motion is based on 16 x 16 pixel blocks and is transmitted together with the spatial information. The motion information is compressed using variable-length codes to achieve maximum efficiency of video and audio data compression for data stored on mass media, such as optical media including CD-ROM and writable CD, network servers, and DAT Tape; and storage disks. MPEG compression techniques are geared to asymmetric applications where the decompression process is extremely faster than the compression process. Such applications as electronic publishing, video games, and delivery of movies make heavy use of this technology.

Maturity: The underlying technology of compression via the use of the MPEG-1 transformation functions has been in existence for several years. The MPEG-1 standard is now accepted universally, and embedded in numerous applications. It is also the preferred way for downloading and uploading video and other motion images to the World Wide Web.

Stability: The standard is considered to be very stable. New variations, however, are being developed constantly (i.e., MPEG-2). The shell format is interoperable across platforms and is considered to be platform independent.

Known Problems/Limitations: This specification is considered to be a *lossy* compression technology whereby image information is lost in the compression process. Inter-frame compression is achieved by dropping duplicate information contained in each frame and regenerating that information from previous frames or from a transform algorithm. At times, the regenerated information does not quite match reality. If one needs to have the original digital image representation in tact, then a *lossless* compression technology, such as LZW, would be better suited for that particular case. Note that LZW is a patented algorithm and requires licensing for use. In general, most of the color spectrum that is lost in the compression process is not missed by the normal optics of human vision.

Conformance Testing: There are no standardized conformance tests for the standard. Most implementations use a format that is very specific in nature and with no variations of the shell structure. This makes it an interoperable format specification.

Future Plans: Refinement of inter-frame compression technology is a continuing developmental process being carried out by ISO/IEC/JTC1/SC2/WG11.

Alternative Specifications: Proprietary technologies are the only alternatives to the standard. Licensing is an issue with respect to implementations based on those technologies. Fractal compression formats for moving imagery as well as still imagery are being developed by industry. This technology promises to deliver very high compression ratios (e.g., 800 to 1) with resolution independence. It is also a lossy compression technology with the added problem of introducing false artifacts that are not part of the original image. Fractal compression technology is also considered to involve an asymmetric process where enormous amounts of processing power is needed on the compression side, but very little is needed on the decompression side (or the viewing side). Other standards using this specification include SGML, and various transmission protocol standards.

4.12.9 Compact Disk File and Directory System

Specification Title: CD-ROM Volume/File Structure ISO/IEC IS9660:1988

Specification Available From: American National Standards Institute (ANSI)

Publication Date: 1988

Sponsoring Organization: ISO/IEC

Applicability: ISO 9660 is used as a standard publishing specification in the creation of compact disk read-only memories (CD-ROM) and compact disk (CD) recordable media. This standard describes volume, directory, and file systems on CD-ROM optical storage media as well as CD recordable media.

Level of Consensus: ISO 9660 is the universal standard defining the preferred volume and file structure for all CD-ROM authored disks. It is used across a variety of processing platforms, and is the only viable standard in this area at this time.

Availability: Virtually all CD-ROM manufacturers and CD-ROM drive software providers use ISO 9660 as the file system for organizing and locating files and directories on CDs.

Completeness: The specification is both extensive and complete. Extensions exist that are referenced as the "XA" extensions that permit the interleaving of audio recorded data with textual data.

Maturity: The standard has acheived a very high level of user acceptance, and virtually all CD-ROM players are able to access the ISO format. In use since 1988, the standard was preceded by multiple specifications before industry developed concensus on a single specification. Other standards, such as SGML, JPEG, and MPEG use or rely on aspects of the ISO 9660 specification.

Stability: Modifications to the specification are planned within the next 1 to 2 years to add CD recording programming interfaces and multi-session interfaces. No changes in the basic format provided in the specification are foreseen.

Known Problems/Limitations: The ISO format has limited file naming capabilities (maximum 8-character names with 3-character file extension). Sub-directory depth is limited to 8 levels.

Conformance Testing: None.

Future Plans: Work is underway to define interfaces for multi-session and CD-recordable options. This work is expected to be completed within 1 to 2 years.

Alternative Specifications: None.

4.12.10 Graphical Product Data Interchange

Specification title: FIPS 177 Initial Graphics Exchange Specification (IGES)

Specification available from: NTIS, ANSI, USPro

Publication date: December 1992

Sponsoring organization: IGES/PDES Organization (IPO) of the U.S. Product Data Association (US PRO)

Applicability: IGES standardizes the representation of specific types of complex graphic objects and attributes for data interchange. In this instance, product data interchange encompasses technical drawings, documentation, and other data required for product design and manufacturing, including geometric and nongeometric data such as form features, tolerances, material properties, and surfaces. The information typically associated with computer-aided design and manufaeturing (CAD/CAM) can be described. IGES does not cover the complete lifecycle of manufactured products: it addresses only the specification of products; not the manufacturing process relationships.

Level of consensus: The specification was originally defined in National Bureau of Standards Interim Report (NBSIR) 88-3813. It has been defined as ANSI standard, ANSI Y14.26-1989 (also known as IGES 4.0), by the American Society of Mechanical Engineers (ASME). IGES 5.2 (US PRO/IPO-100) was released in November 1993 and is an American National Standard. The FIPS is being revised to adopt IGES 5.2.

Product availability: Numerous implementations of IGES are available in the marketplace.

Completeness: IGES defines the representation of engineering data as well as technical illustrations. The IGES specification allows for the exchange of computer-aided design/computer-aided manufacturing (CAD/CAM) data through the extensive support of wireframe geometry as well as advanced surfaces and solids (both B-rep and Constructive Solid Geometry). The IGES specification preserves the topology and geometry of modeled objects through the use of 3-D coordinates, vectors, and transformation matrices. IGES is further enhanced by CALS Specification MIL-PRF-28000, which defines the content of IGES files for the following classes of applications:

Class I -- Technical Illustration Subset
Class II -- Engineering Drawing Subset
Class III -- Electrical/electronic Applications Subset (slated to be replaced by Layered Electrical Product Application Protocol)
Class IV -- Numerical Control Manufacturing Subset
Class V -- 3-D Piping Application Protocol

In addition, the IGES 5.1 Recommended Practices Guide, released in May 1992, assists both users and implementors in the utilization of the IGES specification.

Maturity: IGES development and implementation has been active for the last 15 years and the specification is expected to be utilized into the next century. The National IGES User Group (NIUG), established in 1990, facilitates the use of IGES through educational programs, articles, and user forums. Work on registration of IGES on the Internet as a MIME format was completed in April 1995.

Stability: IGES 5.3 will be published by US PRO in 1995. As the specification advances with newer versions, compatibility will be maintained.

Known problems/limitations: In order to achieve interoperability where SGML is concerned, users should refer to MIL-HDBK-28001 and MIL-PRF-28001 in addition to MIL-PRF-28000. The SGML interoperability requirements and profiling specifications for SGML within the IGES environment are included there.

Conformance testing: NIST operates an IGES testing service for FIPS 177 (IGES 4.0), CALS MIL-PRF-28000 Class II (Engineering Drawing Application Subset), and IGES 5.1. These services have been available since November 1994.

Future plans: Work is underway on the next version of IGES which will contain a new global parameter field indicating the application protocol, subset, or CALS class to which the IGES file belongs. Publication of a Layered Electrical Product (LEP) Application Protocol for use in CALS

is expected in 1995. Development of a FIPS is expected for MIL-PRF-28000 Class II (CALS) as well as IGES 5.2 and beyond.

Alternative specifications: STEP (See sec. 4.12.11).

4.12.11 Product Lifecycle Data Interchange

Specification title: Planned FIPS on Standard for the Exchange of Product Model Data (STEP) [ISO 10303]

Specification available from: ISO TC184/SC4 Secretariat (NIST)

Publication date: December 1994 (draft FIPS available)

Sponsoring organization: ISO (NIST)

Applicability: STEP is an advanced form of representing complex data objects for interchange. It is used in total lifecycle descriptions of engineered products that can be implemented on advanced manufacturing systems. This includes specification of products throughout the stages of their lifetimes. These stages consist of initial concept design, engineering analysis, manufacturing production, and product support. ISO 10303 consists of multiple volumes. These volumes specify the elements of the STEP strategy (i.e., Application Protocols, Information Models, Implementation Methods, Conformance Tools, and Description Methods).

Level of consensus: The specification is defined in international standard ISO 10303. (STEP was previously known as Product Data Exchange Specification [PDES], but the name of the proposed standard was changed to differentiate it from PDES which is actually the initiative that is creating STEP. PDES is now called Product Data Exchange using STEP.) A draft FIPS has been announced and is planned to be published in early 1996.

Product availability: Key elements of STEP are already an international standard. Several vendors have released commercial products and many others have announced 1995 delivery dates. Pilot projects are underway with some early implementations expected in late 1995 or early 1996.

Completeness: The standard defines a complete product lifecycle including all aspects of describing technical diagrams and documents in a neutral format for transmission over communications networks and processing by numerically controlled machining and assembly tools.

Maturity: STEP includes the full life cycle of products from initial requirements and design through final production and installation. Elements of STEP that address geometry and configuration management are stabilizing as international standards.

Stability: The core requirements of STEP have been defined in the international standard. Further work is being done on application profiles that define specific environments for the use of STEP.

Known problems/limitations: None.

Conformance testing: A testing program is planned for implementation by the end of 1995. Tests will include Application Protocol 203 (ISO 10303 Part 203) Configuration Controlled Design. The standard includes abstract test suites.

Future plans: Additional elements of STEP are currently in development. A FIPS based on the international standard is expected to be approved in 1996.

Alternative specifications: IGES

4.12.12 Electronic Data Interchange

Specification title: FIPS 161 Electronic Data Interchange (EDI)

Specification available from: NTIS

Publication data: March 29, 1991

Sponsoring organization: X12, United Nations Working Party UN/ECE/WP.4

Applicability: Electronic data interchange (EDI) is a procedure in which instances of documents to be interchanged between separate organizations are converted to strictly formatted sequences of data elements and transmitted as messages between computers. The strict formatting permits computer programs to assemble and disassemble the messages and communicate the data of the messages to and from application programs. EDI is intended primarily for documents that are nontext (i.e., that consist of a sequence of numeric or alphanumeric fields), although an application standard has been developed that allows for the inclusion of product specifications in the form of graphics as parts of such messages. Typical applications are in the procurement process, such as transmitting invoices and purchase orders, and for governmental regulatory activities, such as submission of tax returns and customs forms.

Implementation of EDI requires a family of standards. A family must include (1) syntax standards that specify message organization, the character set for data, and the control characters that start, end, and separate data elements and other groupings within the message; (2) standards for message envelopes that enable a communications protocol to carry and direct the message; (3) data element standards that specify data element types, and for some data elements, the list of data items permitted; (4) data segment standards that form meaningful groupings of data elements; and (5) standards for specific document types.

Level of consensus: There are two widely used families of standards. The U.S. domestic standards have been developed by ANSI-accredited standards committee, X12. There may be as many as 30 000 domestic implementations of X12 EDI at this time. The international family of standards, called EDIFACT (EDI For Administration, Commerce, and Transport) is developed and maintained by the United Nations Economic Commission for Europe, Working Party Four on Trade Facilitation (UN/ECE/WP.4). U.S. input to EDIFACT development is through the Pan American EDIFACT Board, one of five EDIFACT boards that cover the world. There may be several thousand EDIFACT implementations at this time, and the X12 committee has recently voted to adopt the EDIFACT syntax by 1997.

Product availability: Implementation software is widely available. Users with more than a few interchange partners employ computer-based networks as store-and-forward delivery agents. These so-called value-added networks, or VANs, are similarly widely available.

Completeness: The two families of standards, X12 and EDIFACT, are complete to the extent that the syntax and supporting standards are available to enable interchanges to occur for any document type that has been standardized. Development of standards that support additional document types is continuing at a rapid pace in both families of standards.

Maturity: The concept is proven, and the number of implementations continues to increase.

Stability: New versions and releases are being produced approximately on a yearly basis. Users need to stay current. The conversion of X12 implementations to EDIFACT could introduce costs of retrofitting.

Known problems/limitations: The acceptance of electronic documents in a court of law has been considered questionable in the past. With wide use of EDI, and with change and/or reinterpretation of statutes and regulations, as well as with adoption of electronic techniques for originator authentication and transmission integrity, this issue will be less important in the future. Maintenance of audit trails and assurance of trustworthy recordkeeping will assist, however, in providing confidence in the authenticity of electronic documents.

Conformance testing: NIST is studying this issue at the present time.

Future plans: FIPS 161 will be updated to reflect X12 adoption of EDIFACT standards. The implementation of a Federal digital signature standard and development of a national infrastructure for management and distribution of cryptographic keys for that standard will promote the use and acceptance of EDI. Development of products that implement CCITT standards X.400, X.435, and the X.500 series will further enhance EDI as an accepted data interchange procedure.

Alternative specifications: None.

4.12.13 Spatial Data Interchange

Specification title: FIPS 173-1 Spatial Data Transfer Standard (SDTS)

Specification available from: National Mapping Division, U.S. Geological Survey (USGS)

Publication date: Draft available.

Sponsoring organization: USGS

Applicability: This standard is mandatory in the acquisition and development of government applications and programs involving the transfer of digital spatial data among heterogeneous computer systems. The use of the SDTS applies when the transfer of digital spatial data occurs, or is likely to occur, within or outside of the Federal government. SDTS is not tied to particular data structures, classes of computer platforms, or distribution media.

Level of consensus: A recent Geographic Information System (GIS) industry survey indicates that 65 percent of GIS vendors intend to support SDTS. This is significant since more than 90 percent of GIS are turn-key systems. Many of the specifications included in SDTS have long histories of development and use.

Product availability: The U.S. Geological Survey (USGS) has developed public domain software for encoding and decoding data into and out of the SDTS neutral exchange file.

Completeness: SDTS provides specifications for the organization and structure of digital spatial data transfer, definition of spatial features and attributes, and data transfer encoding.

Maturity: Work began on this standard in 1982 with the participation of academia, industry, and the U.S. Government. International efforts to develop a spatial data interchange standard have all emulated SDTS in various ways. The testing, modification, and refinement of SDTS has occurred over an 8 year period.

Stability: SDTS was designed to be modular and extensible. The neutral exchange format specified for SDTS implementation is independent of SDTS.

Problems/limitations: Unknown

Conformance Testing: Software for conformance testing of SDTS is currently being planned.

Future plans: The SDTS Vector Profile has undergone several revisions and is now in the final refinement and testing phase. SDTS Raster Profile development is underway.

Alternate specification: None

4.13 Graphics Services

Graphics services provide the interfaces for manipulating and programming applications concerning images and graphics in a device-independent manner. The specifications included in this service area are the Graphical Kernel System (GKS) FIPS 120-1, and the Programmer's Hierarchical Interactive Graphics System (PHIGS) FIPS 153-1. They are targeted at different types of users and applications.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	PRL
FIPS 120-1 GKS	●	●	●	●	●	●
FIPS 153-1 PHIGS	●	●	●	●	●	●

Legend: ●-high evaluation O-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
PRL -- Problems/limitations

4.13.1 Two-Dimensional Graphics

Specification title: FIPS 120-1 Graphical Kernel System (GKS)

Specification available from: NTIS

Publication date: January 8, 1991

Sponsoring organization: Standards Committee X3H3

Applicability: GKS provides a language to program two-dimensional graphical objects that will be displayed or plotted on appropriate devices (raster graphics and vector graphics devices).

Level of consensus: The GKS FIPS is based on ANSI Standard X3.124-1985 and ISO Standard 7942:1985.

Product availability: A full range of products and automated tools based on GKS has been available from various vendors for 7 or more years.

Completeness: The standard includes constructs and library calls for virtually any kind of two-dimensional graphic image.

Maturity: Initial work started on this specification in 1978 and has been developed substantially by international organizations in the ensuing years. It was founded on a graphics standards methodology developed in 1976.

Stability: The GKS specification is in the process of being updated.

Known problems/limitations: None.

Conformance testing: NIST licenses and maintains a conformance test suite for GKS. Using this test suite, NIST is currently operating a GKS Test Service to test implementations for conformance to the FIPS. The test suite is available for the Fortran binding to GKS. A registered test report will be issued after the conduct of tests. A certificate of validation will be issued only to implementations passing the tests with no failures. If failures have occurred, the specific failures will be identified in the registered test report. The results of tests on individual implementations that receive certificates will be posted in the NIST VPL. A C language binding for the test suite will be available by late 1995.

Bindings: Bindings for Ada, Fortran, and Pascal have been defined and standardized.

Future plans: The GKS test suite underwent revision when NIST became the maintenance organization for the test suite.

Alternative specifications: PHIGS (see sec. 4.13.2)

4.13.2 Interactive and Three-dimensional Graphics

Specification title: FIPS 153-1 Programmer's Hierarchical Interactive Graphics System (PHIGS)

Specification available from: NTIS

Publication date: January 18, 1995

Sponsoring organization: Standards Committee X3H3

Applicability: PHIGS defines a language to program two- and three-dimensional graphical objects that will be displayed or plotted on appropriate devices in interactive, high-performance environments, and for managing hierarchical database structures containing graphics data.

Level of consensus: The FIPS is based on ANSI Standards X3.144-1988 and X3.144.1-1988, and ISO Standard 9592:1988.

Product availability: Numerous implementations are available for various hardware/software platforms.

Completeness: PHIGS is a full-functioned specification for the development of interactive two- and three-dimensional graphics applications that manage hierarchical database structures containing graphics data.

Maturity: Many of the concepts for this standard were drawn from previous work. Chief among those works are the Association for Computing Machinery (ACM) SIGGRAPH Graphics Planning Committee Core Graphics System and the Standard Graphical Kernel System (GKS) ANSI X3.124-1985.

Stability: No changes are planned in the next 1 to 3 years.

Known problems/limitations: Unknown

Conformance testing: The PHIGS test suite tests implementations using the Fortran and C bindings for conformance to the FIPS. A registered test report is issued upon completion of testing. A certificate of validation will be issued only to implementations passing the tests with no failures. If any failures have occurred, they will be identified in the registered test report.

Bindings: Bindings for Fortran, C, and Ada have been adopted.

Future plans: A binding for Pascal is under development. A new standard, called PHIGS Plus, is being developed which adds shading, lighting, and other advanced graphics programming capabilities that were not intended for inclusion in the original version. Conforming PHIGS programs will be able to execute under PHIGS Plus with no changes.

Alternative specifications: None.

4.14 Network Services

This area of the APP includes data communications, transparent file access, personal/microcomputer support, distributed computing support, distributed systems management, and network application program interfaces.

SPECIFICATION	LOC	PAV	CMP	MAT	STB	PRL
PII API IEEE P1003.1g		O		O		
ACSE IEEE 1238					●	
FIPS 146-2 POSIT	●	●	●	●	●	●
ISDN ASI	●		O	●	O	O
ISDN FIPS 182	●	O	●	●	●	●
DCE RPC	O	O	O	O	O	O
CORBA	O		O	O		
X.400 API IEEE 1224.1	O	O	●	O	●	●
X.500 API IEEE P1224.2	O		●	●	●	●
OMNI*Point*	●	O	O	●	●	O
FIPS 192 GILS	●	●	●	●	●	●
NISO Z39.50	●	●	●	O	●	●
DES FIPS 46-2	●	●	●	●	●	●
DSS FIPS 186			●	●		●

Legend: ●-high evaluation O-average evaluation blank-low evaluation

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
PRL -- Problems/limitations

4.14.1 Communication API for Protocol Independent Interfaces

Specification title: Protocol Independent Interfaces (PII) IEEE P1003.1g

Specification available from: IEEE

Publication date: Draft available

Sponsoring organization: IEEE

Applicability: P1003.1g (formerly P1003.12) defines the protocol-independent application interfaces to enable one process to communicate with another local process or a remote process over a network.

The Detailed Network Interface (DNI) specification supports protocol-independent local and network process-to-process communications with access to protocol-dependent features. DNI is intended to provide access to protocol-specific features of the underlying network for highly portable applications that need access to sophisticated network features. Since two currently recognized industry practices in the DNI specification are X/Open Transport Interface (XTI) and BSD Socket interface, a dual DNI standard (DNI/XTI and DNI/sockets) specification is being created for P1003.12. The DNI/XTI and DNI/Sockets APIs will provide transport layer access. The DNI/Socket API will also allow access to lower layers. The intermixing of DNI/XTI calls and DNI/Sockets will not be specified. That is, the specification will not prescribe what combinations or subsets of both XTI and Sockets should be implemented.

Level of consensus: An approved standard is expected in late 1995.

Product availability: Products currently exist based on XTI and sockets.

Completeness: The completed specification will contain language independent specification (LIS) and C bindings.

Maturity: The draft specification incorporates the technology of the XPG4 version of the X/Open CAE Specification—X/Open Transport Interface (XTI), dated January 1992, and the 4.4 BSD sockets interface, with interface mappings to ISO Transport and Internet Transport information for XTI. These are implementations of products that have existed for 5 or more years.

Stability: The specification is in ballot and may undergo modifications because of this process.

Known problems/limitations: Work on the Simple Network Interface (SNI) and the Naming Interface has been postponed in order to ballot the DNI specification.

Conformance testing: Test methods will be defined for measuring the conformance of implementations to this specification.

Bindings: The standard is defined in terms of a language independent specification and a C language specification.

Future plans: Considerable work still needs to be done on the Simple Network Interface (SNI) and the Naming Interface. SNI and the Naming Interface will be included in the future. Simple Network Interface (SNI) will support protocol-independent network process-to- process communications in a protocol-independent manner. SNI is intended to provide a simple view of underlying networks for portable applications that do not need access to sophisticated network features. The Naming Interface will support naming/addressing needs for SNI and DNI. The P1003.12 naming interface will be based on the P1224.2 naming interface and P1224 Object Management work.

Alternative specifications: X/Open CAE Specification—X/Open Transport Interface (XTI), January 1992.

4.14.2 Communication API for OSI Services

Specification title: OSI ACSE/Presentation Application Program Interfaces IEEE P1238

Specification available from: IEEE

Publication date: December 1994

Sponsoring organization: IEEE

Applicability: This specification provides an API between applications and the OSI Association Control Service Element (ACSE) and presentation services.

Level of consensus: Consensus has been reached on a base document for an OSI ACSE/Presentation API. It is now being processed through ISO fast-tracking to become an international standard.

Product availability: Implementations are beginning to become available.

Completeness: The specification has language-independent and C language bindings, as well as Test Methods.

Maturity: The specification is under development. The underlying model is the OSI seven-layer model.

Stability: No changes are expected for the next 3 to 5 years.

Known problems/limitations: Suitability of different language bindings may be a concern, as well as high-level to low-level mappings among different layers in the OSI Reference Model.

Conformance testing: Test assertions are under development as part of the specification. These assertions are compatible with existing ACSE/Presentation tests.

Bindings: IEEE 1353 defines a C binding for ACSE.

Future plans: POSIT will include the ACSE API as one of its specifications.

Alternative specification: None

4.14.3 Communication Protocols

Specification title: FIPS 146-2 Profiles for Open Systems Internetworking Technologies (POSIT)

Rationale: The primary objectives of this standard are to achieve interconnection and interoperability of computers and systems that are acquired from different manufacturers in an open systems environment; to reduce the costs of computer network systems by increasing alternative sources of supply; to facilitate the use of advanced technology by the Federal Government; to provide guidance for the acquisition and use of networking products implementing open, voluntary standards such as those developed by the Internet Engineering Task Force (IETF), the International Telecommunication Union—Telecommunications Standardization Sector (ITU-T; formerly the Consultative Committee on International Telegraph and Telephone [CCITT]), and the International Organization for Standardization (ISO).

Specification available from: NTIS

Publication date: May 15, 1995

Sponsoring organization: NIST

Applicability: FIPS 146-1 adopted the Government Open Systems Interconnection Profile (GOSIP) which defines a common set of Open Systems Interconnection (OSI) protocols that enable systems developed by different vendors to interoperate and the users of different applications on those systems to exchange information. FIPS 146-2 modifies FIPS 146-1 by expanding the selections of protocol suites that Federal agencies can specify when they acquire networking products and services, and communications systems and services.

POSIT provides for use of several protocol suites that are widely available in U.S. and international markets. These include GOSIP and TCP/IP (the Internet Protocol Suite or IPS) as the two primary protocol suites. The reference document containing the combined profiles for Open Systems Interconnection (OSI) specifications is the IGOSS—Industry/Government Open Systems Specification NIST Special Publication 500-217. IGOSS was issued jointly by U.S. industry, the U.S. Government, and the Government of Canada. NIST Special Publication 500-224, "Stable Implementation Agreements for Open System Environments, Version 8, Edition 1, Part 26," December 1994 contains a series of IPS (TCP/IP) profiles for use in acquisitions.

Level of consensus: Many of the protocols included in POSIT, particularly those from TCP/IP, have existed for more than 20 years. Each of the TCP/IP protocols has been tested through expert review and implementation of experimental models before acceptance by the IETF. The OSI protocols are founded on a solid theoretical basis and have been implemented in numerous products. The OSE Implementors' Workshop (OIW) has been working on appropriate implementation agreements between vendors and users for over 5 years.

Product availability: Numerous products that implement the POSIT protocols exist and are available in the marketplace.

Completeness: The set of protocols covers a large portion of the computer networking, manufacturing and office automation, and industrial information protocols necessary for disparate types of organizations to communicate internally and externally.

Maturity: All of the protocols have existed since before 1988 and many of the protocols have a basis in theoretical and pragmatic work done since the early 1970s.

Stability: Most of the changes that will occur over the next 2 to 3 years will be in the areas of additional capabilities. One significant change that will occur in this period is the expansion of potential identifiers and addresses for individual network nodes. Additional security protocols will also expand POSIT capabilities.

Known problems/limitations: Not all of the protocols map to one another within each of the protocol suites included in POSIT. Translation between protocols will require new methods of affecting the interaction between protocols from different suites.

Conformance testing: Conformance testing is available for many of the OSI protocols refereneed in POSIT. Several U.S. Government and industry organizations are researching the possibilities of developing other conformance testing methods for additional protocols that are not already covered by existing programs.

Future plans: NIST plans to work with other government agencies and with industry to develop additional profiles based on open, voluntary standards and to publish these profiles in independent documents.

Alternative specifications: None.

4.14.4 Communication API for Integrated Digital, Video, and Voice

Specification title: Application Software Interface (ASI) (for accessing and administering Integrated Services Digital Network [ISDN] services) (Defined in the *North American ISDN Users' Forum Agreements on Integrated Services Digital Network (ISDN)*)

Specification available from: National Institute of Standards and Technology

Publication date: March 1994

Sponsoring organization: NIST

Applicability: The Application Software Interface (ASI) focuses on the definition of a common application interface for accessing and administering ISDN services provided by hardware commonly referred to in the vendor community as Network Adapters (NAs).

Level of consensus: The ASI is based on the implementation agreements produced by the North American ISDN Users' Forum (NIUF). These agreements are, in general, based upon relevant ANSI standards.

Product availability: Current products are proprietary products based on proprietary specifications. Products based on ASI Version 1 are emerging. More products are expected as the standardization process continues and the specification becomes more stable. Various communications providers across the United States are either providing ISDN services or are expanding in order to offer ISDN services.

Completeness: The ASI is an evolving specification. Items for inclusion are based on services defined in ANSI and the NIUF. As the definitions emerge from these bodies, they are included in the ASI. The existing agreements include the ISDN architecture, base protocol specifications, service specifications, and conformance testing requirements.

Maturity: While ISDN usage is not widespread, the technology is well defined and understood. The ASI specification provides a uniform interface to these services.

Stability: This specification is an evolving interface and changes are anticipated to incorporate new features. These changes are primarily due to additional ISDN features as specified by ANSI and the NIUF. These changes are expected to be in the form of additions to the existing specification.

Known problems/limitations: The greatest known problem is the limited set of service interfaces available through the ASI today. As the services are defined in the standards bodies and the NIUF, the interfaces will be included in the ASI.

Conformance testing: Conformance tests are planned for the ASI.

Future plans: The ASI will continue to include additional ISDN services in its specification. Additional work includes device control and an additional higher level interface for POSIX and other operating system interfaces. Future versions of the FIPS for ISDN are expected to include the ASI. The ASI is expected to be submitted for consideration as an ANSI standard.

Alternative specification: None.

4.14.5 Communication Protocols for Integrated Digital, Video, and Voice

Specification title: FIPS 182 Integrated Services Digital Network (ISDN)

Specification available from: National Institute of Standards and Technology

Publication date: October 1993

Sponsoring organization: NIST

Applicability: FIPS 182 compiles the existing NIUF agreements for ISDN as developed and approved in the NIUF. The agreements are published in *North American ISDN Users' Forum Agreements on Integrated Services Digital Network (ISDN)*. These agreements cover Layer 1 Basic Rate Interface (BRI) at the U, and S/T reference points; Layer 1 Primary Rate Interface (PRI) at

the U reference point; Layer 2 BRI and PRI; Layer 3 BRI Basic Call Control for Class I equipment; and Layer 3 PRI Basic Call Control for Class II equipment.

Level of consensus: The ISDN FIPS is based on the implementation agreements produced by the NIUF. These are, in general, based upon relevant ANSI standards.

Product availability: Currently, only proprietary products are available. Vendors will soon propose products based on Bellcore National ISDN-X (NI-X), for which the current version is NI-1. Various communications providers across the United States are either providing ISDN services or are expanding in order to offer ISDN services.

Completeness: The ISDN FIPS adopts the implementation agreements from the NIUF. These agreements evolve through an ongoing process. As additional agreements are made, these will become a part of future revisions of the FIPS.

Maturity: While ISDN usage is not widespread in the United States, the technology is well defined and understood. Standards for ISDN have existed for a number of years.

Stability: It is expected that this FIPS will be revised to include additional implementation agreements from the NIUF.

Known problems/limitations: While the protocols provide basic services, additional protocols are needed to complete the architecture. Interfaces to these protocols are being defined for various operating system implementations, but they are incomplete.

Conformance testing: The FIPS references the conformance tests that have been completed by the NIUF. These include the Layer 1 BRI S/T interface and the Layer 2 BRI Link Access Procedure on the D channel (LAPD). Plans exist for continuing this process.

Future plans: The Bellcore National ISDN-X process continues to evolve and to produce ISDN implementation agreements. Vendors are now implementing NI-1. The work of the NIUF is an ongoing process. This work will be included in future revisions of the FIPS as updates to implementation agreements.

Alternative specifications: None.

4.14.6 Remote Procedure Call

Specification title: OSF Distributed Computing Environment (DCE) Remote Procedure Call (RPC) Component

Specification available from: Open Software Foundation (OSF)

Publication date: July 1995

Sponsoring organization: OSF

Rationale: Distributed system technology is one of the major focal points of open systems. The ability to distribute processing among heterogeneous platforms in a network is a requirement for establishing distributed open systems.

Applicability: Distributed computing services include specifications for remote procedure calls and distributed realtime support in heterogeneous networks (as opposed to single node support as specified in operating system services). Distributed access services include functional support for submitting, starting, and stopping processes among processors in a heterogeneous network. OSF RPC includes support for naming, dynamic binding, and security (authentication, data privacy, and integrity protection). An API for OSF RPC is defined.

Level of consensus: The content of OSF RPC is determined by OSF members.

Product availability: Vendor partial implementations are available and based on the OSF specification.

Completeness: No specifications exist that define a complete set of functions necessary to provide remote procedure communications for all types of application platforms (i.e., the language-independent representation of remote procedure calls). OSF RPC contains a language mapping for C.

Maturity: In general, OSF specifications are based on object-oriented structures and relationships. The underlying services and data formats are well-established, but the objects to be managed are still evolving.

Stability: Other industry consortia are reviewing the possibility of adopting OSF RPC. Other specifications are emerging as possible alternatives.

Known problems/limitations: The specification is incomplete and still in a draft state.

Conformance testing: Validation suites will be available at the time the specification is complete for OSF RPC.

Bindings: A language mapping for C function and subroutine calls is defined in the specification.

Future plans: Continued development of the specification to include new technology as it becomes available.

Alternative specifications: ONC RPC (Open Network Computing Remote Procedure Call). CORBA (Common Object Request Broker Architecture).

4.14.7 Object Request Broker

Specification Title: The Common Object Request Broker: Architecture and Specification (Revision 2.0); and CORBAservices: Common Object Services Specification (Revised Edition)

Specification Available From: The Object Management Group (OMG)

Publication Date: July 1995 (CORBA 2.0) and March 1995 (CORBAservices)

Sponsoring Organization: The Object Management Group (OMG).

Rationale: The use of object request broker (ORB) interoperability and services is important to many organizations. The differences among object architectures from competing vendors leads to the need to provide a mechanism for describing these architectures to external environments and to allow objects based on these architectures to interact.

Applicability: The CORBA specifications address requirements for object request broker interoperability and services including—

- standard application program interfaces (APIs) provided by an ORB to enable the construction of request level inter-ORB bridges; and

- an Internet Inter-ORB Procotol (Internet IOP, or IIOP), which can be supported at application or ORB level.

The CORBA specifications provide the capability to develop object systems which consist of client applications and object implementations (CORBA terminology for server). The client application may access the object implementation wherever that object implementation may reside, i.e., in a library on the same host as the client, in another process on the same host as the client, or on a different host from the client where the two hosts are connected by a network.

CORBA interoperability provides interoperability between client applications and object implementations when the client application and object implementation are located on different hosts connected by a network. This capability has two dimensions. The ORB specification provides the implementation guidance enabling a client application to locate the object implementation even if the object implementation migrates to another host. The ORB specification also provides the implementation guidance enabling the client application to transmit a request to an object implementation and receive the response from that object implementation.

At a minimum, a CORBA implementation includes the ORB, the Interface Definition Language (IDL), the standard services in the CORBA specification, and one language mapping. Optionally, a CORBA implementation may include additional language mappings, interoperability, and additional services from the CORBAservices specification. Note that all of the components of a CORBA Implementation need not come from a single producer. In particular, services from the CORBAservices specification may come from a producer different from the one that provides the ORB.

Level of Consensus: The CORBA specifications were developed by and adopted for use by the membership of the OMG, including over 500 companies of which 103 vote on final technology adoption. Membership is open to any organization.

Product Availability: At present, there are four implementations which claim compliance with the CORBA 2.0 specification, with 15 more sources committed to implementation. Twenty-two implementations are based on the previous specification.

Completeness: The CORBA specification is a complete definition of the API specification (CORBA IDL) and language mappings that should provide application portability. The IDL and a language mapping are used to develop the client applications and the object implementations. IDL is used as the ORB interface language and is expected to be translated into a specific implementation language depending on the environment. It may be used to specify both APIs and API Classes, i.e., frameworks, for other programming interface specifications.

CORBA interoperability specifies two protocols: the General Inter-ORB Protocol (GIOP) and the DCE Common Inter-ORB Protocol (DCE-CIOP). Support for the GIOP will be mandatory for all implementations. The GIOP specifies protocols that are supported by the TCP/IP protocol suite. The CORBA interoperability specification will permit the inclusion of additional optional protocols beyond the DCE-CIOP.

Language compilers and editors which are not part of CORBA implementations will be used with the CORBA implementation to develop applications and must be acquired separately.

Maturity: The concept of software object technology was developed initially in the late 1960's and remained somewhat dormant until the early 1980's. In recent years, many methodologies and new concepts concerning the development of object systems (i.e., object-oriented and object-based systems) have developed. As of the date of this report's publication, at least 20 different object methodologies and object models were in existence. The CORBA specifications provide a common basic architecture and language for allowing these disparate object technologies to be described and interoperate.

Stability: CORBA and CORBAservices have been balloted and approved by OMG. Additional capabilities will be added within the next 2 to 3 years in the areas of language mappings, security, management, and query services.

Known problems/limitations: CORBA and CORBAservices do not provide security services, management services, or query services. OMG has projects underway in each of these areas. Each application must add these capabilities as needed.

The current CORBA 1.2 implementations provide for distributed application portability, i.e., an application developed using one vendor's implementation will port to another vendor's implementation. Since current CORBA implementations do not as yet support interoperability, they may not support interoperability among different vendor implementations. This means that object systems developed using a particular vendor's current implementation of CORBA may only interoperate with other object systems that are developed using that vendor's implementation.

Conformance testing: No conformance tests exist, although a test service is scheduled to be available through third-parties sometime during 1995. OMG intends to proceed with a full testing and branding certification process.

The CORBA 2.0 specification does not guarantee interoperability. Interoperability is a compliance issue that is separate from the conformance of a particular implementation to the syntax and semantics of the CORBA specification. An experimental test suite has been developed by third parties based on the Assertion Definition Language (ADL) and the Test Environment Toolkit (TET).

Bindings: CORBA includes mappings for C, C++, and Smalltalk.

Future Plans: A language mapping for Ada has been completed but not yet adopted. A mapping for COBOL is under development. In addition, security and management services are under development. A query service is currently in the final stages of development. OMG is investigating specifications to address additional modes of interoperability and document interchange.

Alternative specification: None.

4.14.8 Electronic Messaging API

Specification title: X.400 Based Electronic Messaging Application Program Interface (API) IEEE 1224.1

Specification available from: IEEE Working Group P1224.1

Publication date: March 1993

Sponsoring organization: IEEE

Applicability: X.400 provides electronic mail interoperability among heterogeneous computer systems. X.400 is an international standard protocol definition. The X.400 API defines an interface between the user of a mail system and the mail system. IEEE P1224.1 is a language-independent specification.

Level of consensus: The IEEE standard is proceeding through the ISO fast-track process to become an international standard.

Product availability: Once the standard is complete, numerous products are expected.

Completeness: This specification is a complete detailed level X.400 interface. A high-level interface has not yet been defined. The X.400 API is contained in four documents which are (1) P1224.1—Language Independent Specification; (2) P1326.1—Language Independent Test Methods; (3) P1327.1—C Language Bindings; (4) P1328.1—C Language Test Methods.

Maturity: The principal elements of the X.400 API have been agreed upon for the last 3 years. In time, as the API is fully implemented, the standard will reach a high level of maturity.

Stability: This specification is stable. Tuning modifications can be expected until the final specification is accepted as an IEEE standard.

Known problems/limitations: None.

Conformance testing: Test methods have been defined for measuring the conformance of implementations to this specification.

Bindings: IEEE 1327.1 defines the C language binding.

Future plans: The Electronic Data Interchange (EDI) and X.400 Message Store APIs will be addenda to the X.400 API standard. Additionally, a high-level API may be standardized in the future.

Alternative specification: None.

4.14.9 Directory Services API

Specification title: Directory Services Application Program Interface (API) IEEE 1224.2

Specification available from: IEEE Working Group P1224.2

Publication date: November 1992.

Sponsoring organization: IEEE

Applicability: CCITT X.500, which is an international standard protocol definition, provides Directory Services interoperability among heterogeneous computer systems. The Directory Services Application Program Interface (DS API) defines a standard directory service user agent interface to support application portability at the source-code level. Although the DS API is intended to provide access to CCITT X.500 functionality, its scope is not limited to just X.500, and could be used to access other directory services as well. IEEE P1224.2 is a language-independent specification.

Level of consensus: The IEEE standard is proceeding through the ISO fast-track process to become an international standard.

Product availability: Once the standard is complete, numerous products are expected. P1224.2 (and related specifications) are based on X/Open's XDS specification, which has subsequently been adopted by OSF for inclusion in its Distributed Computing Environment (DCE), and by UNIX International (UI) for inclusion in the UI Atlas environment.

Completeness: This specification is a complete detailed level X.500 interface to directory services. The DS API is contained in four documents which are 1) P1224.2 - Language Independent Specification; 2) P1326.2 -Language Independent Test Methods; 3) P1327.2 - C Language Bindings; and 4) P1328.2 - C Language Test Methods.

Maturity: The principal elements of the DS API have been agreed upon for several years. In time, as the API is fully implemented, the standard will reach a high level of maturity. The DS API is based on X/Open's XDS, which is part of the XPG4 specification.

Stability: No significant changes are foreseen over the next 1 to 2 years.

Known problems/limitations: None.

Conformance testing: Test methods have been defined for measuring the conformance of implementations to this specification.

Bindings: IEEE 1327.2 is the C language binding.

Future plans: Directory services protocol mapping will be included in future versions of GOSIP.

Alternative specification: X/Open Directory Service (XDS).

4.14.10 Network Management

Specification title: Open Management Interoperability Points (OMNI*Point*)

Specification available from: Network Management Forum

Publication date: August, 1992

Sponsoring organization : Network Management Forum

Applicability: The OMNI*Point* program defines a collection of specifications for the management of network and distributed systems using open standards and specifications. The intention of this program is to expand the collection of specifications to embrace new technologies as needed. Future sets will be issued every few years as product cycles mature. The latest OMNI*Point* release is Version 1.0, published in the 3rd quarter of 1993.

Level of consensus: Within the telecommunications industry, the OMNIPoint program is widely accepted and being implemented. In other markets (e.g., LANS), competing technologies (notably the Internet Protocol Suite) are much more prevalent.

Product Availability: Products are available in the telecommunications industry. In other industries, OMNI*Point* products are not as common, but the OMNI*Point* technology is easily adaptable to other industries. Market demand will dictate if OMNI*Point* products are adapted for additional industries.

Completeness: OMNI*Point* is useful in its current release. Additional management information is needed to describe new resources (e.g., ATM switches). In addition, evolving software methodologies such as object-oriented programming (OOP) are causing new techniques (e.g., Common Object Request Broker Architecture - CORBA) to be strongly considered for future OMNI*Point* versions.

Maturity: The current OMNI*Point* release is close to the state-of-the-art and will be revised as the state-of-the-art advances.

Stability: The OMNI*Point* specification will be revised as technology advances and products mature, but it is a goal of the Network Management Forum to keep new releases upwardly compatible with older releases.

Known problems/limitations: Coexistence and convergence between OSI and Internet Protocol Stack technologies remains an issue, although some solutions have been proposed and implemented.

Conformance testing: Conformance tests were developed for early Network Management (NM) Forum specifications, but proved to be very expensive to develop. They were not comprehensive tests of the products and ultimately were not popular. Consequently, no conformance testing exists nor is planned.

Future plans: OMNI*Point* releases are tied to product cycles. As products develop, consideration will be given to high priority functionality to be added to the specification.

Alternative specifications: None

4.14.11 Network Information Locator

Specification title: FIPS 192 Government Information Locator Service (GILS)

Specification available from: NTIS

Publication date: December 7, 1994

Sponsoring organization: United States Department of the Interior, U.S. Geological Survey

Applicability: This standard is recommended for use by Federal agencies in the development and establishment of information locators, i.e., information resources that identify other information resources, describe the information available in those resources, and provide assistance in how to obtain the information. It establishes a structure for organizing network information about information sources available within Federal agencies.

Level of consensus: This FIPS adopts the specification of an Application Profile for the Government Information Locator Service as agreed to by the Open Systems Environment Implementors Workshop (OIW), Special Interest Group on Library Applications. It is based on ANSI/NISO Z39.50 Information Retrieval Service and Protocol.

Product availability: Products compliant with FIPS 192 are available from multiple vendors.

Completeness: The Application Profile is considered a complete specification of the application level functions required to achieve interoperability among separate implementations of network-based information locator systems.

Maturity: The GILS specification is derived from common capabilities of existing public and private implementations of similar products that are in current use. The standard becomes effective June 30, 1995.

Stability: In May 1994, a Stable Implementors Agreement concerning the Application Profile for the Government Information Locator Service was approved by the Open Systems Environment Implementors Workshop, Special Interest Group on Library Applications. Capabilities will be added as warranted. No outstanding major changes are foreseen for the next 2 years.

Known problems/limitations: The Stable Implementors Agreement is expected to undergo planned periodic revisions for correction and clarification and to specify some additional optional elements. In certain cases, FIPS specifications make specific optional elements and parameters of the adopted agreement mandatory for use within defined domains.

Conformance testing: Testing for conformance to this standard is at the discretion of the agency. Agencies may select the tests to be administered and the testing organizations that administer the tests. The U.S. Government currently has no plans to issue a test suite or provide testing services.

Future plans: Unknown at this time.

Alternative specifications: None.

4.14.12 Distributed Information Service

Specification title: ANSI/NISO Z39.50 Information Retrieval Service and Protocol

Specification available from: NISO

Publication date: July 1992

Sponsoring organization: ANSI/NISO

Applicability: This is an OSI application layer service definition and protocol that specifies the procedures and structures for the intersystem submission of a search request, responses to the request, access control, and resource control. The protocol addresses communication between corresponding information retrieval applications on the origin and target systems; it does not address interaction between the origin computer and user. This standard is intended particularly for use in facilitating access to network-based information sources by an uninitiated clientele. The standard will be used to implement publicly accessible locators to Federal data and information, including data system inventories, data directories, information catalogs, bulletin boards, and published CD-ROM titles, among other information products.

Level of consensus: This is an approved ANSI/NISO standard that is aligned with ISO 10162/10163, the Search and Retrieve Service Definition and Protocol Specification.

Product availability: Products implementing the 1992 version are available utilizing full OSI telecommunications protocols as well as TCP/IP. Also expected are implementations using other protocols and interprocess implementations without external telecommunications.

Completeness: This specification describes the protocol and provides the ASN.1 syntax. A reference implementation of the 1992 version is being placed in the public domain under Federal government funding by the Clearinghouse for Networked Information Discovery and Retrieval (CNIDR).

Maturity: The current specification has been available for 1 year.

Stability: This specification is stable. New versions of the standard are expected to be fully compatible enhancements.

Known problems/limitations: The generality of the protocol is intended to allow accommodation of new services as they are required.

Conformance testing: Conformance tests for Z39.50 are conducted in the Z39.50 Implementation Testbed organized by the Z39.50 Implementors Group that serves as an advisory body to the Z39.50 Maintenance Agency. CNIDR is responsible for the reference implementation in the public domain expected to be widely used for Federal locator applications.

Future plans: Some services being considered in the next version of Z39.50 are:

a) "Explain" - to allow an origin to obtain details of the target implementation;
b) "Define Element Set" - to allow an origin to define and name a set of elements to compose a retrieval record;
c) "Scan" - to allow an origin to obtain a list of access point values from a database index;
d) "Object Access" - to allow an origin to perform operations including create, delete, sort, export, activate, and permit, on various objects, including result sets and queries; and
e) "Segmentation" - to allow a target to return multiple responses to a single presentation request

Alternative specifications: None.

4.14.13 Data Encryption

Specification title: FIPS 46-2 Data Encryption Standard (DES)

Specification available from: NTIS

Publication date: December 30, 1993

Sponsoring organization: NIST

Applicability: The DES specifies an algorithm which is used to encrypt and decrypt sensitive data, to provide for its confidentiality. It is to be used by Federal departments and agencies when 1) an authorized official or manager responsible for data security or the security of any computer system decides that cryptographic protection is required, and 2) the data is not classified according to the National Security Act of 1947, as amended, or the Atomic Energy Act of 1954, as amended.

Level of consensus: This FIPS, originally established as FIPS 46 in July 1977, was later adopted as a national standard (ANSI X3.92-1981).

Product availability: Numerous products implementing the DES in hardware, firmware, and software have been developed by a large number of vendors. NIST has currently validated over eighty products from more than 55 vendors.

Completeness: The DES defines an algorithm that can be used to encrypt and decrypt electronic information. This FIPS specification allows for the algorithm to be implemented in hardware, firmware, software, or any combination thereof. FIPS 81, DES Modes of Operation (December 1980), defines four modes of operation for the DES which may be used in a wide variety of applications. An approved method for maintaining cryptographic keys used by the DES algorithm is described in FIPS 171, ANSI X9.17 Key Management (Wholesale). Cryptographic modules which implement this standard must conform to the requirements of FIPS 140-1, Security Requirements for Cryptographic Modules.

Maturity: The DES has been a U.S. Government standard for data encryption (for unclassified but sensitive material) since 1977, and a national (ANSI) standard since 1981. No successful attacks on the cryptographic algorithm specified by the standard have been documented.

Stability: In 1998, the FIPS will be considered for reaffirmation. Before that time, no foreseeable changes will take place with the Data Encryption Standard, although NIST may begin to consider alternatives to the DES.

Known problems/limitations: Cryptographic devices and technical data regarding them are subject to Federal export controls. Some exports of cryptographic modules implementing this standard and technical data regarding them must comply with these Federal regulations and must be licensed by the U.S. Department of State. Other exports of cryptographic modules implementing this standard and technical data regarding them fall under the licensing authority of the Bureau of Export Administration, U.S. Department of Commerce.

Conformance testing: NIST currently provides a validation program, which consists of a Monte Carlo test to determine the correctness of the implementation of the DES algorithm. In the future, laboratories that perform FIPS 140-1 validation testing will be responsible for running the DES validation program.

Future plans: At the next review in 1998, the algorithm specified will be over twenty years old. NIST will consider alternatives which offer a higher level of security. One of these alternatives may be proposed as a replacement standard at the 1998 review. The development of any new algorithm should allow for a gradual transition from the DES.

Alternative specifications: Algorithms other than the one specified in FIPS 46-2 may be used for data encryption, provided that these algorithms are approved for government use in a FIPS.

4.14.14 Digital Signatures

Specification title: FIPS 186 Digital Signature Standard (DSS)

Specification available from: NTIS

Publication date: May 19, 1994

Sponsoring organization: NIST

Applicability: The DSS is used in designing and implementing public-key based digital signature systems which Federal departments and agencies operate or which are operated for them under contract. The Digital Signature Algorithm (DSA) specified in the DSS authenticates the integrity of the signed data and the identity of the signatory. A third party may use the DSA to determine that data was actually signed by the generator of the signature (non-repudiation). The DSA is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications which require data integrity assurance and data origin authentication.

Level of consensus: The algorithm specified in the DSS is in the process of being adopted as both a national standard (Draft ANSI X9.30-199x Part 1) and an international standard (Project 1.27.08 "Digital Signature with Appendix," being developed by ISO/IEC JTC1/SC27/WG2).

Product availability: Currently there are relatively few implementations of the DSS, due to the recent adoption of the standard (effective December 1, 1994). However it is anticipated that many more vendors will be implementing the standard as the number of applications requiring authentication and data integrity increases.

Completeness: The DSS is complete in that it defines both the algorithm for generating and verifying digital signatures, and the generation of other values which are used by the DSA.

Maturity: Public key cryptography, which serves as the basis for digital signature technology, has been in use for almost 20 years. The standard itself underwent two comment periods over the span of 3 years before it was adopted. Numerous Federal agencies are currently considering implementing the DSS to improve efficiency and reduce paperwork.

Stability: At this time, there are no plans to modify this standard. However, the Secure Hash Algorithm (SHA, FIPS 180) that is used in the DSS was updated on March 14, 1995, and is now FIPS 180-1 (SHA-1). It is a slightly modified version of the SHA that provides greater security, but the two algorithms are not interoperable. This means that implementations of the DSS using SHA and SHA-1 are not interoperable. For those entities that have implemented the SHA, there is a period of six months following the approval of FIPS 180-1 during which a changeover may be made to implementing the SHA-1.

Known problems/limitations: Implementation of the DSS will assure proper authentication as long as the secrecy of users' private keys is maintained. The overall implementation should provide an acceptable level of security, but conformance to the DSS alone does not assure this.

Conformance testing: NIST is developing a validation program to test implementations for conformance to the DSS.

Future plans: The DSS will be reviewed every 5 years to assess its adequacy.

Alternative specifications: None.

5. STRATEGIC EVALUATIONS

As part of the evaluation of APP specifications, users should take into account the strategic value of each specification. Table 1 summarizes NIST's views on the strategic value of each specification recommended in this report.

The valuations are made according to the following guidelines:

a) Strategic now (STR)—In selecting these specifications, users would be reasonably safe in making substantial investment and long-term plans covering mission-critical systems and the infrastructure needed to support them. Changes are expected to be upwardly compatible.

b) Strategic in the future (FTR)—Specifications that are subject to change but appear to be headed for standardization fall into this category. Existing standards that may be subject to changes that are not entirely upwardly compatible also fall into this category. There are some long-term risks involved, but the actions of the consensus-building process will tend to minimize them. Users should select these specifications where strategic specifications are unavailable and an investment must be made, but should plan for possible evolution in the future.

c) Nonstrategic (GAP)—These specifications are stop-gap measures recommended with the warning that any user investment will be at significant risk. They are not appropriate for long-term planning. Users should, for these reasons, minimize their risk by minimizing investment.

Subsequent versions of this report may incorporate this dimension of evaluation in the overall evaluation criteria.

Table 1. Strategic Value of APP Specifications

OSE SERVICE AREA / Applicable Specifications	STR	FTR	GAP
OPERATING SYSTEM SERVICES			
FIPS 151-2 Portable Operating System Interface (POSIX)—System Application Program Interface [C Language]	●		
FIPS 189 Portable Operating System Interface (POSIX)—Part 2: Shell and Utilities	●		
Portable Operating System Interface (POSIX) Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension [C Language] IEEE 1003.1b-1993		●	
POSIX—Security Extensions IEEE 1003.1e	●		
POSIX—Security Extensions IEEE 1003.2c	●		
Standard for Information Technology - Portable Operating System Interface (POSIX) System Administration - Part 2: Software Administration IEEE P1387.2, Part 3: User and Group Account Management IEEE P1387.3, Part 4: Printing Interfaces IEEE P1387.4		●	
HUMAN/COMPUTER INTERFACE SERVICES			
FIPS 158-1 User Interface Component of Applications Portability Profile	●		
Standard for Information Technology—X Window System Graphical User Interface—Part 1: Modular Toolkit Environment (IEEE 1295)	●		
SOFTWARE ENGINEERING SERVICES			
FIPS 119-1 Ada	●		
FIPS 160 C	●		
FIPS 21-4 COBOL	●		
FIPS 69-1 Fortran	●		
Portable Common Tool Environment (PCTE) Application Programmer's Interface ISO/IEC 13719-1	●		
DATA MANAGEMENT SERVICES			
FIPS 127-2 Database Language SQL	●		
FIPS 156 Information Resource Dictionary System (IRDS)	●		
Remote Database Access (RDA) ISO/IEC 9579:1993	●		
FIPS 193 SQL Environments	●		
DATA INTERCHANGE SERVICES			
FIPS 152 Standard Generalized Markup Language (SGML)	●		
PDDF			●
Electronic Manuscript Preparation and Markup (EMPM) ANSI/NISO Z39.59-1988		●	
Standard Data Elements ISO 11179, Parts 3, 4, and 5		●	
FIPS 128-1 Computer Graphics Metafile (CGM)	●		
FIPS 194 Raster	●		

OSE SERVICE AREA / Applicable Specifications	STR	FTR	GAP
JPEG ISO 10918	●		
MPEG ISO 11172	●		
FIPS 177 Initial Graphic Exchange Specification (IGES)	●		
Standard for the Exchange of Product Model Data (STEP) ISO 10303	●		
FIPS 161-1 Electronic Data Interchange (EDI)	●		
FIPS 173-1 Spatial Data Transfer Specification (SDTS)	●		
GRAPHICS SERVICES			
FIPS 120-1 Graphical Kernel System (GKS)	●		
FIPS 153-1 Programmer's Hierarchical Interactive Graphics System (PHIGS)	●		
NETWORK SERVICES			
IEEE P1003.1g Protocol-independent Interfaces		●	
IEEE P1238 OSI ACSE API		●	
FIPS 146-2 POSIT		●	
ISDN ASI		●	
FIPS 182 ISDN Protocols	●		
OSF DCE Remote Procedure Call			●
Common Object Request Broker Architecture (CORBA), CORBAservices			●
IEEE 1224.1 X.400 Electronic Messaging API		●	
IEEE 1224.2 X.500 Directory Services API		●	
FIPS 192 GILS	●		
NISO Z39.50	●		
FIPS 46-2 DES	●		
FIPS 186 DSS	●		

6. CONCLUSION

The long-term goal of the program on which this report is based is the establishment of an open system environment for use in Federal information systems support. In this open system environment, interoperability, portability, and scalability must be the driving forces for the development of standard interfaces, services, protocols, and formats. Eventually, users would like to see all of the OSE specifications take the form of international standards. In the interim, NIST has reviewed many of the specifications that are now available and has made recommendations on those that are believed to have a higher probability of becoming successful additions to the suite of OSE specifications.

The short term goals of Federal information requirements demand action now. In response to these goals, NIST has developed a suite of recommended specifications that can be used in system development and acquisition. Many of these specifications are Federal standards, and others are national or international standards. These specifications are relatively stable and can be used with little risk.

There is, however, a measure of risk involved in using nonstrategic specifications, such as standards work-in-progress with its inherent risk of change, and those based on non-open specifications. The risk associated with these specifications is based on the premise that the Federal user has virtually no control in the direction that these specifications may take.

The tradeoffs amount to accepting less portability and interoperability in return for meeting current information requirements, and not waiting until all open system specifications have become available. No clearly right or wrong decisions will be made in selecting specifications. Some decisions will be more right than others. Users can only hope with today's technology to ameliorate the effects of long-term changes. NIST will continue to perform evaluations and publish its recommendations. *Users must decide for themselves what is best for them.*

ANNEX A — DOCUMENT SOURCES: CONTACT INFORMATION

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 addressees.

AAP
Association of American Publishers
EPSIG (Electronic Publishing Special Interest Group)
c/o OCLC
6565 Frantz Road
Dublin, OH 43017-0702
Phone: (614) 764-6000

ANSI
American National Standards Institute
11 West 42d Street, 13th Floor
New York, NY 10036
Phone: (212) 642-4900

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

CCITT (renamed ITU-T)
International Telegraph and Telephone Consultative Committee
Place des Nations
CH-1211 Geneva 20
Switzerland

COSMIC
Computer Software Management and Information Center
The University of Georgia
382 East Broad Street
Athens, GA 30602
Phone: (706) 542-3265
FAX: (706) 542-4807

Department of Defense
Defense Printing Service
Standardization Documents Order Desk
700 Robbins Avenue
Building 4-D
Philadelphia, PA 19111-5094
Phone: (215) 697-1187 or (215) 697-2179
Any Federal organization or DoD contractor can order numerous types of standards, including FIPSes 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)
U.S. Department of Commerce
National Technical Information Service (NTIS)
5285 Port Royal
Springfield, VA 22161
Phone: (703) 487-4650
FAX: (703) 321-8547
NIST publishes an index of FIPS that is available through NTIS. Request "NIST Publications List 58."

GCA
Graphic Communications Association
199 Daingerfield Road
Alexandria, VA 22314-2888
Phone: (703) 519-8160
FAX: (703) 548-2867

GPO
Government Printing Office
Superintendent of Documents
U. S. Government Printing Office
Washington, DC 20402
Phone: (202) 512-1800

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: (800) 678-IEEE or (800) 678-4333

IEEE (for draft standards)
1730 Massachusetts Avenue, NW
Washington, DC 20036-1903
Phone: (202) 371-0101

IETF
Internet Engineering Task Force
IETF Secretariat
c/o Corporation for National Research Initiatives
1895 Preston White Drive, Suite 100
Reston, VA 22091
Phone: (703) 620-8990
FAX: (703) 620-0913
Internet: ietf-secretariat@cnri.reston.va.us
WWW: http://www.ietf.cnri.reston.va.us/home.htm

ISO
International Organization for Standardization
Central Secretariat
1 Rue de Varembe
P. O. Box 56
CH-1211 Geneva 20
Switzerland
Phone: 011-41-22-34-12-40

ISOC
Internet Society
12020 Sunrise Valley Drive, Suite 270
Reston, VA 22091
Phone: (703) 648-6888
FAX: (703) 648-9887 or (800) 468-9707 (USA only)
E-mail: isoc@isoc.org

ITU-T (formerly CCITT)
International Telecommunication Union—Telecommunications Standardization Sector
Place des Nations
CH-1211 Geneva 20
Switzerland

JTC1 TAG
Joint Technical Committee 1 Technical Advisory Group
Information Technology Industry Council (ITI)
Director, JTC1 TAG 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

National Computer Graphics Association
2722 Merrilee Drive, Suite 200
Fairfax, VA 22031
Phone: (703) 698-9600

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

National IGES Users Group (NIUG)
c/o NCGA, Suite 200
2722 Merrilee Drive
Fairfax, VA 22031-4499
Phone: (703) 698-9606 x330
E-mail: jzink@uspro.fairfax.va.us
FAX: (703) 560-2752

National Institute of Standards and Technology (NIST)
Computer Systems Laboratory (CSL)
ATTN: APP Guide
Building 225, Room B266
Gaithersburg, MD 20899
Phone: (301) 975-2821
FAX: (301) 926-3696
WWW: http://nemo.ncsl.nist.gov/

National Technical Information Service (NTIS)
U.S. Department of Commerce
5285 Port Royal
Springfield, VA 22161
Phone: (703) 487-4650
FAX: (703) 321-8547

Network Management Forum
1201 Mt. Kemble Avenue
Morristown, NJ 07960-6628

Object Management Group (OMG)
492 Old Connecticut Path
Framingham, MA 01701
Phone: (508) 820-4300
FAX: (508) 820-4303

OSF
Open Software Foundation
11 Cambridge Center
Cambridge, MA 02142

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, NW, Suite 500
Washington, DC 20005
Phone: (202) 434-8845
FAX: (202) 393-5453

UniForum
2901 Tasman Drive, #201
Santa Clara, CA 95054
Phone: (800) 255-5620 or (408) 986-8840
FAX: (408) 986-1645

U.S. Product Data Association (US PRO)
c/o NCGA, Suite 200
2722 Merrilee Drive
Fairfax, VA 22031-4499
Phone: (703) 698-9606 x308
FAX: (703) 560-2752
E-mail: uspro@uspro.fairfax.va.us

X3
American Standards Committee X3 -- Information Technology
Information Technology Industry Council (ITI)
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

X/OPEN — X/OPEN Portability Guide (XPG)
1750 Montgomery Street
San Francisco, CA 94111
Phone: (415) 323-7992

ANNEX B — BIBLIOGRAPHY

A Guide for Acquiring Integration Services, Acquisition of Information Resources, U.S. General Services Administration, Information Resources Management Service, Division KMPP, Washington, DC, November 1991, pp. 125.

Model RFP -- Request for Proposals, Federal Computer Acquisition Center (FEDCAC), Boston, MA, as of 17 April 1992, pp. 300+.

An Analysis of Application Environments, Emerging Technologies Group, Inc., Dix Hills, NY, 1989, pp. 494.

Guide on Open System Environment (OSE) Procurements, NIST Special Publication 500-220, Computer Systems Laboratory (CSL), October 1994, pp. 147.

Guide to the POSIX Open Systems Environment -- Draft 18, IEEE 1003.0, February 1995.

Model RFP -- Request for Proposals, Department of the Air Force, Air Force Computer Acquisition Center (AFCAC), Hanscom Air Force Base, Massachusetts, as of 14 August 1991, pp. 500+. (The major part of AFCAC has been absorbed by the General Services Administration's Federal Computer Acquisition Center [FEDCAC].)

Strategies for Open Systems — Stage Two — The Experience With Open Systems, DMR Group, Inc., Boston, 1990, pp. 196.

Validated Products List (VPL) Volume 1 1995 No. 2, NISTIR 5629 (Supersedes NISTIR 5585), Computer Systems Laboratory (CSL), April 1995. (Note: This publication is updated several times per year. Each new edition replaces the previous edition and is identified by a new NISTIR number.)

INDEX

Abstract Syntax Notation One 3
Ada . . . . . v, 3, 14, 20, 23, 33, 34, 38, 40, 41, 63, 64, 75, 84
American National Standards Institute 3, 34, 87
ANSI Standard X3.124-1985 63
ANSI Standard X3.135-1992 40
ANSI Standard X3.138-1988 41
ANSI Standard X3.185-1992 42
ANSI Standard X3.23-1985 35
ANSI Standard X3.9-1978 36
ANSI/ISO 8632:1992 50
ANSI/NISO Z39.59 . . . . . 45, 48, 84
API . . . . . v, 3, 10, 13, 16, 20, 22, 23, 25, 26, 29, 31, 32, 65-67, 69, 72, 74-76, 84, 85
Application Portability Profile . . . . . 1, 3, iii, 2, 3, 10
application program interface 3, 5, 9, 10, 22, 23, 25, 31, 42, 75, 76, 84
application software interface 3, 69
architecture 3, 30, 38, 43, 48, 51, 70-72, 74, 77, 85
assertions 15, 24, 26, 27, 41, 67
authentication 17, 61, 72, 82
Basic Call Control 71
Basic Rate Interface 3, 70
Bitmap Distribution Format 30
BSD Socket interface 66
CAD/CAM 3, 57, 58
CALS 46, 47, 51, 58, 59
CASE . . . . . iii, 3, 13, 19, 42, 48, 54, 56
CCITT 3, 4, 61, 76, 87, 90
Certificates of validation 23, 41, 51
CGM 3, 45, 50, 51, 53, 84
client-server architecture 30, 43
client-server operations 13
COBOL . . . . . v, 3, 14, 33, 35, 36, 40, 41, 75, 84
commands and utilities 13, 22-24
Common Object Request Broker Architecture 3, 38, 72, 77, 85
Computer Graphics Metafile 3, 50, 84
Computer Systems Laboratory . . . . . 3, vi, 3, 90, 93
computer-aided design and manufacturing 3, 57
Computer-Aided Software Engineering 3
contact information 87
CORBA . . . . . v, 3, 39, 65, 72-75, 77, 85
Corporation for Open Systems 3
COS 3
CSL . . . . . vi, 2, 3, 17, 20, 21, 23, 38, 42, 46, 47, 90, 93
DAC 3, 40
data communication 16
data dictionary/directory 15, 39, 41

data element specification 49
data format 12, 16
data interchange . . . . . iv, v, 4, 8, 11, 15, 16, 20, 45, 49, 50, 57, 59-62, 76, 82, 84, 85, 88
data management . . . . . v, 11, 12, 15, 39, 41, 42, 84
Database Language SQL 39, 84
DCE 3, 65, 71, 74, 76, 85
directory services 15, 41, 76, 77, 85
distributed data services 15
document sources 87
ECMA PCTE v
EDIFACT 4, 49, 60, 61
EEI 4, 10
Electronic Data Interchange 4, 49, 60, 76, 82, 85
Electronic Manuscript Preparation and Markup 4, 46, 48, 84
EMPM 4, 45, 46, 48, 49, 84
European Computer Manufacturers Association 3, 88
evaluation criteria . . . . . iv, 2, 18, 40, 83
External Environment Interface 4, 9, 10
FDDI 4
Federal Information Processing Standard 4, 22
Fiber Distributed Data Interface 4
FORTRAN 14, 20, 33, 36, 37, 40, 41, 63, 64, 84
framework . . . . . iii, iv, 8, 12, 37, 38, 46, 49
FTAM v
Geographic Information System 4, 62
GIS 4, 62
GKS 4, 20, 62-64, 85
GNMP v
GOSIP . . . . . v, 4, 68, 77
Government Open System Interconnection Profile 4
Graphical Kernel System 4, 20, 62-64, 85
Graphical User Interface 4, 13, 29-32, 84
Graphics Services . . . . . v, 11, 16, 62, 85
GUI 4, 31, 32
HCI 4, 11, 13
human/computer interface . . . . . v, 4, 7, 10-14, 29, 30, 84
IEEE P1201.2 31
IEEE P1238 . . . . . 67, 85
IGES/PDES Organization (IPO) 57
IGOSS 4, 68
Industry/Government Open Systems Specification 4, 68
information interchange 10
Initial Graphics Exchange Specification 4, 57
Institute of Electrical and Electronics Engineers . . . . . iii, iv, 4, 8, 22, 89
Integrated Services Digital Network 4, 20, 69, 70
integrated software engineering environment 4, 37, 38
Inter-Client Communications Conventions Manual 4

International Organization for Standardization ..... iii, 4, 34, 68, 89
Internet Protocol 68, 77, 78
interoperability ..... iii, 1, 4, 7, 8, 10, 16, 17, 28, 37, 40, 41, 43, 58, 68, 73-78, 86
IRDS 4, 39, 41, 42, 84
ISDN ..... v, 4, 5, 65, 69-71, 85
ISEE ..... v, 3, 4, 14, 33, 37, 38
ISO 10180 v
ISO 10303 ..... v, 45, 59, 60, 85
ISO 11179 ..... v, 45, 49, 50, 84
ISO 1539:1980 36
ISO Standard 7942:1985 63
ISO Standard 9592:1988 64
ISO TC184/SC4 59
ISO/IEC 9579:1993 ..... 42, 84
ISO/IEC JTC1 ..... 37, 42, 46, 48, 50, 52, 82
ISO/IEC Standard 9075:1992 40
kernel operations 12, 22, 23, 26
MAC 4, 40
Mandatory Access Control 4, 40
Manufacturing Automation Protocol/Technical and Office Protocols 4
MAP/TOP 4
MIT X Window System 30
multimedia specifications 13
National Bureau of Standards 5, 58
National Computer Security Center 5, 26, 27, 40, 90
National IGES Users Group 90
National Technical Information Service 5, 21, 22, 88, 91
National Voluntary Laboratory Accreditation Program 5, 21, 31
NIU-Forum 5
NIUG 58, 90
NTIS 5, 21-23, 30, 33-36, 39, 41, 44, 46, 50, 51, 57, 60, 63, 64, 68, 78, 80, 82, 88, 91
NVLAP 5, 21, 31
Object Management Group 5, 38, 73, 91
object-oriented 35, 36, 38, 42, 72, 74, 77
ODA/ODIF v
ODL v
OIW 5, 20, 43, 52, 68, 78
OMG 5, 39, 73-75, 91
OMNIPoint ..... v, 65, 77, 78
open system environment ..... 1, 3, iii, iv, vi, 1, 2, 5, 7, 9, 20, 43, 86, 93
OSE Implementor's Workshop 5
OSE Profile ..... iii, 10
OSE Reference Model 2, 8-10
Pascal ..... v, 34, 40, 41, 63, 64
PDDF ..... v, 5, 45, 47, 48, 84
PDES 5, 57, 59
Persistent SQL Modules 41

personal/micro computer support 17
PHIGS . . . . . v, 5, 62-64, 85
portability . . . . . 1, 3, iii, 1-3, 7, 8, 10, 28, 30, 38, 74, 76, 84, 86, 92
Portable Common Tools Environment 5
Portable Document Delivery Format . . . . . v, 5, 47
POSIX.1 28
POSIX.2 . . . . . 24, 28
Primary Rate Interface 5, 70
Product Data Exchange using STEP 5, 59
Programmer's Hierarchical Interactive Graphics System 5, 62, 64, 85
Project Athena 30
protocol 4, 5, 12, 16, 25, 30, 31, 43, 56, 58, 60, 65, 66, 68-70, 74-80, 85
Protocol Independent Interfaces 5, 65
rationale 19, 37, 68, 72, 73
RDA 5, 39-44, 84
realtime extension 13, 22, 25, 84
Remote Database Access 5, 40-42, 84
remote procedure call services 17
routing 4
scalability . . . . . iii, 1, 7, 8, 86
SDTS . . . . . v, 5, 45, 61, 62, 85
security . . . . . iv, v, 1, 5, 12-18, 20, 22-27, 39, 40, 69, 72, 74, 75, 80-82, 84, 90
security services 12-17, 74
SGML 5, 45-49, 54, 56-58, 84
Simple Network Interface 5, 66
SNI 5, 66
Spatial Data Transfer Specification 5, 85
Spatial Data Transfer Standard 61
SPDL . . . . . v, 5
SQL . . . . . v, 5, 34, 39-41, 43-45, 84, 91
SQL Call Level Interface 41
SQL/CLI 41
SQL3 41
Standard for the Exchange of Product Model Data 5, 59, 85
Standard Generalized Markup Language 5, 46, 84
Standards Committee X3 . . . . . 6, 92
Standards Committee X3H2 39
Standards Committee X3H3 . . . . . 50, 63, 64
Standards Committee X3H4 . . . . . 39, 41
Standards Committee X3J11 . . . . . 34, 35
Standards Committee X3J3 36
Standards Committee X3J4 35
STEP . . . . . v, 5, 45, 59, 60, 85
Structured Query Language 5
system management 12, 13, 22, 28
TCP/IP 68, 74, 79
test suite 21, 23, 26, 27, 34, 38, 41, 43, 44, 63, 64, 75, 79

testing laboratories 23
TFA . . . . . v, 6, 25
Transparent File Access 6, 16, 25, 65
triggers 41
Trusted Database Management System 40
United Nations Working Party UN/ECE/WP.4 60
US PRO 57, 58, 92
User Interface Component 30, 84
Validated Products List 6, 21, 23, 34-37, 40, 42, 93
VPL 6, 21, 23, 34-37, 51, 63, 93
Window management 13
X Window System . . . . . v, 29-32, 84
X/Open Transport Interface 6, 66, 67
X12 . . . . . 60, 61, 88
Xlib 30, 31
XPG4 . . . . . 66, 76
Xt Intrinsics 31
Y14.26-1989 58

*U.S. G.P.O.:1996-404-525:57904

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SYSTEMS TECHNOLOGY

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 500–.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bimonthly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program in support of the efforts of private-sector standardizing organizations.

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards
and Technology
Gaithersburg, MD 20899–0001