NIST Special Publication 500–220

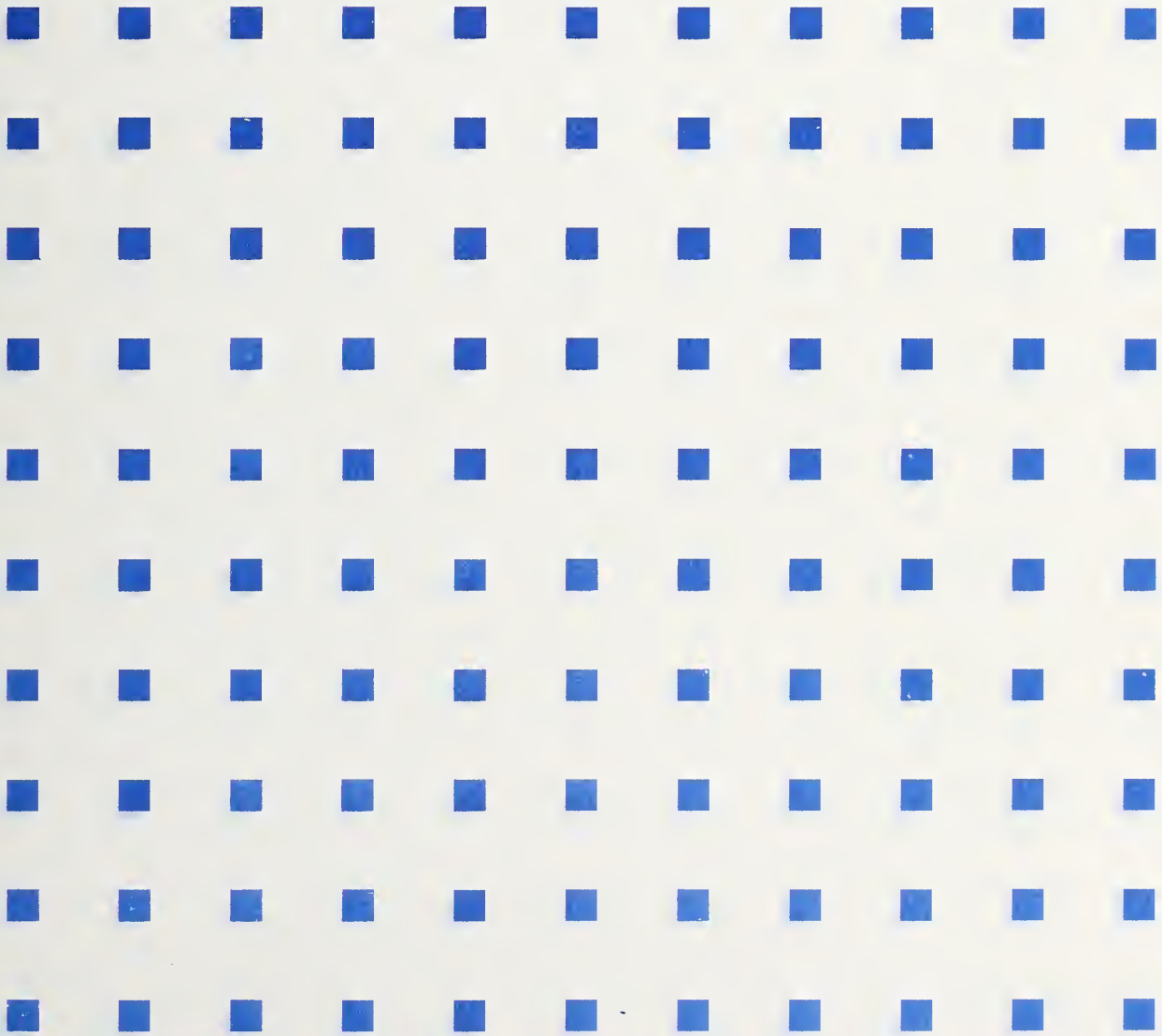
Computer Systems Technology

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

NIST

Guide on Open System Environment (OSE) Procurements

Gary E. Fisher



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 performs 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.

Technology Services
- Manufacturing Technology Centers Program
- Standards Services
- Technology Commercialization
- Measurement Services
- Technology Evaluation and Assessment
- Information Services

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

Chemical Science and Technology Laboratory
- Biotechnology
- Chemical Engineering[1]
- Chemical Kinetics and Thermodynamics
- Inorganic Analytical Research
- Organic Analytical 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
- Robot Systems
- Factory Automation
- Fabrication Technology

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

Building and Fire Research Laboratory
- Structures
- Building Materials
- Building Environment
- Fire Science and Engineering
- Fire Measurement and Research

Computer Systems Laboratory
- 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[2]
- Computer Systems and Communications[2]
- Information Systems

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

NIST Special Publication 500–220

Guide on Open System Environment (OSE) Procurements

Gary E. Fisher

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

October 1994

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 500-220
Natl. Inst. Stand. Technol. Spec. Publ. 500-220, 153 pages (Oct. 1994)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1994

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

EXECUTIVE SUMMARY

The guidance in this report pertains to U.S. Government acquisition of Open System Environment (OSE) infrastructure including operating system, human/computer interface, software engineering, data management, data interchange, graphics, network, security, and system/network management services based on implementations of standard application program interfaces, programming languages, data formats, and protocols. Other organizations, such as state and local governments, academic, and private institutions also may find the information helpful in defining computing environments that promote application portability, interoperability, and scalability.

The procurement of information technology that provides an OSE can be complex and difficult to manage. Much can be learned from procurement actions that have been instituted for acquiring the technology to support an OSE. This report provides a source of such information.

An Open System Environment encompasses the functionality needed to provide interoperability, portability, and scalability of computerized applications across networks of heterogeneous, multi-vendor 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.

The Open System Environment concept has become ubiquitous throughout both the public and private sectors. Federal agencies are finding that open systems provide a more flexible, cost-effective, and beneficial environment for supporting mission-critical applications than previous infrastructures based on proprietary technology. They are also finding that the initial move to open systems can be expensive and difficult to manage if not planned carefully.

There are many acquisition strategies possible when implementing an OSE. The implementation of OSEs will most likely be accomplished in a series or combination of acquisitions. The planning and design of the OSE may be a single procurement where engineering services and information systems are purchased under the same contract through an integrator. This strategy has risks associated with it. If the acquisition is delayed, then the implementation will be delayed. Another acquisition strategy may involve a series of separate acquisitions where the agency may perform the integration or establish a contract for integration services.

Agencies have requested assistance from the Computer Systems Laboratory (CSL) in an effort to control the evolution of open systems and provide guidance on managing the transition from current environments to the OSE. In the process of implementing open systems, agencies have found that significant up-front planning and current knowledge of technology are necessary to remain flexible and to take advantage of targets of opportunity as they arise. Many lessons-learned in OSE acquisition programs that agencies have undertaken are included in this report. This

information is meant to assist program managers and senior project engineers in acquiring an OSE on which to build flexible, modular systems and applications.

LIMITATIONS OF THIS GUIDE

This report can go only so far in describing what is needed to specify an OSE. It does not identify within a particular OSE service area where there are gaps and overlaps between standards. Therefore, a comprehensive OSE cannot be achieved solely by the specifications and standards used in this guide. Applications are normally not standard from the mere fact that each organization will have requirements that are different from every other organization's requirements. Because of these differences and the lack of standards to cover every conceivable combination of requirements, organizations must be prepared to complete the specification of the OSE with information from other sources.

ACKNOWLEDGMENT

Numerous individuals and organizations have provided significant information or effort to help create this document. Foremost among them are Jean Lakey of the U.S. Army's Sustaining Base Automation (SBA) Program, Patrick Plunkett of the U.S. General Services Administration (GSA), William Bushman of the U.S. Army's SBA Technical Management Division (TMD), and Martha Gray of the National Institute of Standards and Technology.

The mention of specification names in certain instances should not be interpreted to mean that the National Institute of Standards and Technology (NIST) nor the Computer Systems Laboratory (CSL) endorses the acquisition of any specific products based on these specifications. NIST has endeavored to separate references to the specifications from products and services, and has provided guidance, where applicable, to enable users to make their own judgments of the applicability of the recommended specifications to their requirements. For specific individual and organizational requirements, other specifications not mentioned here may be more applicable.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

HOW TO USE THIS REPORT

This "Guide on Open System Environment (OSE) Procurements" provides information on developing an organizational Open System Environment through the Federal procurement process. It contains a rudimentary decision model for organizing and preparing for the implementation of an OSE. The information presented in this report is not based on any specific requirements or development methodology and does not recommend a methodology for deriving requirements. It starts with the assumption that the organization has performed an analysis to determine requirements and has derived a detailed list of functional specifications. These requirements and specifications are the basis of all follow-on actions in establishing the OSE.

The Guide also assumes that the establishment of the OSE is a major undertaking for the organization, that there will be few other programs that will have as large an effect on the organization. By definition, OSE produces a standards-based environment for heterogeneous, distributed systems. By virtue of the size of such a program, a plan and process for carrying out the establishment of an OSE are necessary. An outline of the process for acquiring the technology to support an OSE is described in the following:

1. Functional requirements and specifications are broadly classed into one or more of several OSE service areas. Each of the service areas is described and related to the other service areas in NIST Special Publication 500-210, "Application Portability Profile" (i.e., the APP Guide). These service areas are—

    a. operating system services;
    b. human/computer interface services;
    c. data management services;
    d. data interchange services;
    e. software engineering services;
    f. graphics services;
    g. network services;
    h. security services; and
    i. management services.

2. An organizational OSE profile of open standards and other nonproprietary specifications is developed around the required service areas. This step and the next require the help of experts in specific standards (standards are too complex, numerous, and detailed for any one person to be knowledgeable enough to make coherent decisions about the entire profile.)

3. The organizational profile is tailored to set options and parameters called for in specific standards and specifications.

4. The profile is augmented where there are gaps not covered by standards, and where conflicts among policies, organizational objectives, and the standards exist. Interoperability concerns among different standards and specifications are also taken into consideration.

5. Develop acquisition strategies to acquire the Federal Information Processing (FIP) resources needed to transition from current information system environments to an OSE.

6. Procurements are organized and carried out according to resources, time, and technology available for implementation.

With the information provided in this guide, program managers and senior project engineers can formulate questions to ask of the standards experts. Examples of such questions are the following:

- For a specific set of requirements, which standards best meet the needs of the organization?
- What are the interdependencies of different standards?
- How will selection of specific standards affect the long-term capabilities of the organization?

The lessons-learned contained in this report's recommendations are meant to provide the answers to many of these questions and are the result of actual procurements that have been used to implement and support open system environments over the last 5 years. They have evolved through debate and wide-spread agreement on the effects produced within the affected procurements and have been abstracted in this report for application across many types of procurements.

The typical plan of action for using this report is the following:

1. Examine applicability descriptions in the "Application Portability Profile" and the "Federal ADP and Telecommunications Standards Index" for each specification. Determine from these descriptions whether there is significant overlap between the functional requirements of the procurement and the applicability of the involved specifications.

2. For those specifications that are applicable, evaluate the information provided in this guide to determine if the use of the specification is economically and technically feasible. Additional information may be required in this evaluation process, especially from standards experts, the APP Guide (see NIST Special Publication 500-210), and other publications.

3. For those specifications selected from the previous two steps, determine where in the Request for Proposals (RFP) the specification should be referenced and when it should be required.

4. Use the italicized requirements text and reference material suggested within each section. This text should be modified as necessary to suit organizational policies and provide clearer requirements.

Once the above process has been completed, further restructuring of the functional requirements and standard specifications may be required to provide continuity and clarity in the overall RFP.

Text in *italics* is presented as suggested wording to use in solicitation documents. Lessons-learned sidebars and boxed comments are used to explain or illuminate the reasoning behind certain requirements, or to provide additional information that may require consideration in the determination of requirements for inclusion in the Statement of Work (SOW). The normal text describes the context for use of specific standards and provides information that directly impacts the procurement based on the use of each standard.

1. INTRODUCTION

The publication of the first version of the Application Portability Profile (APP) in National Institute of Standards and Technology (NIST) Special Publication 500-184 (April 1991) marked the beginning of a new phase in technology acquisition within the U.S. Government. The APP defined the boundaries of an Open System Environment (OSE) in which information systems could evolve independent of proprietary solutions and technology. The APP provided NIST's recommendations on specifications to use in defining an OSE.

The Open System Environment concept has become ubiquitous throughout both the public and private sectors. Federal agencies are finding that open systems provide a more flexible, cost-effective, and beneficial environment for supporting mission-critical applications than previous infrastructures based on proprietary technology. They are also finding that the initial move to open systems can be expensive and difficult to manage if not planned carefully.

Building or acquiring an OSE is no small task. Various procurement programs have involved directly as few as twenty and as many as one hundred and fifty personnel in the procurement process. These procurements are generally $100 million or more in value, with several in the $500 million to $1 billion-plus range, and span implementation periods of 5 or more years. They are complex to the technically uninformed and require significant planning for success. There is a redeeming factor about OSE: it does not have to be built or acquired all at once. It can be accomplished in smaller steps (e.g., procurements and programs) each of which fits under the OSE umbrella.

Because of the magnitude and complexity of establishing an OSE, many Federal agencies have asked NIST's Computer Systems Laboratory (CSL) for assistance in defining the requirements for an OSE and in evaluating procurement documents for acquiring the infrastructure necessary to support an OSE. This report includes a compilation of lessons-learned in evaluating the documents and plans associated with OSE procurement, and is meant to assist agencies in implementing OSE-based procurements.

1.1 Purpose

This report provides agency program managers and senior project engineers with a model and guidance for developing the plans and specifications necessary to define the open system environment (OSE) requirements in Requests for Proposals (RFPs). Additional information is provided for assisting agencies in determining which portions of the report are applicable to their specific acquisition plans. Lessons-learned are highlighted in sidebars and annotated text that accompany many of the report's subsections. This report assumes that users are familiar with the OSE concept and contents of the Application Portability Profile as described in the current version, Version 2.0, of the APP Guide, NIST Special Publication 500-210, dated June 1993.

1.2 Scope

The specifications referenced in this report reflect the current state of specifications that are applicable and usable within federal acquisitions. They will change over time as new technology

is added and obsolescent technology is replaced. Other specifications, such as Federal Acquisition Regulations (FAR); Federal Information Resources Management Regulations (FIRMR); Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources"; the Brooks Act of 1965; the Competition in Contracting Act (CICA), and other U.S. laws and codes prescribe constraints and conditions on the Federal acquisition of information technology. Together, these documents form much of the context for this report.

Table 1. RFP Sections Emphasized in the OSE Procurement Guide

SECTION	TITLE
B	Solicitation/Contract Form (Standard Form 33)
B	Supplies or Services and Prices and Costs
C	DESCRIPTIONS/SPECIFICATIONS/STATEMENT OF WORK
D	Packaging and Marking
E	Inspection and Acceptance
F	Deliveries or Performance
G	Contract Administration Data
H	Special Contract Requirements
I	Contract Clauses
J	List of Attachments
K	Representations, Certifications, and Other Statements of Offerors or Quoters
L	INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS
M	EVALUATION FACTORS FOR AWARD

The procurement process targeted in this report focuses on the specification of requirements in terms of standards that can be used in Sections C, L, and M of Federal Requests for Proposals (RFP). Other sections of the RFP are not covered. Table 1 lists all sections required in Requests for Proposals and illustrates those sections that are emphasized in this report.

The guidance in this report pertains to U.S. Government acquisition of OSE infrastructure including operating system, human/computer interface, software engineering, data management, data interchange, graphics, network, security, and system/network management services based on implementations of standard application program interfaces, programming languages, data formats, and protocols. Other organizations, such as state and local governments, academic, and private institutions also may find the information helpful in defining computing environments that promote application portability, interoperability, and scalability.

A cursory listing of other functional, nonstandard requirements, such as would be found in individual procurements, is also provided where appropriate. These are added to illustrate that each procurement is unique and individual according to an agency's purpose in entering a large-scale procurement program. They also show that agency-specific requirements are somewhat different from the OSE requirements and cannot necessarily be formulated as standards. Requirements that are specific to an individual agency's procurement must be defined by the acquiring agency. These requirements may take various forms. In some cases, where augmentation or conflict resolution are required, the organizational requirements may override the OSE requirements.

The ability to provide the appropriate OSE infrastructure is in part dependent on specifying the appropriate subsets, options, modules, and levels of FIPS implementations. Programming languages such as Ada, COBOL, and Fortran have various "required" and "optional" features which can be selected. This is also true for POSIX, SQL, and other standards implementations as well. Requirements developers need to evaluate these subsets, options, modules, and levels and then clearly specify them in acquisition documents.

1.3 Report Organization

This report includes guidance for determining when to use a particular specification. The guidance consists of short descriptions of applicability that illustrate the use of each specification. This guidance is not intended to be all-encompassing, nor can it be. Each agency will have unique requirements that can be stated only in terms of the particular acquisition planned by the agency. Only the acquiring agency can know how individual decisions will affect the overall plans for acquiring the technology to support an OSE. The guidance presented in this report is generic in nature and provides a cursory view of a range of possibilities. Further analysis by the agency business and standards experts is recommended in order to determine applicability of each specification to an individual procurement.

Section 2 provides an overview and outline for organizing OSE requirements. Sections 3 through 14 provide details for examining individual specifications within each OSE service area and their applicability to functional requirements. Within each of these sections, users will find information to assist in the decision-making process, to specify what the offerors should include in proposals, and how the offerors' proposals should be evaluated. Section 15 describes requirements for transitioning from closed to open systems. Section 16 emphasizes the evaluation of proposals, and section 17 concludes the report. Annex A presents criteria for selecting OSE proposal evaluators. Annex B illustrates part of a sample Section C Statement of Work based on recommendations in this report. Annex C provides a list of references to be used with this report. Annex D provides an abstract decision model consisting of questions that users should ask about their systems when developing the set of specifications and standards on which to build the OSE. A glossary of terms and an index complete the report.

2. OSE REQUIREMENTS AND SPECIFICATIONS

OSE requirements stem from organizational requirements that are used to derive a profile or selected list of specifications. These specifications define the environment in which the organizational OSE is to operate.

The Institute of Electrical and Electronics Engineers (IEEE) POSIX P1003.0 Working Group is developing a Guide to Open Systems (i.e., the POSIX Guide). The POSIX Guide describes how to go about developing an organizational profile starting with requirements found in existing and planned applications. These applications provide the basis for profiles of specifications necessary to support all organizational requirements.

In the process of identifying requirements, salient concepts tend to become the focus of the organization's attention. In general, these concepts are similar for all types of organizations and are used in this report to assist agencies in identifying which specifications to select. Examples of such concepts are the implementation of centralized versus decentralized databases; client-server versus master-slave computing relationships; local and wide area network access; secure operations; and various types of data interchange. Figure 1 illustrates where OSE requirements evolve and become part of the procurement process, and the relationship of this report with the procurement process.

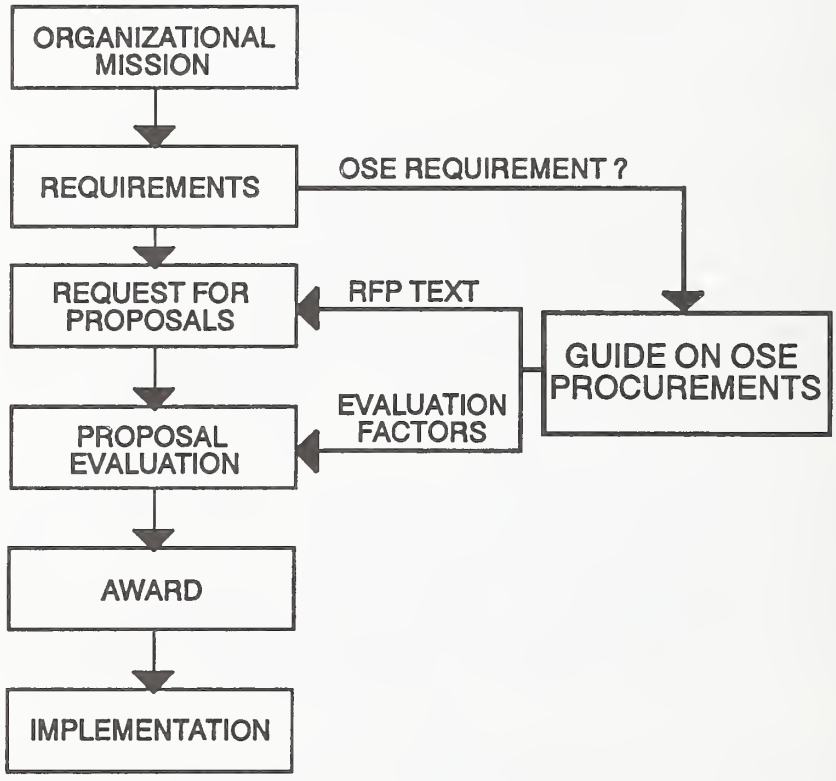


Figure 1. Relationship of OSE Requirements to Procurement Process.

The specifications and standards referenced in the APP are directed to implementors of open systems, not to users of open systems. Within this context, the specifications contain information that is extremely technical and meaningful only in very narrowly defined domains. Most users will never even be aware of the existence of these specifications. Their use, however, is necessary in implementing an OSE.

Section C of Federal RFPs is used to describe the functional requirements of the solution space. The general organization for specifying an open system environment in a procurement parallels the service sections described in the APP Guide, with a few modifications. If a particular service or

component is not required in the procurement, it may be omitted. Otherwise, all sections included in the following outline should be specified in the OSE requirements sections of the RFP.

Requirement for Open System Environment
Operating System Services
Human/computer Interface Services
Software Engineering Services
Data Management Services
Data Interchange Services
Graphics Services
Network Services
Security Services
Management Services

Additional sections specifying other requirements are added as required. The following paragraphs are taken from the APP Guide, Version 2.0, and provide a short description of these service areas. Any differences between these descriptions and the APP Guide text are a result of the process through which these documents are evolving. In any case, the APP Guide text is the authoritative text.

Lesson learned...
In general, the RFPs that CSL has reviewed include thick sections C. Such specifications normally turn out to be difficult to evaluate and very time-consuming. In this report, a "thin" statement of work is proposed containing only the mandatory requirements to be met. All of the optional requirements are specified in section M as evaluation factors. This has two large-grained effects on the proposal evaluation process. First, vendors are freer to propose technical solutions that are more attuned to the needs of an organization, including the latest technology. Second, evaluation can be judged on "best value" (for those vendors that can meet the minimum mandatory requirements) by virtue of extra points awarded for more options proposed. In many cases, the information needed to award extra points can be captured in automated evaluation systems that automatically assign a score based on the number of optional requirements met. Of course, this implies that the optional requirements are detailed enough for evaluators to make generally objective assessments of capabilities.

2.1 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 peripheral devices.

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

c) 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.

2.2 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.

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 art world, is the integration of two or more different modes of expression within a single work of art, such as the mixing of sculpture and music or painting and dance. In the world of information processing, multimedia 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-dependant representations, and multi-channel input and output.

2.3 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 Ada, C, COBOL, FORTRAN, and Pascal.

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.

2.4 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 data about data (i.e., metadata). Such data may include internal and external formats, integrity and security rules, and be located within a distributed system.

b) Database management 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, although some of these services could be provided by general file management capabilities described in operating system services.

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

2.5 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 currently 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 device independent definition of picture elements.

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.

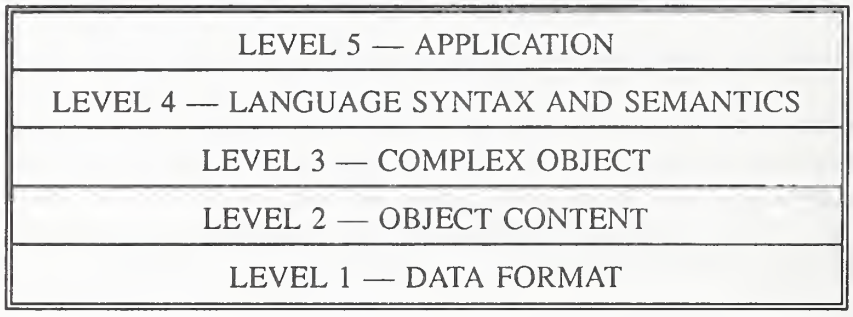


Figure 2. Data Interchange Complexity Levels.

There are various levels of complexity of data interchange. At the lowest level of complexity, Level 1, 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, Level 2, represents content. Text, raster images, and audio are examples of different content types. Level 3 includes 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, Level 4. The language level is suitable for humans to understand what is being represented. Level 5, 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. Figure 2 illustrates the hierarchy among these levels of complexity.

2.6 Graphics Services

The graphics services required by applications fall into two distinct categories. First, there are the graphics features used by human/computer interfaces (HCI). These are also called graphical user interfaces (GUI) when non-text information other than color is to be displayed. HCI is concerned with providing efficient and reliable methods for exchanging information between the application and user. These interfaces normally use only simple two-dimensional graphics and their functionality could, in theory, be supported by a purely textual interface. The second category

includes applications in which the information to be displayed is inherently graphical, such as pie charts, maps, architectural plans, molecular modelling, flight-training simulations, etc.

These two categories are not mutually exclusive. Although both categories include requirements for true graphical operations, applications requiring a combination of these services may be able to take advantage of implementations from one category with augmentation by implementations in the other.

2.7 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 standardized in a national or international standard.

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

2.8 Integral Supporting Services

Two supporting services are integrated within and permeate the other seven service areas. In many cases, separate specifications are not available for these supporting services within each of the seven service areas. These two services are security and management services described as follows.

2.8.1 Security Services

Security services are provided to support the secure distribution and integrity of information and to protect the computing infrastructure from unauthorized access. These services include the following:

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

b) 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.; and the functions that provide human/computer interface services such as human/computer interface management systems.

c) Programming 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.

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.

e) 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.

f) 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).

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

2.8.2 Management Services

Management services are integral to the operation of an open system environment. They provide the mechanisms to monitor and control the operation of individual applications, databases, systems, platforms, networks, and user interactions with these components. Management services enable users and systems to become more efficient in performing required work. Management is better able to streamline the operation, administration, and maintenance of open system components. These services include the following:

a) Fault management and control services that detect, log, and reconfigure systems through human intervention or through automatic means.

b) Configuration control services that provide mechanisms for performing version control.

c) Accounting services for monitoring system and network usage.

d) Performance monitoring services for computing effectiveness of configurations and estimating future performance requirements.

2.9 Additional Services Requirements

The first section mentioned, "Requirement for Open System Environment (OSE)," describes the overall characteristics of the computing environment to be acquired and describes some of the terminology used in the other sections. The subsections defining requirements for each service needed to support organizational objectives are specified in order as above. Additional sections and subsections may be required depending on the type of procurement under development. For

example, the subsection dealing with data management services may contain additional requirements that are not specified in the standards, but that are needed for the subject procurement. These might include requirements for interfaces to specific database management systems that are already installed, or a requirement for data administration software to be included in proposals.

3. ACQUIRING AN OPEN SYSTEM ENVIRONMENT

In this section, guidance to assist agencies in determining the applicability of each specification, along with sample RFP sections (in *italicized text*) are provided. Where appropriate, these requirements are translated into text referencing specific standards. The introductory material in the initial section, "Requirement for Open System Environment" places the requirements in context and provides references to other publications for background reading. It describes the overall scope of the acquisition.

3.1 Scope of the Acquisition

Introductory material is presented to explain to prospective bidders that the procurement is based on open systems and what concepts and systems are involved. The following text can be included in the RFP to define some of the main concepts and features of the OSE.

> *The National Institute of Standards and Technology (NIST) has developed an Open System Environment (OSE) framework that is directed at supporting a broad range of Federal applications. This framework is called the Application Portability Profile (APP) and is currently defined in NIST Special Publication 500-210.*

NIST Special Publication 500-210 changes with each version released. Version 1.0 of the APP was released as NIST Special Publication 500-187, Version 2.0 as NIST Special Publication 500-210. Program managers should check the current Special Publication number.

> *The APP describes the component interfaces, protocols, and supporting data formats necessary to provide the services required by applications. A profile, or selected list of specifications, options, and parameters defines specific interfaces, protocols, and data formats and has been recommended by NIST for use by Federal agencies and is included in the APP.*
>
> *The main purpose of establishing an OSE is to provide a stable environment in which interoperability, portability, and scalability of applications are the major focus. These terms are described as follows:*
>
> > *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 (defined below) 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.

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

The focus of this section is on the description of requirements for establishing an agency-wide Open System Environment.

3.1.1 Systems and Applications

The establishment of an OSE is not the only purpose for a procurement. Usually, the support of specific applications and systems will become the real crux of the procurement. These applications and systems must be enumerated within the RFP.

The following four specific systems are listed only as examples of the types of information included in this subsection. These systems and applications are related to the OSE through various other requirements specified in additional technical requirements sections throughout the RFP and are specific to an individual organization's procurement.

> For each system or application mentioned, information about its level of openness and the nature of this openness (i.e., what standards are already in place) should be described.

The systems and applications affected by this procurement include the following:

Time and Attendance System (TAS)

A description of Time and Attendance System requirements would be placed here.

Payroll System

A description of Payroll System requirements would be placed here.

Contracts Administration System

A description of Contracts Administration System requirements would be placed here.

Local Area Network Installation

A description of Local Area Network Installation requirements would be placed here. Note that the requirements established in this section are general in nature and do not necessarily duplicate those found in the network services section. For example, a requirement in this section might take the form, "Contractor shall determine the requirements for implementing Local Area Networks where

none currently exist. The implementation shall conform to the requirements in section [Computer Network Services][1]."

Legacy Systems Interoperability

Legacy systems are those that will remain in operation, but will not transition to the OSE for a number of reasons (e.g., they are not mission-critical, they are due to be replaced, they are the responsibility of another organization, etc.). In many cases, the systems to be implemented in the OSE will still have to communicate and share data with legacy systems. The requirements should spell out which systems will be considered as legacy systems, and the data and communications requirements necessary to support interactions among the legacy systems and the OSE.

Organizational Requirements

The number of systems and applications included is open-ended. Other pertinent environmental information may be inserted here. Examples include the number and types of system users, organizations to be supported, geographic locations, etc.

3.1.1.1 Instructions to Offerors

Section L should require the offeror to respond as follows:

> *For each system and application described in section [Systems and Applications], the offeror shall provide a description of the proposed OSE architecture components that will support each application or system in enough detail to allow evaluation of the offeror's grasp of the complexity of the existing system and transitioning it to the OSE. A matrix consisting of and indexed by applicable section C RFP requirements and the responses from the offeror's proposal shall be provided for each system and application required.*

3.1.1.2 Evaluation of Proposals

Offerors should provide a detailed description of the overall OSE and how each application and system fits within the infrastructure proposed. This information should include context descriptions and diagrams showing where major components of applications and systems are located, the infrastructure proposed to support each application or system at each location, and how all of these components are linked within the OSE. (See fig. 4 on page 63 for an example of such a diagram.)

---

[1]Titles or phrases surrounded by square brackets, [], indicate that a section number from the RFP associated with the referenced section should be inserted in place of the bracketed title or phrase. For example, [Computer Network Services] references the section entitled "Computer Network Services" from this report. In an actual RFP containing a Computer Network Services section, a section or paragraph number will be associated with that section. The number of that section is actually being referenced by the bracketed phrase and should be inserted in its place. If the actual Computer Network Services section were numbered C.4.5, then C.4.5 would replace [Computer Network Services].

CLIN	PRODUCT NAME	PRODUCT IDENT.	PLATFORM	VALIDATION TYPE	VALIDATION IDENT.	DESCRIPTION	REF. DOC.
0100	ABC-SQL	Release 1.01	486/100	VPL	NIST/930929-0001 VPL 6/93, p. 37	Data Management, ABC Company	Vol. 1 #105

Figure 3. Example of OSE Configuration Summary.

3.1.2 Requirement for Open System Environment

The following paragraph explicitly requires an OSE implementation.

Requirement for Open System Environment (OSE)

All information technology (IT) products and services offered in response to this solicitation shall operate in and execute upon platforms that provide an open system environment as described in the National Institute of Standards and Technology's (NIST) Special Publication 500-210 and modified in this contract[2]*. The contractor shall provide evidence to show that these products and services conform to the standards and specifications cited elsewhere in this contract. In addition, the contractor shall provide evidence showing that products, in fact, interoperate and are portable in the proposed OSE and within the constraints identified by these specifications.*

3.1.2.1 Instructions to Offerors

An easy way to organize evaluations of products proposed by a particular offeror is to require a table of information, such as in figure 3.

The contractor shall provide information for each product proposed for use in the OSE as follows:

Contract Line Item Number (CLIN)

Name and identification of each product including version or release number that identifies the implementation explicitly from all other versions or configurations

Name and identification of the platforms upon which the products identified above are to be executed

Validation identifier, Validated Products List (VPL) date and page number; capability demonstration report date; or trademark/branding certificate identifier and issuing organization

---

[2]The word *contract* instead of *solicitation* is used throughout text that refers to requirements in Section C of the RFP and the statement of work. This is done for two reasons: 1) normally these sections are included in the contract when an offer is accepted, and including it within the RFP in this manner eliminates the necessity for making global word changes in the final contract when it is signed; 2) the word *contract* differentiates requirements in these sections from those that pertain solely to proposal requirements and preparation. In the second case, the word *offer* is used instead of *contract*.

Description of the product (e.g., applicability, manufacturer identification, commercial availability date, product interoperation requirements, errors reported in the VPL, supporting test reports, etc. In short, include information that will differentiate this product from all other similar products and manufacturers.)

The CSL Validated Products List (VPL) is produced four times a year. If a product has been validated, but is not yet listed in the VPL, an agency may still admit the product if all test requirements specified under other clauses have been met (i.e., test reports, etc. have been submitted), or an updated online VPL is available.

Reference document identifiers that support contractor product claims as required, and cross-reference to section numbers as described in [Hardware Components][3]

A summary of this information shall be provided in a table formatted as in the example in figure 3.

A text description of each product and platform proposed for use in the OSE shall be provided and included as subparagraphs of this section.

This table and descriptions shall be updated for each intermediate target implementation.

3.1.2.2 Evaluation of Proposals

Depending on the types of proof required and offered, evaluation may proceed in checklist fashion, as an in-depth analysis of products, or a combination of these techniques.

A checklist may be used to cross-reference deliverables to products. For example, products that have CSL validation certificates should be accompanied by references to the VPL page and publication date, or a copy of the validation certificate, or a copy of the test report, depending on what is requested in the RFP instructions. For those products that require capability demonstration, a schedule date and description of tests to be used should be referenced.

Detailed validation reports are kept on file within CSL for each implementation listed in the VPL. These reports should be used for further analysis in those cases where questions arise about the suitability of a particular product.

In-depth product analysis takes this several steps further. For each platform proposed, a set of validation deliverables may be required. In some very large procurements or procurements with highly critical requirements, a case can be made for requiring validation of all products on the platforms proposed. In this case, testing can become very expensive for offerors. The cost of such testing may be a valid concern, but such costs must be weighed against the benefits of performing

[3]See footnote 2.

these tests, such as reducing the risk of protests and acquiring products that work as specified in the RFP. The following section describes more about testing.

3.2 Standards Testing

Software testing is expensive. In software development, it is not uncommon to find that 50 percent of the development budget is set aside for testing. Testing to standards and interoperability testing, however, are generally insignificant costs in relation to the overall testing budget. Standards and interoperability testing provide a cost-effective means of removing substantial risk that products will not be suitable for use. This section describes various levels of testing that may be applicable to a particular procurement.

Adequate testing within the requirements of an RFP can be determined solely by the acquiring agency, regardless of how an implementation is listed in the VPL. Even if an implementation meets the requirements of a particular standard, but does not meet the detailed requirements within the RFP, such as specific subsets, options, modules, or levels of the standard, it may not be suitable for use by the agency.

Validation testing requires a single implementation to successfully pass a series of tests that stem from the requirements of a standard. Interoperability testing requires an implementation to communicate information successfully to another implementation and for the receiving implementation to be able to use that information.

3.2.1 Applicability of FIPS

To determine what testing is applicable, agencies must determine what standards apply. In general, a FIPS states whether it is mandatory or optional. For mandatory FIPS requirements, a waiver may be granted by the head of the agency. The acquiring agency can override an optional FIPS and make it mandatory within agency policy or within the requirements of a specific procurement. In any case, validation of mandatory or optional FIPS implementations may be warranted.

Validation of FIPS implementations shall be required when the following conditions are met:

a) A FIPS exists and is required by this contract.
b) An official conformance test suite exists.
c) A FIPS testing procedure has been defined.
d) NIST-accredited or CSL-recognized testing laboratories exist.

Standards experts and organizational requirements experts need to determine together whether individual specifications, including subsets, options, modules, and levels, provide the required functionality needed within the contract. Functionally, the requirement is defined directly through inclusion of succinct wording that makes the requirement clear, e.g., "if the offeror submits an implementation that is covered by a FIPS, then the FIPS applies and the offeror must also submit proof of conformance to that FIPS."

General requirements of testing and instructions for providing proof of validation testing are included in the following paragraphs.

Unless otherwise specified, all standards-based validation testing shall be conducted by CSL, or by testing laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) of NIST, or by testing laboratories that are officially recognized by CSL as the sole validation authority for specific standards, or by organizations named specifically in this contract.

3.2.2 Validation Testing

The General Services Administration's (GSA) "Federal ADP and Telecommunications Standards Index" describes three types of validation testing.

3.2.2.1 Delayed Validation

When an agency determines that the nature of the requirement is such that implementations of a FIPS may be offered that have not yet been tested for conformance to that FIPS, the following solicitation wording should be included:

The offeror shall certify in the offer that all implementations of FIPS, including applicable FIPS options, offered in response to this document will be submitted for validation upon contract award with a request that the validation be completed at the earliest possible date permitted by the CSL validation procedures, or have been previously submitted by the CSL validation procedures, or have been previously tested or validated and included on the current list of validated products maintained by the CSL. Unless specified elsewhere, proof of submission for validation shall be in the form of a letter scheduling the validation, and the subsequent delivery by the offeror of a CSL registered report or CSL certificate immediately upon receipt thereof. Proof of testing shall be provided in the form of a CSL registered validation summary report. Proof of validation shall be in the form of a CSL Certificate of Validation.

The following are some of the reasons an agency may want to allow delayed validation:

- A standard may be relatively new or few implementations may be available, and offerors need additional time (and possibly funding) to finish product development.
- There are few validated implementations available.
- The cost of proposal preparation may be minimized by requiring only the winning contractor to incur the cost of validation.
- It allows contractors who would be prohibited otherwise from competing to get their products validated and enter the competition.
- When the validation process has not been completed due to schedule conflicts at testing laboratories, or when a longer than anticipated validation review process is realized.

3.2.2.2 Prior Validation Testing

When an agency determines that it is essential for implementations of a FIPS to be previously tested for conformance to that FIPS before being offered, and the nature of the requirement is such that an implementation of a FIPS may be initially offered that has not been fully validated (i.e., an implementation has not fully demonstrated compliance with the FIPS due to test failures or incomplete implementation), the following wording shall be included:

> *The offeror shall certify in the offer that all implementations of FIPS, including applicable FIPS options, offered in response to this document have been previously tested or validated and included on the current list of validated products maintained by the CSL. Unless specified elsewhere, proof of testing shall be provided in the form of a CSL registered validation summary report. Proof of validation shall be in the form of a CSL Certificate of Validation.*

Agencies should use this requirement when it is immediately necessary to increase the sources of implementations in the competition base. This option enables implementations to be included in the competition which have already been tested, but failed one or more validation tests and have to be retested after the offeror provides corrections.

This approach allows implementations to be offered which fully qualify for a certificate of validation as well as those which may only qualify to receive a registration report. For those implementations with test failures, the registered test report may be required as part of the proposal submissions to allow the acquiring agency to review the nature of test failures and their impact on the OSE implementation.

3.2.2.3 Prior Validation

When an agency determines that only validated implementations may be offered (i.e., an implementation has been tested and has demonstrated conformance to the FIPS), the following wording shall be included:

> *The offeror shall certify in the offer that all implementations of FIPS, including applicable FIPS options, offered in response to this solicitation have been previously validated and included on the current list of validated products maintained by the CSL. Unless specified elsewhere in this solicitation, proof of validation shall be in the form of a CSL Certificate of Validation.*

The differences in the above requirements amount to this: *delayed validation* is used when conforming implementations do not necessarily exist and the agency wishes to give offerors a chance to get products validated within a specific time after contract award; *prior validation testing* is used when implementations have been tested but do not conform to the FIPS and have to be retested or a waiver through interpretation procedures is obtained; *prior validation* is used to require that only validated implementations may be offered.

Validation can also be referred to by class as described in the following.

3.2.2.4 Validation

The term *validation* with no modifiers refers to the result of testing when the following conditions have been met:

a. A FIPS exists.
b. An official validation or conformance test suite exists.
c. FIPS testing procedures exist.
d. Accredited FIPS testing laboratories exist.

If any of these elements are missing, then validation as the term is used cannot be required. Instead, capability demonstration which is described later may be required.

Successful validation results in the issuance of a Certificate of Validation and registration of the certificate and product name in the Computer Systems Laboratory's quarterly Validated Products List (VPL). If an implementation is tested but fails one or more tests, a certificate is not issued, but the product name and the test report on the results of testing (which includes a description of test failures) may be listed as tested in the VPL.

The registration consists of identifying information including the name and vendor of the product, the associated validation certificate number and date if applicable, and the platform upon which the test was performed.

Vendors have reported various levels of cost for validating products. At the time of this report, some of the fees required for validation testing included the following:

POSIX.1	$4,000 per implementation
Ada, C, COBOL, FORTRAN, Pascal, and SQL	$2,500 to $11,000 per implementation, fee based on level of effort depending on vendor assistance required, and number of interfaces, platforms, and options tested
GKS	$12,000 for first implementation, $3,000 per additional platform, $1,300 per additional implementation
PHIGS	$17,500 for first implementation, $5,000 per additional platform, $2,000 per additional implementation
CGM	$500 for up to 5 metafile tests, $9,000 per generator, $5,000 per interpreter
GOSIP	$20,000 to $100,000 per protocol

POSIX and GOSIP testing include additional costs for contracting with independent testing laboratories.

In some cases, NIST's Computer Systems Laboratory (CSL) performs FIPS validation tests. In other cases, independent first party and third party laboratories perform the tests and submit the test results to CSL for verification. In virtually all cases, CSL determines whether a certificate shall be issued and is responsible for the issuance of validation certificates or registration of validation. NIST accredits these first party and third party testing laboratories through the National Voluntary Laboratory Accreditation Program (NVLAP).

In still other cases, as with DoD's Ada Joint Program Office (AJPO), CSL officially recognizes another Government organization as the validating/testing authority for a specific standard and registers validation certificates and test results provided by those agencies. DoD's Joint Interoperability Test Center (JITC) is CSL's agent for validating computer communications implementations. Specifically, types of organizations that validate individual FIPS implementations are listed in table 2 (See page 21.)

Communications implementations are not issued validation certificates. Instead, they are registered on accredited product registers maintained by DoD's Joint Interoperability Test Center (JITC). These are classed as either base or derived validations (see the following section) and are listed in the VPL as such.

An agency is not required to accept implementations if test failures have occurred. It is up to the acquiring agency to determine if the failed tests will cause the implementation to be unusable within the agency's requirements. In addition, the agency may issue requirements that preclude the proposal of implementations with test failures (see *prior validation* above).

Table 2. Specifications and Testing Organizations

SPECIFICATION	VALIDATION ORGANIZATION
FIPS 21-3 COBOL	CSL
FIPS 46-2 DES	CSL
FIPS 69-1 Fortran	CSL
FIPS 113 Computer Data Authentication	CSL
FIPS 119 Ada	Ada Joint Program Office (AJPO)
FIPS 120-1 GKS	CSL
FIPS 127-2 SQL	CSL
FIPS 128 CGM	CSL (two different certificates can be issued)
Planned FIPS 146-2 (POSIT)	CSL (DoD Joint Interoperability Test Center)
FIPS 151-2 POSIX	NVLAP accredited laboratories
FIPS 153-1 PHIGS	CSL
FIPS 160 C	CSL
FIPS 171 Key Management Using ANSI X9.17	CSL

Alternative wording for specifying FIPS validation in OSE procurements is contained in the following:

> *Validation: Where a FIPS is specified, and a validation test suite is available, and CSL validation testing procedures are in place, and one or more CSL-recognized testing laboratories are available, only validated implementations shall be used. The implementations shall implement all of the requirements of the FIPS and specified options, and test results shall contain no failures. Proof of conformance shall be submitted in the form of an entry for*

the validated product in the current CSL Validated Products List (VPL). This entry shall indicate that such testing has been executed on the platform configurations proposed under this contract. In addition, a CSL-registered test report shall be submitted. Derived validations will not be accepted in this category. (Derived validation is defined in the following section.)

3.2.2.5 Derived Validation

Derived validation is also known as validation by registration for certain standards, most notably Ada. In derived validation, an existing implementation of the standard has been validated by CSL or a recognized laboratory and has passed all of the validation requirements, and the implementation has further been ported to another platform environment that is not significantly different from the platform used in the original or base validation test. In addition, the contractor must certify that the official test suite has been executed on this new platform. The test results must have been submitted to CSL for review. In these cases, no certificates are issued. Instead, the vendor of the product certifies that the test was executed according to the applicable validation procedures, and the implementation is named in a public list of products that purport to have passed validation testing (i.e., the CSL Validated Products List [VPL]).

Vendors of FIPS implementations are allowed to derive validations. That is, the vendor of a product that has been validated formally by NIST on a particular platform may acquire the test suite, test it on another related platform, and register the test results with NIST. Since NIST does not witness the test in this case, a certificate is not issued. The name of the product will be listed, however, in the Validated Products List (VPL) as a product with a derived validation.

The only FIPS implementations that are not subject to derived validations are those for FIPS 151-2 and those FIPS dealing with security implementations.

Derived Validation: Where a FIPS is specified and a validation test suite is available and CSL validation testing procedures are in place, only validated implementations shall be used. The implementations shall implement all of the requirements of the FIPS and test results shall contain no failures. Proof of conformance shall be submitted in the form of an entry for the validated product in the current CSL Validated Products List (VPL). A currently valid base validation certificate and a reference to the entry in the VPL listing the base validation may be submitted as proof of derived validation or validation by registration, as long as the implementation submitted is essentially the same as the implementation cited on the base certificate (i.e., errors may have been corrected, or performance changes may have been implemented, but no significant capabilities shall have been changed), and the platform configuration cited on the base certificate is the minimum when compared to the platform configuration proposed under this contract, and the proposed platform is binary compatible (i.e., uses the same CPU instruction set in native mode) with the base certificate platform. Final assessment of the acceptability and suitability of any implementation changes shall be the sole decision of the acquiring authority. The test results shall have been generated during the period that the base certificate is valid.

An agency is not required to accept implementations which have been registered as derived validation. Agency requirements may preempt or restrict acceptability requirements defined within specific FIPSes.

Derived validation may be more than adequate for small-scale procurements. For large-scale procurements, derived validation is not recommended. Instead, validation should be required for those implementations based on FIPS, and capability demonstration for those based on non-FIPS.

3.2.3 Interoperability Testing

The acquiring agency should select one or more of the following paragraphs to define how interoperability testing is to be carried out or proven on offered platforms. Interoperability testing involves testing the capability of a particular product to operate correctly with the proper communications software in a network.

Interoperability among implementations shall be proven through current registration of offered products and test results with a CSL-approved interoperability registration service, where such service exists. Proof of registration shall be in the form of a reference to a current listing of the proposed product on the interoperability registration service.

Where CSL-approved interoperability registration service does not exist, the contractor shall demonstrate interoperability by executing demonstration tests on the proposed platforms as required by this contract for each individual specification affected.

CSL accredits testing services available from third-party laboratories. In communications testing, DoD's Joint Interoperability Test Center (JITC) in Fort Huachuca, Arizona, is the interoperability registration service for the U.S. Government. Once products have been validated and have demonstrated interoperability, they are registered in the JITC's database of validated products and also published as part of the Validated Products List (VPL).

Agencies must thoroughly test each application program that is to be provided to the offerors to preclude test failures during live test demonstrations. The Government tests should be conducted on multiple platforms to ensure interoperability prior to receipt of proposals.

3.2.4 Portability Testing

Portability testing specifies how applications should be tested for proving that minimum modifications are required to move them between different offered and legacy platforms. Normally, part of this can be shown through validation testing as defined above. Capability demonstration also may be used. One or more of the following paragraphs should be selected by the agency to define how portability testing is to be carried out or proven.

A Government-provided application program in source code form shall be compiled and executed on one or more of the proposed platforms selected at random. The application program shall be moved to another platform that is not of the same model and the program shall be compiled and executed on this platform. A detailed report of the modifications made to the source code to achieve successful compilation and execution shall be submitted.

The above test may be executed with contractor-provided application programs that have been approved by the Government.

Two or more references in the current Validated Products List (VPL) shall indicate that the same implementation of the proposed software (i.e., same version and release) has been validated on at least two other manufacturer's platforms.

Two or more certificates from industry-recognized trademarking or branding organizations shall indicate that the same implementation of the proposed software (i.e., same version and release) has been validated on at least two different contractors' platforms.

Agencies must thoroughly test each application program that is to be provided to the offerors to preclude test failures during live test demonstrations. The Government tests should be conducted on multiple platforms to ensure portability prior to receipt of proposals.

3.2.5 Scalability Testing

Scalability testing specifies how applications should be tested for proving that minimum modifications are required to move them between platforms of significantly different capability including legacy platforms and platforms offered by the contractor. Capability demonstration is used in conjunction with validation testing to prove that scalability requirements have been met. The following instructions are provided as a means of testing scalability.

A Government-provided application program in source code form shall be compiled and executed on one or more of the proposed platforms selected at random. The application program shall be moved to another platform that is not of the same model nor architecture (i.e., multiple processors versus single processor, different CPU instruction set, etc.) and the program shall be compiled and executed on this platform. A detailed report of the modifications made to the source code to achieve successful compilation and execution shall be submitted. This test and report may be combined with the application portability proof defined above, as long as the individual tests and results can be identified in the report.

The above test may be executed with contractor-provided application programs that have been approved by the Government.

Agencies must thoroughly test each application program that is to be provided to the offerors to preclude test failures during live test demonstrations. The Government tests should be conducted on multiple platforms to ensure scalability prior to receipt of proposals.

3.2.6 Capability Demonstration

Not all FIPS and non-FIPS implementations can be tested due to lack of a test suite, testing laboratories, or testing procedures. Capability demonstration is used in these instances. A capability demonstration is a planned demonstration of the functionality of an implementation witnessed by the Government or an acceptable third party. The results of such demonstrations are collected and evaluated according to the evaluation factors specified in the RFP.

> *In cases where capability demonstration is the required form of validation testing, the following instructions shall apply:*
>
> *Capability demonstration: Where a FIPS is not the required specification, or where a FIPS is required and a validation test suite is not available or a CSL validation testing procedure has not been established, or where official CSL-recognized test laboratories do not exist, the contractor shall demonstrate conformance to the specification in order to allow the acquiring organization to assess the proposed implementation's suitability under this contract. The contractor shall demonstrate the implementation in a manner that exhibits the implementation's portability, scalability, and interoperability characteristics.*

Agencies should select from the following requirements for specifying capability demonstrations.

> *A Government-provided application shall be installed and executed on two of the proposed platforms selected at random. (If only one platform is proposed, then a second platform of different model supplied by the Government/contractor shall be temporarily used for the execution of this test.)*
>
> *A data file of Government-provided information shall be transmitted through network communications directly (i.e., using a null modem or other similar connection) from one platform to the other. Both applications shall then be executed and a report printed of the file's contents on external storage, such as diskette or magnetic tape.*
>
> *A second test shall be executed to replicate the first test, but without direct platform connection (i.e., communications shall be routed through an independent electronic routing or bridging device before connection shall be complete). Transmission of data shall proceed at a communications speed different from that used in the first test (e.g., 19K bits per second [bps] versus 56K bps). A detailed report of the modifications made to the source code to achieve successful compilation and execution shall be submitted along with machine-readable file contents generated by both platforms during both tests. This test and report may be combined with the application portability and scalability proofs defined above, as long as the individual tests and results can be identified in the report.*
>
> *The above tests may be executed with contractor-provided data files that have been approved by the Government.*

Additional requirements may be specified for support software that is used in the development of acquired software (e.g., computer-aided software engineering [CASE] tools or language compilers that are used to develop custom software, but that are themselves not part of the contract

deliverables). The following specifies that support software should also be subject to the FIPS requirements.

> *In addition to the standard implementation requirements specified elsewhere in this contract, all implementations of Federal Information Processing Standards (FIPS) that are brought into the Federal inventory as a result of this contract for which validation is specified, and those implementations used by contractors to develop programs or provide services shall be validated using the official Validation System specified by the National Institute of Standards and Technology's (NIST) Computer Systems Laboratory (CSL). Validation shall be in accordance with CSL validation procedures for the individual FIPS concerned. The results of validation shall be used to confirm that the implementation meets the requirements of the applicable FIPS as specified in this contract.*

In many cases, standards are specified for defining requirements. In other cases, nonstandard specifications are used. In certain instances, the nonstandard specification is expected to become an industry, national, or international standard sometime in the near future (i.e., 1 to 3 years.) The following requirements specify what happens when a specification becomes a FIPS.

> *If a specification becomes a FIPS, and upon availability of a test suite, established testing procedures for the FIPS, and accredited testing laboratories, the contractor shall submit proof of conformance according to the testing requirements of the FIPS involved. As a minimum, validation shall be required within 12 months of the availability of the FIPS, an official CSL test suite, established testing procedures, and one or more CSL-recognized validation test laboratories.*

For those implementations that do not conform to FIPS requirements due to test failures, an interpretation of the standard may be required. The following specifies the procedures for obtaining an interpretation and for implementing the result of interpretation.

> *If an interpretation of the FIPS is required that will invoke the procedures set forth in FIPS 29-3, "Interpretation Procedures for Federal Information Processing Standards for Software," U.S. Department of Commerce, October 29, 1992, such a request for interpretation shall be made within 30 calendar days after contract award. Any corrections that are required as a result of decisions made under the procedures of FIPS 29-3 shall be completed within 12 months of the date of the formal notification to the contractor of the approval of the interpretation. Proof of conformance for correction testing shall be submitted.*

3.2.7 Alternatives to Testing

The following instructions are provided as alternatives to physical testing or demonstration of interoperability specifically for a particular procurement.

> *Two or more references in the current Validated Products List (VPL) shall indicate that the same implementation of the proposed software (i.e., same version and release) has been registered on the interoperability registers for at least two platforms.*

Two or more certificates from industry-recognized trademarking or branding organizations shall indicate that the same implementation of the proposed software (i.e., same version and release) has been tested for interoperability on at least two of the offered platforms.

The following paragraph is added to complete this section, but is generally not recommended as described. This concept is the weakest part of validation specification. It has not been tested in any legal sense. If adding this to the SOW causes contracting officers to be concerned, and compromise wording or evaluation factors cannot be determined, then a prudent course of action would be to omit this paragraph and rely solely on other methods of determining conformance.

Manufacturer's declarations and self-certification may be applied to essentially similar products that have been tested in similar platform configurations, only if one or more members of the proposed products have been tested and validated by CSL or a NVLAP-accredited laboratory. Contractors shall certify that products covered by these manufacturer's declarations and self-certifications comply with the appropriate standard.

3.2.8 Instructions to Offerors

The verification of test results can be very time-consuming and difficult if not approached with a rigorous plan, stringent requirements, and a pragmatic attitude. Instructions for providing proof of the required levels of compliance were described in the preceding sections. Without stringent requirements and steadfast adherence to the letter of these requirements, agencies will be strapped by having to accept less-than-adequate implementations.

Offerors should make sure that the letter of the requirement is followed in proposals. For example, if a certificate of validation is required for submission in the proposal, the certificate should match the offered product at every point in the requirements. Marketing literature and other substitute documents are not acceptable. The requirements in the RFP must make this explicitly clear. Additionally, agencies should require offerors to certify in section K of proposal responses that products meet the requirements of the appropriate standards cited in the RFP.

3.2.9 Evaluation of Proposals

The acquiring agency should require a Government-approved witness to be present during capability demonstrations unless an industry-recognized branding and trademarking authority is used to perform the demonstration. In this case, a Government-approved witness may be optional. In all cases, questions concerning the validation of individual products may be settled through the use of official test reports and test files used in the performance of the tests and submitted to the Government as described in the following clauses.

The implementation shall be tested using a test suite provided by the acquiring agency, such test to be witnessed by approved Government representative [most rigorous requirement]; or

The implementation shall be tested using a test suite provided by the contractor and acceptable to the acquiring agency, such test to be witnessed by approved Government representative [less rigorous requirement]; or

The implementation shall be tested using test suites provided by industry-recognized branding organizations and the contractor shall submit proof of conformance in the form of a certificate or license awarded by the branding organization [least rigorous requirement].

In any of the capability demonstration cases, the contractor shall obtain the approval of the contracting officer to use the proposed test suites and testing methods. The contractor shall provide the test suites, test results, and environment configuration parameters in the form of a test report containing this information. The test report shall provide other appropriate information to allow the acquiring agency to assess the demonstration.

In any case, agencies should perform an in-depth analysis of the proposed products by cross-referencing them against specific RFP instructions and requirements, certificates, capability demonstration results, etc.

4. OPERATING SYSTEM SERVICES

POSIX-like 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 in a multi-tasking environment.

Each of the OSE service areas contains the following: reference specifications define requirements that are based on public specifications and standards; additional technical reference specifications provide additional general and special requirements that are not necessarily covered in public specifications or standards.

The contractor shall provide operating system services including the specified interfaces, protocols, and supporting data formats for implementing portable applications at the application-operating system interface. These services shall include kernel operations, commands and utilities, system management, and operating system security as prescribed in the following:

Operating System Services Requirements Reference Specifications

POSIX-like operating system environments for kernel operations offered as a result of this and other requirements in this contract shall implement FIPS 151-2, as a minimum, and shall require validation in accordance with provisions contained in FIPS 151-2.

Individual agencies must determine what POSIX-like means specifically. The only way to do this is to determine what applications must be supported and what operating system requirements are required to support them. Analysis of the IEEE POSIX standard subroutines, data elements, and functions should provide an indication of the capabilities available through POSIX. Agencies must be careful to ascertain if enough of the application requirements can be satisfied by a POSIX implementation augmented through other means, rather than augmenting nonstandard operating system implementations (i.e., if the requirements are essentially POSIX-like, but a POSIX

implementation is not required in the RFP, the agency's procurement may be vulnerable to protest, unless a full requirements analysis has been performed and a waiver granted.)

The only validation applicable to FIPS 151-2 is "validation." "Derived validation" is not allowed under the testing policy of FIPS 151-2.

In general, applications will not even be aware that POSIX is operating on a platform. Since the operations of POSIX pertain primarily to low-level capabilities, other specifications, such as IEEE 1003.2-1992 Shell and Utility API are required to complete an operating system environment on the platform.

Commands and utilities include mechanisms for operations at the user/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. IEEE 1003.2-1992 can be used independent of FIPS 151-2.

> *Commands and utilities offered in support of FIPS 151-2 implementations shall implement IEEE 1003.2-1992, "POSIX Shell and Utility Application Interface for Computer Operating System Environments," as a minimum, and shall require capability demonstration.*

Most UNIX-derived implementations of POSIX also provide commands and utilities in a form that is very much like those defined in IEEE POSIX Working Group 1003.2 specifications. Those that are not very close implementations of the 1003.2 specification must be demonstrated to ascertain whether they meet the requirements of the standard. The IEEE standard should be reviewed to determine if its contents meet the agency's requirements.

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

> *Realtime operating system services offered in support of FIPS 151-2 implementations shall implement the functionality defined in IEEE 1003.4-1993, "Amendment 1: Realtime Extension [C Language]," and shall require capability demonstration.*

> *As standards and other specifications required in this contract evolve, the contractor shall provide upgrades for implementations based on the current standards within 12 months of the publication of these standards.*

> *Technology based on emerging standards that are not specifically referenced in this contract may be proposed by the contractor when such specifications achieve a high degree of stability and the benefit to the Government can be clearly documented when compared to older technologies and their cost bases.* (See Lessons learned sidebar on this page.)

> *Operating System Services Additional Technical Requirements Specifications*

The requirements that are not necessarily within the scope of OSE, but that are applicable to a particular procurement are defined in sections such as this. Such requirements might include reference to specific applications or systems that will explicitly require POSIX interfaces.

The following requirements are included only as examples of specific contract requirements that may be defined by technical personnel within an organization. These examples may or may not be relevant to a specific procurement.

> *Operating system services shall support the prediction of operating system service completion times. These completion times shall be bounded and shall be documented by the contractor.*
>
> *Operating system services shall provide applications with the ability to configure the implementation for optimal processing as required by the application.*
>
> *Operating system services shall provide applications with the ability to specify response timing constraints for bounded services and determine from system responses whether or not this timing constraint can be met.*
>
> *Operating system services shall allow processes that are not affected by lost services to continue processing.*

Lesson learned...

There are various methods for referencing non-FIPS specifications. The simple resolution implies expanding the required specification into the RFP itself, word for word. While this action is somewhat simple-minded and results in a voluminous RFP, it performs two functions: (1) it makes the requirements explicit within the RFP, and (2) it fixes the specification at a distinct point in time. Future changes in the specification will not directly affect the requirements of the RFP.

The problem with this concept is that changes in the draft specification may develop in the future to correct errors or extend the functionality of the specification. These changes will not necessarily be included in the RFP. Technology experts argue that the latest technology will not be available to the acquiring agency if this course is followed.

A correction for this situation involves the addition of a technology refreshment or technology enhancement clause within the RFP. The adjacent paragraphs include such terminology as an example.

4.1 Instructions to Offerors

For each product to be proposed on the basis of FIPS 151-2, the offeror should provide an entry on the OSE Architecture Summary and reference supporting technical documents. Technical documents to be included are listed in order of importance in the following, most important to least important:

CSL-registered validation test report
CSL-issued validation certificate

copy of page from current or previous Validated Products List identifying registered or validated product proposed
certificate from branding or trademarking organization identifying the product proposed

Marketing brochures, testimonials, and periodical articles are not acceptable as replacements for any of the above documents, although they may be used to augment the information available.

4.2 Evaluation of Proposals

Each product should be clearly identifiable on the OSE Architecture Summary. If validation documentation is provided, it should be identified on the Summary in the reference document column. Evaluation may be scored from highest to lowest based on the following:

Validation certificates on all of the proposed platforms within the parameters of the configurations proposed (At a minimum, this is twice as important as the next item.)
Validation certificates on a member of each family of platforms proposed (e.g., a family may consist of several models based on a type of CPU or architecture)
Validation certificate on a similar platform not proposed (e.g., same CPU but different vendor)
Validation certificate on any platform not proposed
(Award more points for including the full Test Report from CSL for any of the proposed implementations.)

5. HUMAN/COMPUTER INTERFACE SERVICES

Human/computer interface (HCI) services are required as part of the OSE. The following specifications add the capabilities of HCI.

The contractor shall provide human/computer interface (HCI) services including the specified interfaces, protocols, and supporting data formats for implementing portable applications at the application/user interface, and for communicating between the application/platform and the external environment. These services shall include client-server operations, object definition and management, window management, dialogue support, and HCI security and management as described in the following. These services shall be provided for both graphical and character-based display platforms.

Lesson learned...
The realities of the marketplace and the Federal application inventory dictate that both graphics-based and character-based user interfaces be supplied for various applications and domains. Graphics workstations are still quite expensive and can add significant costs to workstation procurements. The large inventory of personal computers within the Federal Government illustrates a need for including the character-based interfaces.

Human/computer Interface Services Requirements Reference Specifications

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.

> *Client-server operations offered as a result of this and other requirements in this contract shall implement FIPS 158-1, and shall require capability demonstration.*

Client-server operations are also defined in other types of specifications, such as communications and data interchange standards, and operating system specifications.

FIPS 158-1 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 based on the OSF MOTIF Application Environment Specification User Environment Volume. It includes a C language application program interface that is consistent with the Graphical User Interface Drivability Recommended Practice developed by IEEE P1202.2.

> *Object definition and management services, window management services, and dialogue support services offered as a result of this and other requirements shall implement the IEEE P1295.1 interface as defined in Draft "Standard for Information Technology—X Window System Graphical User Interface—Part 1: Modular Toolkit Environment," as a minimum, and shall require capability demonstration.*

The following requirement is not part of the OSE specification section. It is included only as an example of specific contract requirements that may be defined by personnel within an acquiring organization. These examples may or may not be relevant to a specific procurement.

User Interface Services Additional Technical Requirements Specifications

> *User interface implementations offered as a result of the requirements of which this is a part shall implement the style guidelines defined in _____ and shall require capability demonstration.*

The blank in the above requirement should be filled-in to include the name of the specification of a style guide for user interface development. The lessons-learned sidebar contains references to two example style guides.

> *User interface implementations based on character-oriented displays offered as a result of the requirements of which this is a part shall provide a means for replacing such interfaces with graphics-oriented displays and shall support the transition to graphics-oriented displays.*

5.1 Instructions to Offerors

Offerors will probably have to demonstrate conformance through means other than validation testing. In such cases, the offeror must be instructed to be prepared for demonstration by submitting a prepared application that illustrates the capabilities of the user interface on the platforms proposed. A good source of HCI evaluation material is contained in the IEEE Working Group P1201.2 draft standard on "drivability."

5.2 Evaluation of Proposals

There are no official validation tests for the X Window System. The X Consortium is in the process of developing a test suite for the library component of the X Window System, but these tests do not illustrate style and actions on-screen. A suggested means of testing the user interface is to establish a script that sends X protocol messages to a server and then visually inspect the responses on the screen as they occur. A checklist for each test may be used to track conformance.

Standards for all services included in HCI services have not been completed. Individual organizations should specify a style guide for use in determining the visual aspects and standard form for application screens, forms, reports, etc. IEEE Working Group P1201.2 is in the process of defining a guide. It is incumbent on the acquiring organization to specify what is required. An example of such a style guide is the Department of Defense Draft "Technical Architecture Framework for Information Management," Volume 7, *Information Technology Standards Guidance—Open Systems Environment (ITSG_OSE)*, Release 1.1.

An alternate style guide is contained in a book by Wilbert O. Galitz entitled *User-Interface Screen Design*, (QED Publishing, Wellesley, Massachusetts, 1993, pp. 512). It provides references to numerous studies and experiments performed on user interface design problems from the past 20 years.

Further evaluations can be made using subjective and objective criteria applied to ease-of-use of different applications supplied with the HCI implementation. Examples of these criteria are described as follows:

Written and programmed guidance and assistance to users in a simple, easy to understand, nontechnical manner.

Screens and function keys that are used in a consistent manner by any executive and other software within the system, and that do not conflict with style guidelines.

Screens and function keys that allow users to customize the operating environment and to save customization information in a user profile that can be invoked at any time.

Features and functionality that aid novice, intermediate, and experienced users in learning and mastering the basic operation of any hardware or software with which users are expected to function. These features shall include the ability for the user to adjust the level of detail for messages, prompts, and screens, as a minimum.

System manuals with comprehensive levels appropriate to the type and experience of users (e.g., user manuals for novice users shall contain extensive graphic presentations [pictures, diagrams, and charts] to aid in rapid learning of and familiarization on system features).

6. SOFTWARE ENGINEERING SERVICES

Most of the specifications included in the OSE pertain to the support of applications. The following requirements provide a means for developing software within the OSE and for specifying the conditions under which software may be developed to execute in the OSE.

Contractors shall propose standard programming languages and language bindings for use in developmental applications provided as required in this contract. Integrated software engineering environments (ISEE) shall also be proposed that support the development of applications in standard programming languages and shall support integrated software engineering methods from initial inception of an application through development and retirement/replacement of the application. Such ISEEs shall operate on one or more proposed platforms within the operating environment required in this RFP.

Software Engineering Services Requirements Reference Specifications

When computer application programs are developed or acquired as a result of the requirements of which this is a part, and one of the FIPS programming languages is specified elsewhere in this contract, only the language elements of that FIPS, as well as any additional language elements specified in this contract shall be used. In these cases, processors used in developing such programs shall be validated as specified in the following requirements.

A procurement may not require all of the programming languages included in this model. Additional information for determining the applicability of various programming languages may be found in NBS Special Publication 500-117 "Selection and Use of General Purpose Programming Languages, Volumes 1 and 2."

Each of the following requirements is written independently of the others in order to facilitate excluding those that are not required for a particular acquisition.

Ada language processors offered as a result of this and other requirements in this contract shall conform to FIPS 119 Ada. These processors shall implement all of the language elements of FIPS 119 Ada and shall require validation.

The following paragraph may be added as a requirement or as an evaluation factor in section M.

In addition, the contractor shall submit Ada Compiler Evaluation Capability (ACEC) results for any and all Ada compilers proposed for use on this procurement. Results shall be submitted for all tests contained in the current version of the ACEC which includes performance tests, symbolic debugger tests, program library manager tests, and diagnostic message tests. The contractor shall also provide documentation which records the

"maintenance switch settings" which were used during the ACEC testing activities. If these switch settings were changed during the course of the testing, then switch settings for each phase or section of testing shall also be identified and provided. The contractor shall also document the test system configuration and the system resources. Test system configuration data shall include host and target identification, single or multi-processor configuration, operating system versions, and other significant configuration elements. Resource descriptions shall include available memory, processor speed (in millions of instructions per second [MIPS]), co-processors used, and other significant components.

C language processors offered as a result of this and other requirements in this contract shall conform to FIPS 160 C. These processors shall implement all of the language elements of FIPS 160 C, and shall implement any additional language elements specified elsewhere in this contract. Such processors shall require validation.

COBOL language processors offered as a result of this and other requirements in this contract shall conform to FIPS 21-3 COBOL. These processors shall implement all of the language elements of the subset and optional modules of FIPS 21-3 COBOL as specified elsewhere in this contract and shall require validation.

FORTRAN language processors offered as a result of this and other requirements in this contract shall conform to FIPS 69-1 FORTRAN. These processors shall implement all of the language elements of FIPS 69-1 FORTRAN, and shall require validation.

Pascal language processors offered as a result of this and other requirements in this contract shall conform to FIPS 109 Pascal. These processors shall implement all of the language elements of FIPS 109 Pascal, and shall require validation.

Integrated software engineering environment (ISEE) implementations offered as a result of this and other requirements in this contract shall provide the functionality defined in the Portable Common Tool Environment (PCTE): Abstract Specification, Standard ECMA-149, European Computer Manufacturers Association (ECMA), and shall require capability demonstration. In addition, ISEE implementations offered shall be compatible with implementations offered for data management services required in [data management section].

Where use of a specification results in difficulty of acquiring implementations, the phrase "shall provide the functionality defined..." is used rather than the more restrictive, "shall implement...". This change will allow implementors to propose other products that function in the same manner as a referenced implementation, and still maintain an open system direction.

The following requires that developmental items (i.e., custom software) and commercial off-the-shelf software be implemented in standard languages.

When computer application programs are developed or acquired as a result of this and other requirements in this contract, and one of the FIPS programming languages is used as the implementation language for such programs, only the language elements of that FIPS, as well

as any additional language elements specified in this contract shall be used. In these cases, processors used in developing such programs shall require validation.

The following requirements are not part of the OSE specification section. They are included only as examples of specific contract requirements that may be defined by contracting personnel within an organization. These examples may or may not be relevant to a specific procurement. Additional information about ISEE can be found in "Reference Model for Frameworks of Software Engineering Environments (Technical Report ECMA TR/55, 3rd Edition)," NIST Special Publication 500-211.

Programming Services Additional Technical Requirements Specifications

ISEE implementations shall provide software engineering tools and interfaces to tools, among which are requirements tools, design tools, program and code analyzers, documentation generator, code generator, test data generator, debuggers, source code editor and formatter, linker, optimizer, cross-reference utility, source dependency listing utility, maintenance tools, and library manager, as a minimum.

The offered ISEE implementation shall provide a testing and training environment that, for all intents and purposes, appears to users as a production environment, but that is isolated from any production environment.

Very high-level languages, such as fourth generation language (4GL) processors and application generators offered shall be required to provide the functionality described in sections 4.1 through 4.9 of NIST Special Publication 500-184, "Functional Benchmarks for Fourth Generation Languages." Contractors shall demonstrate that individual tasks described in the cited publication can be accomplished by the proposed implementation. Such 4GL processors shall be based on and compatible with the pending Xbase specification under development by Standards Committee X3J19.

Xbase is a combination of fourth generation language elements from various commercially available products, including an SQL interface. Standards Committee X3J19 is performing the work on this standard which began in October 1992.

When computer programs are developed or acquired as a result of the requirements of which this is a part, then the contractor shall provide a list of the methods, tools, and techniques used to verify and validate the computer programs during development.

Software verification and validation plans provided with these computer programs shall comply with the requirements in FIPS 101, "Guideline for Life Cycle Validation, Verification, and Testing of Computer Software," and FIPS 132, "Guideline for Software Verification and Validation Plans."

6.1 Instructions to Offerors

Validation certificates or VPL listings should be required for each compiler proposed. In the case of C compilers, those compilers associated with a particular POSIX implementation are not

considered validated unless they have been issued a separate validation certificate from the C compiler testing service at NIST.

Offerors of Ada compilers also have the added requirement of submitting an Ada Compiler Evaluation Capability (ACEC) report.

6.2 Evaluation of Proposals

Compilers that have not been validated should be rejected immediately. There are large numbers of validated compilers on the VPL for virtually every model of every platform. Likewise, compilers that have failed tests should be examined closely.

ACEC reports submitted with Ada compilers should be analyzed for compatibility with the types of applications that will be written in the proposed compiler. For example, a profile of the resource usage of specific existing applications may give an indication how well similar applications will perform if implemented using the proposed Ada compiler.

7. 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.

> *Contractors shall propose data management services including specified interfaces, protocols, and supporting data formats for application level interfaces to data dictionary/directory services, relational database management systems (RDBMS), distributed data services, and data management security as described in the following.*
>
> *Data Management Services Requirements Reference Specifications*

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

> *Data dictionary/directory implementations offered as a result of this and other requirements in this contract shall conform to FIPS 156 Information Resource Dictionary System (IRDS) and shall implement all of the functions defined, and shall require validation.*

The following specification provides a mechanism for an IRDS implementation to be an active IRDS.

> *Application program interfaces (API) to the FIPS 156 implementation shall implement ANSI Standard X3.185-1992 IRDS Services Interface as a minimum and shall require validation.*

This specification provides a mechanism for an IRDS implementation to receive information from and provide information to other dictionary/repository systems, and also to export the information contained in the IRDS.

An export-import facility in support of the FIPS 156 implementation shall implement ANSI Standard X3.195-1991 IRDS Export-Import File Format as a minimum and shall require validation.

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 security interface for granting and revoking privileges does not specify a secure DBMS; only its interface.

The SQL FIPS (FIPS 127-2) defines four levels of conformance:

1. Entry SQL (minimal database management capabilities plus new FIPS SQL requirements, such as integrity enhancement and renaming columns)
2. Transition SQL (entry SQL plus Dynamic SQL, joined tables, date/time data types, union views, implicit casting, multiple schemas per user, referential delete action, insert expressions, explicit defaults, privilege tables, etc.)
3. Intermediate SQL (transition SQL plus domain definition, revoke statement, case expression, unique predicate, schema definition statement, user authorization, long identifiers, full outer joins, scrolled cursors, named character sets, constraint management, etc.)
4. Full SQL (intermediate SQL plus bit data type, assertions, temporary tables, full dynamic SQL, derived tables, row and table constructors, union and cross join, deferrable constraints, session management, full cursor update, etc.)

An additional section on Remote Database Access (RDA) integration is required if RDA is to be used for allowing databases to communicate (includes RDA client and server agents, stored execution, status of actions, etc.). Whichever conformance level is chosen, only one validation is available. Currently, validation is available for entry SQL, but test suites are being developed to provide testing capabilities for transition, intermediate, and full SQL. When a validation certificate is issued to an implementation, it validates the implementation for all levels below and up through the one tested (i.e., a certificate for transition SQL, when it becomes available, will prove validation for both transition and entry SQL).

Further information on selecting database specifications can be found in NBS Special Publication 500-131 "Guide for Selecting Microcomputer Data Management Software." Notwithstanding its microcomputer orientation, much information for consideration in selecting database technology is made available in this publication.

SQL language processors offered as a result of this and other requirements in this contract shall conform to FIPS 127-2 Database Language SQL and FIPS 127-2 Change Number 1. These processors shall implement all of the required language elements of FIPS 127-2, all of the FIPS 127-2 options specified elsewhere in this contract, as well as all default options

required by Section 13 of FIPS 127-2, New FIPS SQL Requirements, and additional requirements as specified in Section(s) [14.1, Transitional SQL, 14.2, Intermediate SQL, 14.3 Full SQL (choose none or one). Integration with RDA as defined in Section 14.4 shall also be required.] Validation shall be required.

RDA provides a mechanism for communicating SQL messages between two relational databases on separate platforms. Other communications capabilities, such as directory services, transparent file access, etc. are also required as specified in the networking services section to support the RDA capability.

If the OSE requirements include distributed database capabilities, several standards must be specified: a database language such as SQL, a protocol for formatting messages between communicating databases such as RDA, and a communications protocol for distributing the messages over a network such as GOSIP or TCP/IP. If a centralized database is required, the RDA component may not be required, but the access (SQL) component and the communications component may still play significant roles.

Distributed database services offered as a result of this and other requirements in this contract shall implement "Remote Database Access (RDA)," ISO/IEC 9759:1993; "Part 1: Generic Model, Service, and Protocol," and "Part 2: SQL Specialization"; and shall require capability demonstration.

Distributed database services offered as a result of these and other requirements in this contract shall interoperate with the proposed ISEE, database implementations, and other tools as appropriate, and shall require capability demonstration.

The following requirements are not part of the OSE specification section. They are included only as examples of specific contract requirements that may be defined by contracting personnel within an organization. These examples may or may not be relevant to a specific procurement.

Data Management Services Additional Technical Requirements Specifications

The contractor shall provide a database management system (DBMS) to implement logical data views independent of the physical underlying data model. The DBMS shall conform to FIPS 127-2.

The DBMS/data dictionary shall maintain and store database descriptions separate from, but available to, applications through an appropriate API. The information stored in this implementation shall be accessible to the IRDS implementation proposed.

The DBMS proposed shall ensure that the full range of tools needed to perform database administration and management, as well as support end-user application generation functionality is provided. As a minimum, such tools shall provide database integrity checking; allocating, initializing, and deallocating physical storage; loading, unloading, reorganizing, and reloading files and parts of files; repairing damaged

information; and logging all transactions selectively before or after the data is updated.

7.1 Instructions to Offerors

Validation certificates should be required for SQL implementations. Validation services are also now available for IRDS. An RDA test method is in development and prototype implementations of RDA are installed in a CSL RDA testbed. Capability demonstration will be required for RDA.

7.2 Evaluation of Proposals

SQL implementations that are not supported by validation certificate or a listing in the VPL should be rejected. Validation for a particular computer family will provide the same basic assurances as for validation on the proposed platforms (i.e., derived validation).

RDA will require capability demonstration. A test implementation will be required to adequately test the functionality of the offered product. Acceptable results should include the ability of an application to locate a central IRDS, request data descriptions from the IRDS, and use these data descriptions in forming a data structure for storing data acquired from a database located on a separate platform. A second test may test the capability of the application to add data to a remote database using the same IRDS and RDA implementations.

8. DATA INTERCHANGE SERVICES

If different implementations of word processors, graphics/drawing tools, imaging tools, etc. are to be used in the context of the applicable systems of a procurement, then multiple specifications from the following may be required to allow file formats to be exchanged among these and other applications.

Contractors shall provide implementations of data interchange services for supporting data formats that provide interchange of documents, graphics data, and product description data between applications as described in the following.

Data Interchange Services Requirements Reference Specifications

Open Document Architecture (ODA) is a framework that enables users to interchange the logical structure, content, presentation style and layout structure (the physical appearance) of documents from one application to another, or from an application to various output devices. ODIF, Open Document Interchange Format, is an ASN.1 (Abstract Syntax Notation One—ISO 8824:1987 and ISO 8825:1987) encoding for documents suitable for interchange between applications. ODL, Open Document Language, is a generic Standard Generalized Markup Language (SGML) encoding for documents suitable for interchange between applications.

ODA/ODIF/ODL can represent complex objects that include different types of contents, such as complex documents with embedded text, graphic images, etc. Typical uses of ODA/ODIF might

include transmitting formatted documents, such as books and technical reports through communications networks from one application to another and then printing or editing the file through various filters (e.g., a text filter, a graphics filter, or a printer driver).

An ODA/ODIF encoded file can be a bitmap representation, a text character representation, or a combination of these and other representations. The physical appearance of the document will normally be maintained throughout the operations of encoding, transmitting, and unencoding. Specific Document Application Profile (DAP) encodings are required to make efficient use of ODA/ODIF, but they are not described in the standard. Users should consult with experts in ODA/ODIF capabilities.

> *Document interchange services offered as a result of this and other requirements in this contract shall implement ISO 8613:1989, "Office Document Architecture (ODA)," and shall require capability demonstration.*

Lesson learned...
The decision whether to use ODA or SGML cannot be answered in this report. A cursory description of the differences between the two is the following: (1) SGML can be used to define the logical structure of a document, whereas (2) ODA can be used to describe both the logical and physical structures of a document. SGML documents can also be described in terms of ODA. GOSIP protocols also define a mapping for ODA. SGML has no such protocol mapping.

SGML provides accessibility to sight-impaired users by meeting international requirements on accessibility of documentation. In this situation, SGML is the preferred specification, although ODA can be used to represent SGML documents.

SGML document processors are now available for numerous word processing applications.

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. Users will normally not use SGML. Instead, they may use Document Type Definitions (DTD) that prescribe consensus-based sets of tags for use in document preparation. These DTDs are defined in terms of SGML grammars.

> *Standard Generalized Markup Language (SGML) systems offered as a result of this and other requirements in this contract shall implement the requirements in FIPS 152 SGML and shall implement all of the language elements of SGML, and shall require capability demonstration.*

An SGML test suite is in beta testing. Once testing procedures have been developed and test laboratories have been accredited, a full SGML testing program will be available. The current schedule projects the program to be in place by early 1995.

CGM standardizes the representation of 2-dimensional graphical data for interchange. The CGM is a device independent format containing vector graphics information and raster graphics information.

All computer graphics metafiles (CGM) acquired to store, and communicate graphical information among different applications, devices, and computer systems shall conform to FIPS 128-1 CGM and shall require validation.

All three components of a CGM system, (i.e., generator, metafile, and interpreter) can be validated. The computer graphics metafiles that are produced by a CGM generator (application) are tested to verify that they contain valid information. CGM generators are tested to verify that they can produce valid metafiles that accurately and correctly represent the intended picture. Interpreters are tested to verify that they can correctly and completely read the metafile and produce the intended picture. These tests result in three separate certificates.

All generators, metafiles, and interpreters acquired shall conform to an application profile. FIPS 128-1 requires the use of MIL-D-28003 "Military Specification: Digital Representation of Communication of Illustration Data: CGM Application Profile" for use in technical illustrations and publications, and when the use of a general-purpose, graphical interchange mechanism is required.

Initial Graphics Exchange Specification (IGES) standardizes the representation of specific types of complex graphic objects and attributes for product 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 manufacturing (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. An IGES test suite is in beta testing and an IGES validation test service is planned for 1995.

Product data interchange services encompassing 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 offered as a result of these and other requirements in this contract shall implement FIPS 177 Initial Graphics Exchange Specification (IGES) and shall require capability demonstration.

"Standard for the Exchange of Product Model Data (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).

Product description lifecycle services offered as a result of these and other requirements in this contract shall conform to Draft Proposed ISO 10303 "Standard for the Exchange of Product Model Data (STEP)" and shall require capability demonstration.

NIST is researching a test bed for performing product model data testing, including STEP data, for the Department of Defense's JCALS Program. While this is still in developmental stages, results of research should provide more input to the testing process in the near future.

Electronic data interchange (EDI) specifies 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. Such 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.

The decision to use EDI and the particular set of standards involved (e.g., X12, or EDIFACT, or both) is usually made at the Chief Information Officer (CIO) or Director of Information Resources Management (IRM) levels and above. This decision entails more than selecting EDI as the electronic data interchange standard. It also involves agreements between the agency and its trading partners in determining which transaction sets (i.e., syntax, message, data element, data segment, and document type standards) should be used. For example, an agency that is involved in submitting environmental information to another agency may agree to submit this information, and the receiving agency to receive the information, according to a particular transaction set under EDI that has been developed by an environmental industry group. This same agency may use a different transaction set developed by an agency of a foreign government to converse with the foreign government on other types of information, such as registration and manifests for international transportation of cargo. A set of transactions must be agreed upon between electronic trading partners for particular purposes; each set of partners may agree on a single or multiple transaction sets, depending on the applicable standards under EDI for those applications of interest.

X12, the standards committee responsible for the EDI standard, has passed a resolution to adopt the European EDIFACT standards by 1997. The current X12 standards will evolve in this direction. Where applicable, new systems should provide EDIFACT transaction sets.

> *Electronic Data Interchange (EDI) services offered as a result of these and other requirements in this contract shall conform to FIPS 161-1 EDI and shall require capability demonstration.*

Standard Page Description Language (SPDL) defines a language for representing images that are to be displayed on a screen, printed on an output device, or transmitted through communications media from one application to another. To support the interchange of SPDL documents in a variety of environments, SPDL provides two document representation formats: a binary interchange format and a clear text interchange format. This standard is intended to be used for documents that are generated by any text processing system. It is particularly applicable to (1) documents that are intended for electronic printed output; (2) documents viewed on windowing systems; and (3) documents that are interchanged among systems with differing text output devices.

Standard Page Description Language (SPDL) services offered as a result of these and other requirements in this contract shall conform to ISO/IEC DIS 10180 and shall require capability demonstration.

Data Interchange Services Additional Technical Requirements Specifications

The contractor shall provide word processing, spreadsheet, personal information manager, personal database, presentation graphics, and other office automation software that imports and exports information in a mix of the formats required in subsections relating to data interchange.

Word processors shall import and export text and page information in SGML form as a minimum, and optionally in ODA form.

Word processors shall print text in properly constructed SPDL form as a minimum.

Presentation graphics processors shall import and export text and graphics information in CGM or SPDL format, or both.

8.1 Instructions to Offerors

Offerors should be required to provide validation certificates for any implementations of CGM. Other implementations, such as EDI, SGML, etc. will require some form of capability demonstration. In these cases, offerors should be asked to construct test files and read these files by each implementation that is purported to have the corresponding capability. A second test should be conducted to show that a standard format file can be created using the appropriate implementations.

8.2 Evaluation of Proposals

Commercial-off-the-shelf (COTS) software is available for producing many of these file formats. Any errors found during reading of specific formatted files should be evaluated to ascertain what effects they will have on the overall usability of the offered products.

9. GRAPHICS SERVICES

The question of whether to use standard graphics implementations, such as PHIGS, or the human/computer interface (HCI) specification, X Window System, in user interfaces has been posed often. These two service areas are separate because they are different services. They have similarities in the ability to display graphic images and provide application program interfaces for drawing various types of graphical devices, but human/computer interface services also provide the protocols for connecting client and server agents in a network and provide application control over the interactions with the HCI input-output device, normally the CRT. Graphics services apply to a separate type of application, namely applications that are used for technical drawings in two and three dimensions. Graphics services apply to those applications that also have to manage the graphics data used to support the drawing of graphic images. The decision reduces to this: if requirements call for control over the input-output device or for client-server capabilities, then X Window System is the specification to use. If requirements include two and three dimensional technical drawing capabilities and management of the data to support these drawings, then graphics services specifications, such as Programmer's Hierarchical Interactive Graphics System (PHIGS) and Graphical Kernel System (GKS), should be chosen.

> *The contractor shall include services, interfaces, protocols, and supporting data formats that provide two- and three-dimensional graphics development and viewing, interactive graphics, graphics data management, and graphics software and data security functionality as described in the following specifications.*
>
> *Graphics Services Requirements Reference Specifications*

The following specification fulfills the requirement for a language to program two-dimensional graphical objects that will be displayed or plotted on appropriate devices (raster graphics and vector graphics devices).

> *All two-dimensional graphics libraries/packages to be used as a programming interface to application programs offered as a result of these and other requirements in this contract shall conform to FIPS 120-1 GKS. These two-dimensional graphics libraries/packages shall implement all of the requirements of FIPS 120-1, and in the case of C or Fortran bindings shall require validation.*

The current language bindings for GKS consist of those defined for Ada and FORTRAN. Separate validations for C and FORTRAN are available and should be specified as required.

The PHIGS specification fulfills the requirement for a language designed 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.

> *All computer graphics software toolbox packages acquired to support very highly interactive graphics applications, or graphics applications needing rapid modification of both the graphics data and the relationships between the graphical data shall conform with FIPS 153-1, the Programmer's Hierarchical Interactive Graphics System (PHIGS). In addition,*

such toolbox packages shall support, as a minimum, one of the programming language bindings as specified in the FIPS, and in the case of C or Fortran bindings shall require validation.

Graphics Services Additional Technical Requirements Specifications

No additional graphics services are specified in this model.

9.1 Instructions to Offerors

Validation certificates should be required for both GKS and PHIGS implementations. If Ada or FORTRAN are part of the required languages, then validation for GKS should be required using the language specified in the requirements.

9.2 Evaluation of Proposals

Before rejecting any implementations that are not validated, check the VPL to determine if a number of products are available on the platforms submitted. If an agency determines that sufficient products are available, then nonvalidated implementations should be rejected.

10. COMPUTER NETWORK SERVICES

NIST is issuing a proposed revision to the Government Open Systems Interconnection Profile[4] (GOSIP) FIPS 146-1 which removes the mandate to acquire only Open Systems Interconnection (OSI) technology to provide interoperability between heterogeneous computer systems. The proposed revision renames GOSIP as "Profiles for Open Systems Internetworking Technologies" (POSIT) and strongly encourages the acquisition of nonproprietary technology, such as OSI and the Internet Protocol Suite (IPS) to provide interoperability between different systems.

Lesson learned...
In any procurement involving communications, full analysis must be given to the communications requirements. This area is too complex to state requirements in a single paragraph, no matter how small or large the procurement. As an example, many agencies assume it is enough to specify a single FIPS as the communications requirement. In reality, communications specifications contain a selection or profile of specifications that have to be carefully chosen in order to attain interoperability.

The Government Network Management Profile (GNMP) is the standard network management reference for all Federal Government agencies. Its use is optional when acquiring network management functions and services for computer and communication systems and networks.

[4]The proposed revision is tentatively planned as FIPS 146-2 and is in public review as of the time of this report's publication.

Network management functionality offered as a result of these and other requirements in this contract shall conform to FIPS 179, "Government Network Management Profile (GNMP), Version 1.0," and shall require capability demonstration.

Transparent file access includes capabilities for managing files and transmitting data through heterogeneous networks in a manner that is transparent (i.e., does not require knowledge of file location or of certain access requirements) to the user.

Transparent file access services offered as a result of these and other requirements in this contract shall conform to IEEE P1003.8, "Transparent File Access (TFA)," and shall require conformance demonstration.

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. Open Software Foundation's Remote Procedure Call (OSF RPC) includes support for naming, dynamic binding, and security (authentication, data privacy, and integrity protection). An API for OSF RPC is defined.

Distributed computing functionality offered as a result of these and other requirements in this contract shall conform to OSF/1 "Distributed Computing Environment (DCE)—Remote Procedure Call (RPC)," and shall require capability demonstration.

In addition, such products offered shall interoperate with and support FIPS 151-1 POSIX, and shall require capability demonstration of this interoperability as specified elsewhere in this contract.

A general requirement is that communications shall execute transparently to the users and shall provide programming interfaces at the application layer where appropriate as a minimum. Additional requirements may augment these requirements as specified elsewhere in this contract.

IGOSS

Users should review NIST Special Publication 500-217, "IGOSS-Industry/Government Open Systems Specification," to determine its impact on organizational requirements and its applicability to specific acquisitions.

IGOSS defines a profile of Open Systems Interconnection (OSI) protocols that updates the technical specifications in FIPS 146-1. IGOSS encompasses the requirements for functionality that include message handling systems (MHS), electronic data interchange (EDI), File Transfer Access and Management (FTAM), Virtual Terminal services (VT), directory services, remote database access, transaction processing, X-windows over OSI, Fiber Distributed Data Interface (FDDI), Frame Relay, and Point-to-point Protocol (PPP).

Following is a summary of standardized communications application programming interfaces (API) and corresponding recommended procurement language.

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. Draft Version 2.0 will consist of a low-level interface specification.

The Detailed Network Interface (DNI) specification in IEEE P1003.12 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 OSI 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.

> *Process communication interfaces proposed shall provide the functionality defined in Protocol Independent Interfaces (PII) IEEE P1003.12 and shall require capability demonstration.*

The following specification provides an API between applications and the OSI Association Control Service Element (ACSE) and presentation services.

> *OSI ACSE/Presentation Application Program Interfaces proposed shall provide the functionality defined in IEEE P1238 and shall require capability demonstration.*

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

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

Recommended Communications Procurement Strategy

In late 1993, CSL formed a task group to recommend a plan of action for tackling computer communications in the future. The task group was formed as the Federal Internetworking Requirements Panel (FIRP) and prepared a draft report on its findings in February 1994. The final report was published in August 1994.

The crux of the report was summed up in the following: "The Panel concluded that no single protocol suite meets the full range of government requirements for data internetworking. Both the Internet Protocol Suite (IPS) and Open System Interconnection (OSI) have strengths and weaknesses, as do proprietary protocols. While a single standard would be preferable, the reality is that there are multiple solutions in networking as in other areas of information technology." Accordingly, agencies should evaluate implementations based on their requirements giving priority to standards-based solutions.

Video, voice, and data communications can be integrated through the use of protocols that can coexist on digitally-switched telephone systems. Users should check the date of the latest North American ISDN Users Forum (NIUF) Agreements. This information can be obtained from the NIUF coordinator at NIST.

Integrated video, voice, and data communications proposed shall implement the protocols defined in FIPS 182, "Integrated Services Digital Network."

X.400 provides electronic mail interoperability among heterogeneous computer systems. X.400 is an international standard protocol definition. The X.400 API defines a human/interface of a mail system. IEEE P1224.1 is a language-independent specification.

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

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.

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

The following requirements are not part of the OSE specification section. They are included only as examples of specific contract requirements that may be defined by contracting personnel within an organization. These examples may or may not be relevant to a specific procurement.

Computer Network Services Additional Technical Requirements Specifications

The contractor shall provide, deliver, install, and test communications software to implement intersite and intrasite communications requirements, via appropriate infrastructure components, common carrier, and other transmission media. Traffic volumes to be accommodated by the communications software will be identified in a baseline inventory (see [Baseline Inventory]). The communications software shall provide the following:

Detection, isolation, and correction of faults; monitoring usage; and recording significant events at the installation, system, network, and subnetwork levels.

Multiprocessing and multitasking in order to exchange information with remote computers or application systems while the operator concurrently performs application processing.

Operating in an unattended mode (e.g., where no operator is present) to exchange information with other computers or application systems.

Interfacing with the communications software employed by applications that are outside the scope of this contract but which exist within the organization or are required for communicating with the organization's external environment.

Interfacing and interoperating with contractor-provided and organizational telecommunications hardware as described in the baseline inventory.

Security features shall be provided through the use of network access control software and system security software in accordance with security guidelines of the National Security Administration (NSA) and NIST. (Draft security guidelines are available through CSL's Security Division.)

Network management software shall be provided for network and security monitoring and managing the network infrastructure, allowing systems personnel to administer the network effectively. Further functionality shall include the following:

Transferring files between any organizational platforms using POSIT-compliant products.

Assisting the network administrators in installation and configuration of the network, operating and maintaining the network, managing performance, and planning for network growth and evolution.

Use existing protocol suites (as described in the baseline inventory) with the following options and additions:

A Simple Network Management Protocol (SNMP).

A Common Management Information Protocol (CMIP) and Common Management Information Services (CMIS) protocol using described managed objects in accordance with ISO/IEC 10165-4.

Fault detection and isolation.

Centralized network configuration.

Monitoring and testing without disruption where possible.

Continuous monitoring.

Flow and congestion control.

Maintenance of a centralized file of registered network object names and associated networks.

Gathering and analyzing usage data for all managed objects within the network and subsequently making this data available for charge-back or usage accounting on a user, account, and group basis.

Software to calculate subnetwork channel utilization and traffic flow among subnetworks in frames and bytes per second shall be provided and shall execute on the proposed platforms.

Remote access to all network management system functions by authorized users across the network.

Network initialization.

Identify the functionality for consumer and server relationships.

Identify changes to logical Internet Protocol (IP) addresses for individual network nodes.

Wide area network (WAN) functionality shall be provided using Government long haul networks, such as FTS 2000.

Local and wide area networks (LAN/WAN) products offered shall use existing infrastructure where feasible. Where existing infrastructure cannot be used, the contractor shall provide rationale for this decision.

Network functionality shall support data transfer synchronously and asynchronously at the program's discretion between a host computer and attached terminals.

Other communications specifications, such as TCP/IP (see the following specifications), would be located in this section.

Network functionality shall support existing communications that are based on the TCP/IP protocol suite, including the following specifications:

"Internet Protocol" RFC 791, "Internet Standard Subnetting Procedure" RFC 950, "Broadcasting IP Datagrams" RFC 919, and "Broadcasting Internet Datagrams in the Presence of Subnets" RFC 922.

"Internet Control Message Protocol" RFC 792.

"Host Extensions for IP Multicasting" RFC 1112.

"User Datagram Protocol" RFC 768.

"Transmission Control Protocol" RFC 793.

"TELNET Protocol Specification" 854 and "TELNET Option Specifications" RFC 855.

"File Transfer Protocol" RFC 959.

"Simple Mail Transfer Protocol."

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

"Content Type Header Field" RFC 1049.

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

"Domain Names—Concepts and Facilities" RFC 1034 and "Domain Names—Implementation and Specification" RFC 1035.

"Mail Routing and the Domain System" RFC 974.

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

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

"Concise MIB Definitions" RFC 1212.

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

"Exterior Gateway Protocol" RFC 904.

10.1 Instructions to Offerors

Offerors should be required to submit registration of standards-based communications products. Not only should software implementations be registered, but any hardware components submitted with integral communications software, such as gateway platforms, should be registered. The acquiring agency should check the current registration database for registered means-of-test (MOT) and abstract test suites (ATS) used. Often, a MOT is not available for testing a particular protocol, in which case, no registration for the protocol in question may be available.

Lesson learned...
Note that communications registration testing is particularly expensive in comparison to other validation testing. Conformance demonstration for cases where communications tests do not exist is even more expensive and complex. Not only does a test for the protocol of interest need to be developed, but also for the underlying protocols.

Registration in most cases must consist of testing a complete suite of protocols. It is not sufficient to test a single protocol within a communications stack. For each registered protocol, the underlying protocols must also be included.

Implementations of other communications specifications should be tested through capability demonstration. Offerors should be required to prepare tests that show the functionality of an implementation under a particular standard.

Additional registration should be required for communications interoperability test results. These test results specifically state that the proposed implementation has successfully physically communicated messages to another implementation from a different vendor across a network.

10.2 Evaluation of Proposals

For each protocol stack submitted, registration should be indicated. Each attachment to the network, such as gateways, network printers with embedded communications, etc., should be accompanied by VPL registration. A report of interoperability should be included for each component, both hardware and software, that will be connected to the network. This report should indicate how the hardware and software were tested, how many and what types of files were used to show interoperability, and the applications that were used for communicating and using the files. Additional information may include detailed specifications of the protocols used by both the sending and receiving components in the interoperability test.

Overall emphasis should be placed on the capability of applications to access remote data files without error through various configurations and combinations of networks.

Agencies should conduct end-to-end testing to determine interoperability at the application level for all protocol suites offered, regardless of other validation and interoperability testing performed.

11. SECURITY SERVICES

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

Security Services Requirements Reference Specifications

> *Operating system security services offered in support of FIPS 151-2 implementations shall implement the functionality defined in IEEE P1003.1e, "Security Interface for the Portable Operating System Interface for Computer Environments," and shall interoperate with and support security measures specified for access control as defined in National Computer Security Center Standard NCSC-STD-020-A, and password management as defined in NCSC-STD-002-85, and shall require capability demonstration. Additional security requirements may be specified elsewhere in this contract.*

The preceding paragraph will require augmentation since some of the functions in the IEEE P1003.1e Security specification are not yet fully defined or are unstable.

Network security features shall be provided in accordance with the selected guidelines in NIST Special Publication 800-4 "Computer Security Considerations in Federal Procurements." The selected security requirements from NIST Special Publication 800-4 include the following: (The acquiring agency would insert the appropriate sections of Special Publication 800-4 at this point. There are requirements in the publication too numerous to discuss in this report.)

A useful source of standardized solicitation wording for security requirements is the National Computer Security Center's (NCSC) technical guide, NCSC-TG-024, "A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work—An Aid to Procurement Initiators," dated June 30, 1993.

Another source of information on security requirements specifically for distributed systems is the IEEE P1003.22 draft "Distributed System Security."

The data/message authentication provided by [the system or specific part of the system as defined in the statement of work] shall be accomplished using message authentication codes as defined by FIPS 113, "Computer Data Authentication," and shall require validation.

The electronic signature capability provided by the system or specific part of the system as defined in the statement of work shall be accomplished in accordance with FIPS 113 and shall require validation.

The key management provided by the system or specific part of the system as defined in the statement of work shall be accomplished in accordance with FIPS 171, "Key Management Using ANSI X9.17."

The design, implementation, and use of the cryptographic module provided by the system or specific part of the system as defined in the statement of work shall conform to FIPS 140-1, "General Security Requirements for Equipment Using the Data Encryption Standard," Level [insert level] and shall require validation.

Security Services Additional Technical Requirements Specifications

Contractor multi-user systems used to process data under this contract shall use the following pre-logon warning message:

```
THIS COMPUTER IS OPERATED BY/FOR THE U.S. GOVERNMENT.
UNAUTHORIZED ACCESS TO AND/OR USE OF THIS COMPUTER SYSTEM IS A
VIOLATION OF LAW AND PUNISHABLE UNDER THE PROVISIONS OF 18 USC
1029, 18 USC 1030, AND OTHER APPLICABLE STATUTES.
```

After contract award, the Contractor shall examine sensitive and critical databases and files, and shall develop a list of data security techniques and methods for review. At a minimum, this list shall include:

Access control, integrity controls, and backup procedures

Data element documentation

Sensitive data procedures and implementation

Existing privacy policies and protections

Data access including authorization and implementation

Application software and how applications are moved into production

Written user responsibilities for management of data and applications

Direct access storage device (DASD) management techniques and the impact on user file integrity

After contract award, the Contractor shall examine the specific operating systems proposed and required in this contract. This examination shall, at a minimum, include:

Review of the operating system and its installation

Review of identification and authentication techniques

Backup and restore procedures

Review of system exits

Verification of audit trails

Review of handling and availability of system logs

Identification of change control procedures (installation of new software releases)

Procedures which ensure that software patches are kept current

Review of installation for integrity

Review of interfaces to access control package (if installed)

Identification of primary access control software and files and procedures for ensuring that all software runs under its control

Review of access authorizations for appropriateness and completeness

Review of interfaces with the access control package for integrity.

After contract award, the Contractor shall review the system development life cycle (SDLC) used to manage application development and maintenance. This review shall minimally include:

Methods for developing and documenting application controls

Adherence to SDLC, including

A review of quality assurance and testing procedures

Change control procedures for corrections and enhancements

Procedures which ensure that software patches are kept current

System documentation and security standards and adherence to both

Updates to all system documentation

Application operation and access to applications.

For controlled access protection of systems, security requirements at the C2 level as defined in section 2.2 of DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," (the Orange Book) shall apply and are incorporated in this solicitation by reference.

Agencies are responsible for ensuring that information resources are adequately protected. One method to meet this responsibility is periodic certification and accreditation of sensitive systems. OMB Circular A-130, Appendix III requires agencies to conduct periodic audits or reviews of sensitive applications and to recertify the adequacy of safeguards. It specifies that this be done at least every three years and that audits and reviews be considered part of the agency vulnerability assessment and internal control reviews conducted in accordance with OMB Circular A-123.

Security certification is a technical review made as part of, and in support of, the accreditation process. Certification shows the extent to which a particular computer system or network design and implementation meets a pre-specified set of security requirements. It also produces a judgment and statement of opinion that the accrediting official can use to officially accredit the system.

Accreditation is the authorization and approval granted to a system or network to process sensitive data in an operational environment. Accreditation is based on a certification by designated technical

personnel that a system's design and implementation meet security requirements and achieve adequate application security commensurate with the risks in the application's environment.

11.1 Instructions to Offerors

A useful source of standardized solicitation wording for security proposal instructions is the National Computer Security Center's (NCSC) technical guide, NCSC-TG-024, "A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work—An Aid to Procurement Initiators," dated June 30, 1993.

11.2 Evaluation of Proposals

The guide listed in section 11.1 provides evaluation information for use in security proposal submissions.

12. MANAGEMENT SERVICES

System and network management capabilities are required to perform tasks associated with managing the resources that are available within a network of various resources and platforms. They provide the mechanisms to monitor and control the operation of individual applications, databases, systems, platforms, networks, and user interactions with these components.

System Management Services Requirements Reference Specifications

System management services offered in support of FIPS 151-2 implementations shall implement the functionality defined in IEEE P1003.2-1993 in a manner that is compatible with current technology and other requirements described in this contract, and shall require capability demonstration. Contractors shall also certify that implementations shall interoperate with generally accepted implementations within the OSI Network Management Framework and shall require capability demonstration.

The neighboring text provides an example of a mechanism for including requirements in the RFP that are based on specifications that will become standards or that are other than standards.

The preceding requirement identifies text that should be incorporated for any known work-in-progress specifications that may have an effect on the primary specification (in this case FIPS 151-2) and may be utilized over the life of the contract.

FIPS 187 is a management specification for the telecommunications infrastructure of commercial buildings. "Administration Standard for the Telecommunications Infrastructure of Federal Buildings" specifies the administrative requirements of the telecommunications infrastructure within a new, existing, or renovated office building or campus. Telecommunications infrastructure can be thought of as the collection of those components (telecommunications equipment spaces, cable pathways, grounding, wiring, and termination hardware) that provide the basic support for the

distribution of all information within a building or campus. Administration of telecommunications outlet boxes, connectors, cables, termination hardware, patching and cross-connect facilities, conduits, other cable pathways, telecommunications closets, and other spaces.

Telecommunications infrastructure administration shall be provided and shall implement the functions and capabilities defined in FIPS 187, "Administration Standard for the Telecommunications Infrastructure of Federal Buildings."

Other system administration specifications have not been recommended. NIST is evaluating the feasibility of recommending IEEE P1387.2, .3, and .4 for software, user, and print management. These specifications, however, are still incomplete and in a great state of flux.

A system administration facility shall be provided and shall implement system administration functions to allocate the use of system resources by individual user, by class of users, and by application. As a minimum, the resources that shall be available for allocation are CPU time available, disk space available, relative priority for CPU access, input and output time available, and input and output volume available.

12.1 Instructions to Offerors

Validation is not available for system administration functions. Capability demonstration should be required. Offerors should be required to submit a script that illustrates the functions required in the RFP and any related specifications.

12.2 Evaluation of Proposals

The system administration script should include tests to illustrate all of the capabilities required in the RFP and those additional capabilities required in any associated specifications, such as IEEE 1003.2-1993, and IEEE P1003.12.

13. NONSTANDARD PROFILE SPECIFICATIONS

This section describes how the acquiring agency should define where other nonstandard specifications are to be identified and used. These specifications could be grouped into a so-called nonstandard profile.

In instances where services, protocols, program interfaces, or data formats are required, but specifications have not been explicitly defined in this contract, the contractor shall propose specific implementations and cite the specifications used. In addition, the contractor shall provide a transition plan for moving to the proposed implementations (if different from existing implementations), a risk/cost/benefit analysis of each proposed implementation, and rationale for proposing a specific implementation as opposed to other available implementations. The contractor shall explain and document what effects such transition will have on the long-term implementation of an OSE and how the contractor shall transition

from the proposed implementation to an OSE when a standard specification becomes available.

14. HARDWARE REQUIREMENTS

Everything to this point has been defined in terms of generally available standards and other specifications that the acquiring agency deems appropriate. Additional requirements are defined by the acquiring agency to augment and tailor the use of the identified specifications and standards. The combination of these two types of specifications can be called the organization's *standard profile.*

Open systems are designed to operate independently from the underlying hardware. There are, however, requirements pertaining to hardware that stem from functional needs rather than from any specific open system requirements. This section is used to define those hardware requirements having an impact on the procurement. Though not extensive, the following examples of such requirements illustrate the concept.

All monitors on user platforms shall provide 256 colors and a 14 inch diagonal viewing area measured from the upper left-most pixel to the lower right-most pixel, as a minimum.

All monitors on non-user platforms (e.g., network servers, test equipment, etc.) shall provide black-and-white, or amber-and-black, or green-and-black screens with a 14 inch diagonal viewing area as defined above, as a minimum.

All monitors on development platforms shall provide 256 colors, graphics, and a 20 inch diagonal viewing area as defined above, as a minimum.

All user and development platforms shall provide 3-key mouse, trackball, or thumbball for controlling cursors and human/computer interfaces. Such devices shall provide functionality for changing operating parameters, such as tracking speed, sensitivity, cursor form, etc.

The contractor shall consider satisfying hardware requirements from Government-Owned Equipment (GOE) and interfaces to existing GOE. The use of this equipment will be at the option of the Government.

Accessibility of systems shall be provided to prevent discrimination against users who have abilities other than average, such as individuals who are sight-impaired or who are impeded by other physical impairments.

Voice input and output devices and braille output devices shall be provided to implement accessibility for sight- and hearing-impaired operators and users.

Other types of standards, such as those used to implement physical connections among telephones, electrical components, etc. are also specified in this section. Examples of such specifications may include RS-232-C, RJ-11, RJ-45, SP-2840, etc.

FIPS 187, "Administration Standard for the Telecommunications Infrastructure of Federal Buildings," also provides references to specifications for wiring standards to support telecommunications infrastructure in federal buildings. An examination of FIPS 187 may identify other elements of hardware that may require further specification within an RFP.

Specifying too many low level minimum hardware requirements may lead to a risk of limiting the degree of interchangeability and openness of the hardware configuration. If these requirements are needed by the acquiring agency, the degree of openness should be an evaluation factor.

15. TRANSITION PLANS

The transition from closed, proprietary systems to open systems will usually take place in a series of phases. Because much of the transition plan is unknown at the outset, such as the technology to be used to replace existing infrastructure in 5 or 10 years, it is impossible to complete a full transition plan in the early stages of the procurement. To be clear, when a contract is awarded for transition services (i.e., planning, analysis, design, and implementation of a transition plan covering multiple years), the capabilities of the successful contractor on the day of contract award are the most critical in evaluation. Future plans become secondary in implementing the transition, but they provide valuable information to evaluators in determining if the contractor is aware of technology developments and how they might affect transition in the long term. This section discusses requirements for transition *after* contract award. In planning for transition services acquisition, the following requirements would apply to the development of a complete transition plan by the contractor, including defining the current baseline, the projected OSE, and the planned paths for obtaining intermediate objectives between the baseline and the OSE.

In general, transition performed by a contractor should be the implementation of a plan such as the following:

a) Upgrade the current baseline to a level of measurable conformance. As an example, standardize on one local area network implementation. This reduces the number of configurations an organization must keep track of and manage. Establishing configuration control of this baseline is necessary to determine where, how, and when specific transition changes should take place.

b) Select specific functions or organizations for implementation of selected technology. For example, replace all existing communications management capabilities with SNMP, or replace different types of databases with SQL databases. Record all changes in the configuration.

c) Establish a technology evaluation group to look at possible technologies, evolving standards, and issues requiring resolution for the future and how they would fit into the transition plan. This group would make recommendations to the contractor for further research into inclusion in intermediate targets.

d) Iterate steps a and b, gradually molding the existing baseline into the objective OSE.

Section L should provide for the offerors to submit an outline of the transition plan and proposed major tasks. A possible method of evaluating a particular offeror's proposal may include analysis of a model site plan with transition to the offeror's proposed implementation based on the model.

After contract award, the contractor shall provide transition plans for accomplishing the move from the current environment to the OSE in an orderly and controlled manner. In particular, where nonstandard specifications are referenced, such as draft standards and other public specifications, the contractor shall provide a method and plan for transitioning from the proposed implementation to a future FIPS implementation when such FIPS has been accepted, and shall certify that transition shall be implemented and complete within 12 months from the date of acceptance of such FIPS, unless otherwise specified elsewhere in this contract. Validation testing shall be accomplished by the contractor according to the requirements in section [Validation].

Some parts of the transition plan, such as baseline configurations, may be supplied by the acquiring agency. In those cases, the appropriate requirements in this section may be reworded or removed.

Transition planning and implementation can "make or break" the move to an open system environment. It would be difficult to require the offerors to submit a full-scale transition plan for the transitioning of systems required in the RFP before contract award, but an alternative is to require the offerors to describe previous experience with transition planning and implementation. The idea is to allow the acquiring agency to evaluate the type and extent of experience gained individually by the offerors.

Alternately, the agency could describe more of the details of existing systems within the RFP or annexes, and require the offerors to submit an overall, high-level transition plan without going into the details of transition implementation. The details of implementation would be filled-in by the contractor upon site inspection or other required analysis phases and would hinge upon acceptance by the acquiring agency.

In general, transition plans shall include tasks for development and use of a baseline environment definition and analysis; specification of an objective OSE architecture; development of an overall strategy for schedule, milestones, and deliverables during transition; and development of implementation plans for intermediate targets. The Transition Plan shall address each of the following goals and shall describe how the contractor will implement and manage the transition process in light of these goals.

Eliminate unnecessary dedicated systems and emphasize common user systems and services.

Provide for management and control visibility, and accountability.

Provide data management support and data standardization as a separate and independent entity. Promote the use of standard data elements in all automated systems and maintain data dictionaries as a management and standardization tool.

Identify the proper technical approach and architecture with which all automation and application systems will be designed as the environment evolves over time from its current baseline to the objective environment.

Devise the software development methodology for the organization's application systems through a minimum of five years from date of award, that will provide modular applications that are effective, reliable, maintainable, and offer a high potential for reuse.

Consolidate existing organizational data processing installations where feasible.

Develop the procedures required to incorporate technology insertions and deletions as they occur and are appropriate.

Minimize user disruptions.

Develop provisions for using and integrating current baseline assets.

Minimize operational impacts resulting from communications service failure.

Ensure that security is an integral part of the architecture.

Strategies for acquiring transition services that have been used by agencies based on available funds, scope of the effort, time constraints, etc. include the following:

- The contractor is required to deliver a transition plan only; or
- the contractor delivers a transition plan and then is required to manage the transition for the acquiring agency; or
- the contractor provides the transition plan, the management, and all implementation including the installation of new infrastructure.

Such choices allow the acquiring agency to remain flexible and to take advantage of opportunities as they arise.

15.1 Baseline Definition and Analysis

A baseline inventory of items may be made available to prospective offerors if the organization has already developed one. To do so would probably be the best alternative to having to pay for a contractor to develop an inventory. To that end, the following requirement is optional.

After contract award, the contractor shall define, through appropriate measures, such as site visitation and inventory, and analyze the baseline configuration of current systems to determine how best to proceed with transition to the OSE, and shall provide specific recommendations based on this analysis.

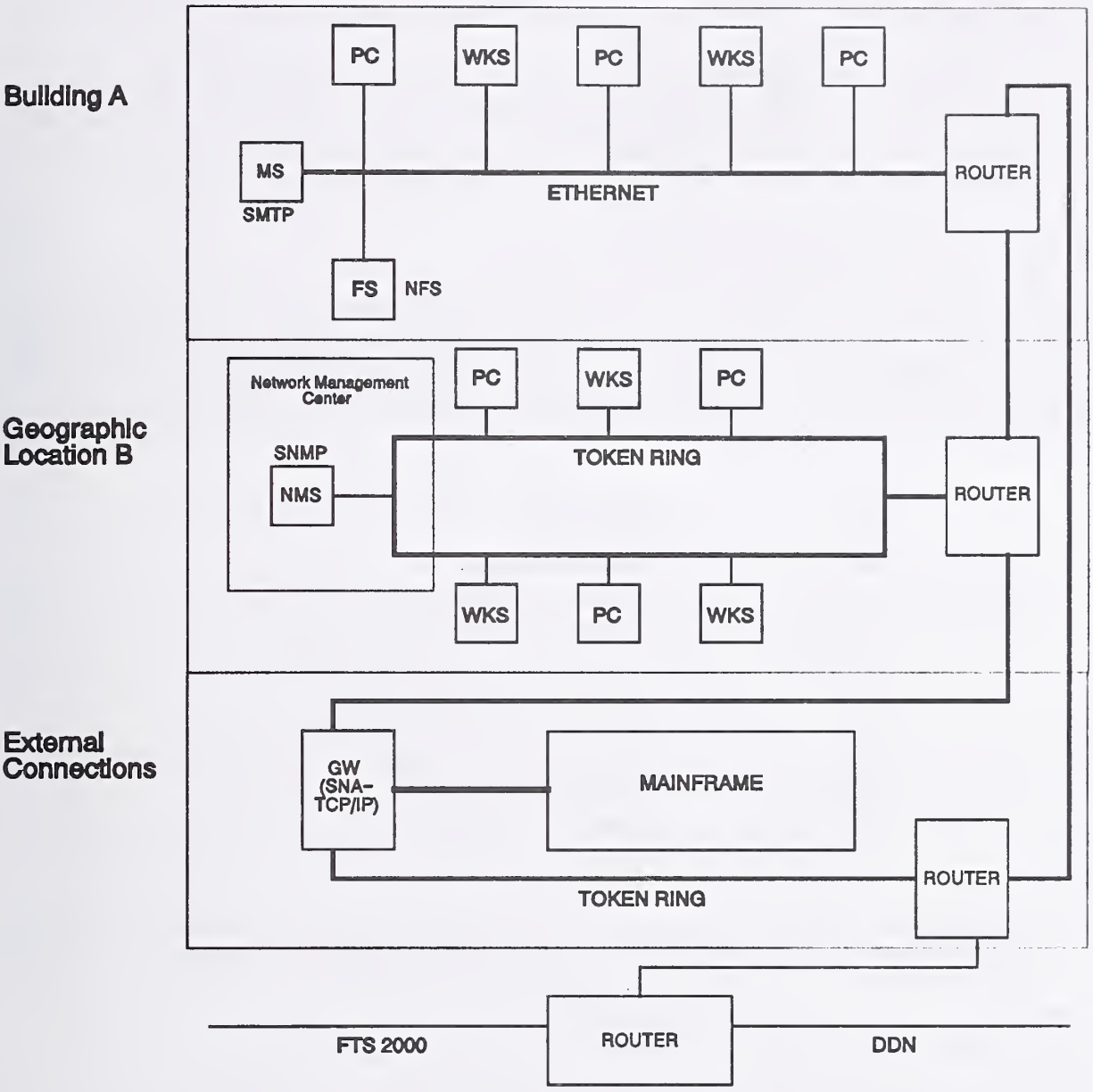


Figure 4. Sample Baseline Configuration Diagram.

After contract award, the contractor shall develop the complete baseline inventory of items including all platforms, communications, and other hardware used in the support of current systems; all software installed, and all data managed by any system within any current configuration; external system interfaces that produce information used by, or use information produced by, the baseline systems; and organizations responsible for each item. Appropriate characteristics of these inventory items, such as transaction volumes, usage statistics, capacities, error histories, maintenance histories, and other measures of software usability and maintainability, shall be included in the baseline. Problem areas, enhancements to existing systems, redundancy (planned or otherwise), and plans for new systems shall be

identified in the analysis and recommendations for changes, additions, and deletions to the baseline.

After contract award, the contractor shall develop a schematic diagram of major components of the baseline environment. The schematic shall contain examples of the major types of installations and organization of hardware, software, and communications and how they are related to one another. (An example of such a schematic is illustrated in figure 4.)

15.1.1 Instructions to Offerors

Diagrams are suggested for use at the organization, installation, and segment levels of networks. More detail is not essential and generally not helpful. Figure 4 provides a rudimentary illustration of a typical TCP/IP network installation. In the diagram produced by the offeror, actual platform and product names and other information would be substituted for the generic indicators used in the figure. These indicators are—

- MS — mail server
- FS — file server
- WKS — workstation
- PC — personal computer
- SMTP — Simple Mail Transfer Protocol
- SNMP — Simple Network Management Protocol
- NMS — network management station
- GW — gateway
- FTS 2000 — Federal Telephone System
- DDN — Defense Data Network
- SNA-TCP/IP — communications protocols (actual protocols would be named)

An overview schematic diagram shall be produced for the entire organization, as well as separate diagrams for each installation, down to local area network (LAN) levels. At the LAN level, individual users do not have to be identified, but inclusion of the numbers of users and types of platforms supported by each LAN segment shall be required.

Contractors shall provide a table of information describing the individual platform product configurations proposed as the baseline infrastructure. The table shall contain elements as listed in table 3 (See page 66.) Each column shall contain the name and release information of specific implementations of the required specifications for all platforms that are proposed. If a specific class of platform is not proposed, then that column may be omitted.

15.1.2 Evaluation of Proposals

Offerors should be evaluated on experience with transition projects of similar scope and complexity, and the extent that they make use of existing agency-provided documents and information. The detail of the configuration schematic diagrams and the product configuration information may become overwhelming. The secret to evaluating this information is to follow two or three threads for specific products or concepts through the entire transition plan. A thread should

be complete from start to finish and should not lead to dead-ends or lost segments. For example, a particular nonstandard product may be part of the baseline and eventually be replaced by another standard product. The original product may be compatible with the baseline configuration, but the replacement may not be. This can be ascertained primarily through analysis of surrounding technology and supporting reference documents. If compatibility cannot be substantiated, then a broken thread is recorded and the proposal is down-graded accordingly.

15.2 Objective Architecture

A few organizations will already have defined the objective environment in terms of an organizational profile. In others, the contractor will be required to provide a proposed profile. The following paragraph may be used when the latter is required. Additional information on the development of an organizational profile can be found in *Strategies for Open Systems* by DMR Group, Inc., Boston, 1990, and *An Analysis of Application Environments*, Emerging Technologies Group, Inc., Dix Hills, NY, 1989.

15.2.1 Instructions to Offerors

Offerors should be required to provide a profile of specifications to be used that parallels the service areas and components defined in the APP. This profile should describe all of the specifications used in detail and should provide rationale sections describing the tradeoffs made and assumptions used in arriving at the decision to include a specification.

> *The objective architecture shall define an open system environment based on the computing requirements defined in this contract, and shall provide OSE services using a building-block approach for evolution to proven future technology developments that may be useful. This architecture shall include identification of components for supporting OSE services, applications, and the user community as specified in this contract, among which are the hardware and software infrastructure proposed to meet these requirements. Rationale for the inclusion of each component and the relationship of each component to other components in the architecture shall be provided by the contractor.*
>
> *After contract award, the contractor shall maintain the organizational OSE profile, including nonstandard specifications, as specified by the objective architecture. The profile shall be continually reviewed for modifying and extending to fit immediate, long-term, and unique requirements. These modifications shall entail evaluating specifications based on their stability, maturity, and the availability of products that implement the specified interfaces.*

15.2.2 Evaluation of Proposals

Evaluators should look for the details of interaction and interrelatedness among different specifications. For example, the use of a certain specification may require the use of another second group of specifications, or prohibit the use of a third group of specifications. These relationships should be documented in the profile and should allow the evaluator to follow the line of reasoning for each thread through the profile. In addition, each product to be used in the OSE should be mapped to the specific services and interfaces defined in the profile.

Table 3. Example of Baseline Product Configuration

SERVICE\CONFIGURATION	PERSONAL COMPUTER	WORKSTATION	NETWORK SERVER/ ROUTER/ BRIDGE/ ETC.	DATABASE SERVER	MAINFRAME
Operating System Commands and Utilities System Administration Security					
Human/computer Interface Graphical user interface Character-based user interface					
Data Management Database Access Data Dictionary Remote Database Access					
Data Interchange Documents Images Graphics Products					
Programming Languages ISEE 4GL					
Graphics 3-D/Interactive Graphics Graphics Data					
Network Transparent File Access Personal Computer Access Network Management Protocols Supported APIs Supported Security					

Gaps among specifications should be identified and proposals should discuss what is to be done about these gaps. Accordingly, if gaps are noticeable and not identified, or if solutions to cover the gaps are not presented, then evaluators should down-grade. If gap coverage is not conclusive or the proposal does not discuss the rationale behind suggested solutions, again evaluations should reflect lower ratings.

15.3 Transition Strategy

The transition to an OSE is dependent upon the "development of an overall strategy for schedule, milestones, and deliverables during transition." The strategies defined accentuate the direction and scope for decision-making. The goals and objectives of the OSE within a particular organizational environment include factors such as these:

- Elimination of unnecessary dedicated systems and emphasis on common user systems and services.

- Provide for management and control visibility, and accountability.

- Provide data management support and data standardization as a separate and independent entity. Promote the use of standard data elements in all automated systems and maintain data dictionaries as a management and standardization tool.

- Identify the proper technical approach and architecture with which all automation and application systems will be designed as the environment evolves over time from its current baseline to the objective environment.

- Devise the software development methodology for the organization's application systems through a minimum of five years from date of award, that will provide modular applications that are effective, reliable, maintainable, and offer a high potential for reuse.

- Consolidate existing organizational data processing installations where feasible.

- Develop the procedures required to incorporate technology insertions and deletions as they occur and are appropriate.

- Minimize user disruptions.

- Develop provisions for using and integrating current baseline assets.

- Minimize operational impacts resulting from communications service failure.

- Ensure that security is an integral part of the architecture.

After contract award, the contractor shall provide a transition strategy for determining the best course of action necessary to implement the transition from the current baseline environment to the objective environment. The strategy shall identify planned actions and provide cost/benefit and risk analyses for each specific action. A master schedule depicting the events, deliverables, milestones, and event dependencies shall be provided by the contractor. The strategy shall also provide a means for maintaining flexibility in changing the schedule to take advantage of targets of opportunity as they arise, with minimal impact on future events and schedules. In addition, the contractor shall submit the items described in the following sections:

> *The approach to software development using integrated computer-aided software engineering (CASE) tools that incorporate interfaces described in the "Project Support Environment (PSE) Reference Model" described in NIST Special Publication 500-213 and the "Framework for Software Engineering Environments Reference Model" described in NIST Special Publication 500-211.*

Requirements gathering, prototyping, database management methodology, and structure.

Approach for data element standardization.

Language and binding considerations.

Transition of the current baseline application services to the OSE within the scheduled timeframe.

Testing functionality.

Data and software distribution.

Local area network and wide area network functionality.

Training requirements.

Interactive processing functionality.

Functional and system requirements definition functionality.

Design, development, and evaluation functionality.

Incorporation of emerging technologies.

15.3.1 Instructions to Offerors

Transitioning to the OSE is a difficult area to assess. Many variations of value-added services will be proposed by offerors making the evaluators' task extremely difficult. In proposals, offerors should provide clear indications of the types and numbers of technologies to be used and the process for using them. An overall plan with strategic decision-points should be included in the offeror's proposal. Because many of the eventual tasks will not be known beforehand, offerors will have a tough time reconciling specific tasks in their proposals with the task list developed after site surveys are completed. Instead, offerors should provide a plan for reconciling these differences in a timely and effective manner. Examples of instructions used in procurements follow:

Transition to the OSE

The offeror shall prepare and provide a description of the transition process as part of this section. The process shall describe generally how transition planning, phasing, staffing, conversion, testing, operation, and maintenance of systems shall be accomplished throughout transition. The offeror shall provide information in sufficient detail for the Government to determine the adequacy and thoroughness of this process for accomplishing the proposed tasks.

In particular, the transition process shall describe the following:

Management and control of the process.

Data management support and data standardization.

Technical approaches and architecture design principles to be used.

Methods for consolidating existing organization data processing installations.

Methods and procedures for incorporating/replacing technology

Minimizing user disruptions.

Ensuring that security is an integral part of the architecture.

Providing for continuity of operations.

The offeror shall recommend tasks or processes that need to be accomplished in addition to those already stated.

15.3.2 Evaluation of Proposals

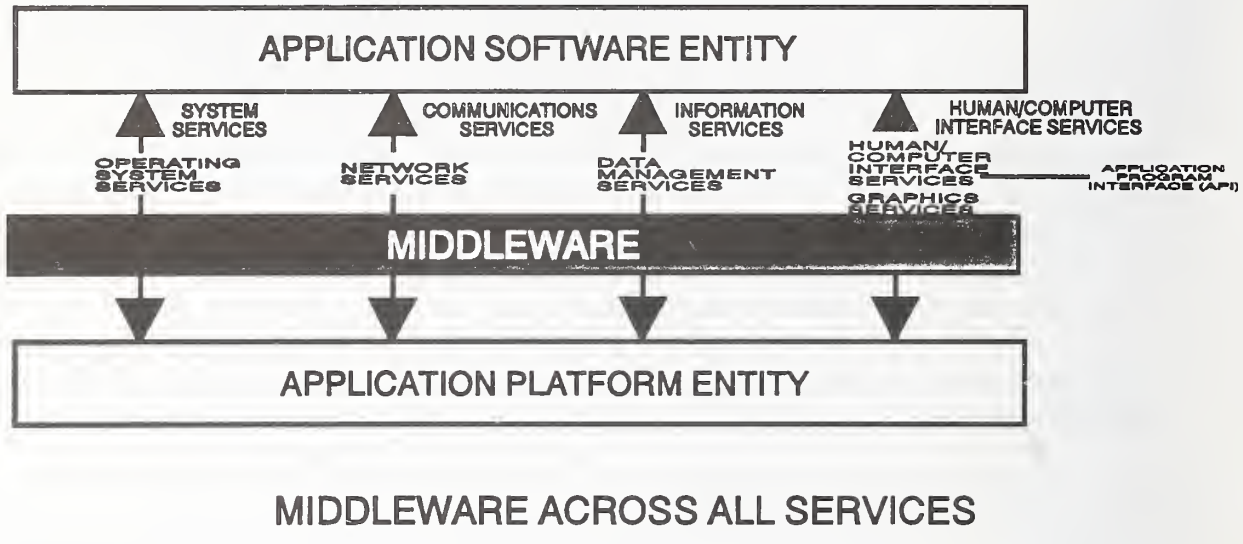
The transition proposal becomes one of the single largest discriminators in the evaluation process. Because of its nature, evaluation can be very subjective and consequently has to be supported through evaluator comment. One of the lessons-learned from transition proposal evaluation includes the concept of *middleware*. Middleware is a term used to describe intermediate code, generally in

the form of proprietary subroutine and function libraries that are loaded with applications at compile- or run-time to translate nonstandard system calls and data into more standardized calls and data. In cases where there are no standards to cite, or where standards-based implementations do not exist, middleware can be of significant value in easing transition. In those cases where standards are available and implemented, middleware makes no sense and can actually corrupt the concept of open systems. The implementation of a standard interface and service is what is required, and if available, should be used.

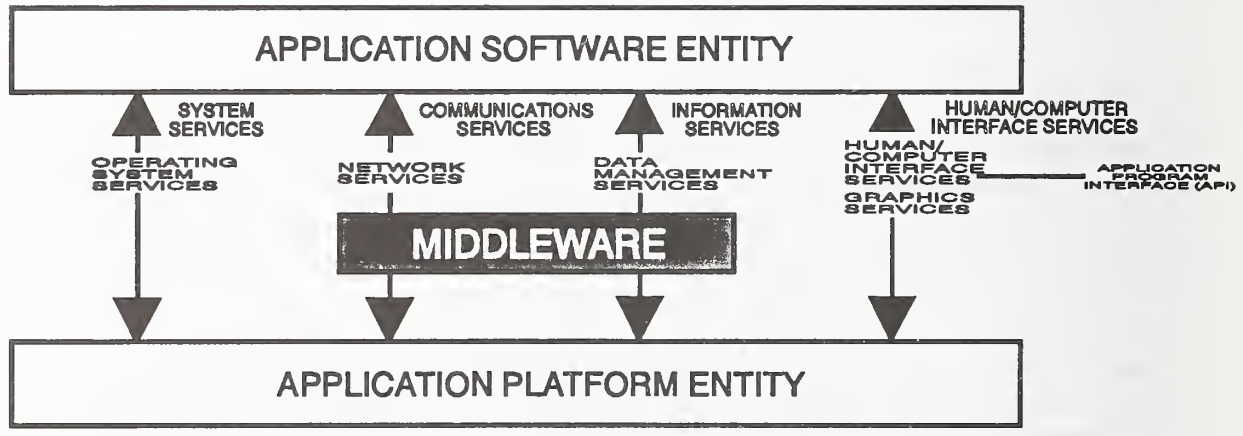
Some vendors have used the argument that middleware should be used wherever applications need to interface with other non-application components, such as the operating system, DBMS, etc. to shield the applications from knowledge of any and all interfaces, including standard ones, to the environment. The upper part of figure 5 illustrates this concept. The middleware component is shown intercepting all interactions between the application and the application platform. This is generally not acceptable.

Specifically, middleware normally is not standard. Middleware introduces another set of interfaces, those between the middleware and the application. These are in addition to the interfaces between the middleware and the platform environment. Unless the source code of the middleware is available for use by the acquiring agency through data rights or software development rights, there should be no middleware where implementations of interfaces based on standards exist. The lower portion of figure 5 illustrates a mix of middleware and standard interface configurations. In this

instance, middleware is used only in circumstances where no standard interfaces or implementations of standard interfaces exist. In other situations, the application makes use of the standard interfaces through standardized subroutine and function calls. The most acceptable case is that where no middleware is used. As illustrated, middleware over some services may be acceptable and sometimes necessary.



MIDDLEWARE ACROSS ALL SERVICES



MIX OF MIDDLEWARE AND STANDARD SERVICES

Figure 5. Middleware and Standard Interface Configurations.

One rule-of-thumb for determining where middleware should not be allowed is this: If a standard specification exists for a specific interface, and that specification is included as part of the OSE profile, then middleware normally should not be used.

The RFP should be written to include instructions to the offerors to identify when and where middleware is utilized by the system and specifically by which applications. If middleware is accepted as a viable alternative, the acquiring agency should make sure that the source code for implementing the middleware is part of the contract deliverables.

15.4 Intermediate Target Implementation Plans

The notion of gaps between standards and other interface specifications is the motivation for implementing intermediate targets.

> *Because not all specifications are supported by implemented products, intermediate targets that provide incremental functionality and transition to the objective environment shall be identified. Intermediate targets shall be defined by the contractor and fully described including changes from the baseline. Detailed plans for managing and implementing the intermediate targets shall be included. Each intermediate target shall include a description of the intermediate target environment, major changes from the baseline, and identification of schedules, deliverables, milestones, and organizational resource requirements, as a minimum.*
>
> *Additional functionality shall be proposed and described that enable organizational management to maintain flexibility to reevaluate and reallocate resources based on targets of opportunity. Targets of opportunity will typically allow the agency to reduce costs and provide more efficient use of resources in implementing the transition to open systems. The contractor shall provide a methodology and procedures for applying resources to take advantage of these targets of opportunity. Examples of such situations may include a reduction in staffing levels available to perform tasks during transition, the loss of contract funding due to unforeseen externally defined requirements, or the addition of new equipment or technology that was not available during initial evaluation of the existing systems and infrastructure.*
>
> *After contract award, the contractor shall develop a schematic diagram of major components of each transition architecture to be implemented. The schematic shall contain examples of the major types of installations and organization of hardware, software, and communications and how they are related to one another.*
>
> *The contractor shall provide a table of information describing the individual platform configurations proposed in each transition architecture to be implemented. The table shall contain elements as listed in the example illustrated in section [Baseline Definition and Analysis]. Each column shall contain the name and release information of specific implementations of the required specifications for all platforms that are proposed. If a specific class of platform is not proposed (e.g., mainframe), then that column may be omitted. Each of the services in the first column shall be addressed by entries in one or more of the adjacent columns.*

15.4.1 Instructions to Offerors

The transition plan is directly tied to intermediate targets based on procurement and transition strategies. For each type of strategy cited, the offeror should provide the outline of a process or mechanism for planning the implementation of various types of targets. For example, a strategy may include moving to a distributed data architecture. The proposal should describe methods for structuring data and associated databases in a distributed environment. The acquiring agency might include sample scenarios for various types of strategies and require the offerors to propose methods for handling the scenarios. While the use of scenarios is less than optimal, offerors should be able to provide realistic appraisals of available information and methods that would fit the situation as opposed to methods that could not be used. Information such as this will illustrate the offeror's grasp of the transition strategy and requirements.

15.4.2 Evaluation of Proposals

For each intermediate target implementation proposed, the offeror should provide evidence of standards compliance and interoperability for each product affected by standards requirements. Examples of the types of requirements that are used to obtain this information are included in the following information on testing.

> *Interoperability among implementations shall be proven through current vendor registration of products and test results with a NIST-approved interoperability registration service, where such service exists.*
>
> *Where NIST-approved interoperability registration service does not exist, the contractor shall demonstrate interoperability by executing demonstration tests on the proposed platforms as required by this contract for each individual specification affected.*

15.5 Training

Training of personnel in OSE concepts, and the use, operation, and maintenance of applications built on the OSE is an important part of the OSE procurement. There are numerous examples of procurement specifications containing detailed integral training requirements, such as the U.S. Army's Sustaining Base Information Services (SBIS). The objective of this report is not to duplicate information that is already available in other reports. Training is an integral part of the transition process and requirements should be spelled out in the RFP.

16. EVALUATING PROPOSALS

The essence of evaluating proposals based on OSE requirements involves the ability of the offeror to understand the validation process, to provide evidence that validation has taken place, and to understand the complexities in transitioning to the OSE. In many cases, a formal, detailed checklist of items can be used by evaluators to ascertain the completeness and correctness of the proposed OSE implementation.

For example, a vendor may propose platform X with operating system Y and compiler Z. Another platform, platform AX may also be proposed with the same software suite. The instructions to offerors may require proof of conformance to standards through validation. In this case, the proposals should contain four certificates of validation or validation test summaries as follows:

validation of operating system Y on platform X
validation of compiler Z on platform X (with operating system Y)
validation of operating system Y on platform AX
validation of compiler Z on platform AX (with operating system Y)

It is easy to identify when one or more of the proofs of validation is missing for such a small set of requirements. In situations where 20 or 30 products are proposed to execute on three to five proposed platforms and communications hardware, then the problem becomes almost unmanageable to keep track of the possible combinations of products and platforms. Using a checklist or chart described above, the work is manageable and shortcomings of the proposed product set will be highlighted.

The evaluation of transition plans is much more subjective and is the major differentiating factor among offerors in determining which proposal is most feasible and cost effective. Section M of the RFP, however, does not provide the detail needed by evaluators to evaluate individual proposals. It is meant to guide offerors in the right directions to place appropriate emphasis on those aspects that are most important to the agency. The evaluators use detailed evaluation checklists and questionnaires that are based on the Section M evaluation factors. (Examples of evaluation checklists are provided in Annex A.)

It is enticing to add a requirement that all validations and capability demonstrations should be submitted and performed before the proposal submission deadline, but there are mitigating factors that cannot be controlled by offerors. For example, the number of products under testing at accredited laboratories may constitute a volume that is more than those laboratories can handle in the allotted time. A reasonable requirement may be to state that all validation documents and capability demonstrations must be submitted prior to the end of discussions with prospective bidders.

17. CONCLUSION

The movement to open systems is gathering steam and momentum. Many agencies within the U.S. Government and industry have already gone through the acquisition process or are preparing system acquisitions based on OSE concepts. These organizations are developing requirements for acquiring open system services and are gradually transitioning their proprietary systems to open system infrastructures.

The process of developing these requirements and issuing contracts has resulted in a body of knowledge that can be applied by other agencies in preparing for OSE acquisitions. This report has structured the combined knowledge of several large-scale acquisitions into a guide that can be used by procurement officials. Care must be taken by these officials in using this information. A blanket,

verbatim approach to including these requirements in a contract will not ensure that the agency will acquire an open system environment that meets it needs.

Each requirement must be reviewed and evaluated according to its worth in defining the organization's open system requirements. In some cases, a requirement can be used as is. In other cases, it may require modification. In addition, evaluation factors and criteria must also be reviewed in order to determine applicability to agency capabilities for evaluating proposals and the relative importance of each requirement in the contract.

Agencies must also possess in-depth expertise in software development, communications, and database technology in order to evaluate true open systems versus marketing hype. This is still an area where *caveat emptor* applies. An agency can only be prepared.

ANNEX A. OSE EVALUATORS

The individual evaluators selected for the Source Selection Evaluation Board (SSEB) are experts in specific areas. The number of evaluators required is dependent upon the scope and magnitude of the acquisition. A specific acquisition program may have many other requirements besides the OSE requirements, but the recommendations in this annex include only those pertaining to evaluation of the OSE requirements.

A.1 Operating System Services Evaluators

Evaluation of operating system services requires SSEB members to identify proposed operating system interfaces, protocols, and data formats to ascertain whether they will provide the measures of interoperability, portability, and scalability required in Federal systems. As a minimum, operating system services proposed should include kernel operations, commands and utilities, system management, and operating system security. The proposed hardware platforms necessary to support these services will be included in evaluations. In addition, these evaluators will be responsible for evaluating transition plans where operating system services are concerned.

To effectively evaluate the offeror's proposal, operating system services evaluators should collectively possess knowledge or experience in at least the italicized topics, and preferably more:

- *System administration*
- *Operating system standards*
- *System security*
- *Operating system conversion*
- Operating system internal processing
- Software/hardware interfacing
- Existing organizational operating systems
- Capacity planning and management
- Chargeback systems
- Operations and maintenance
- System auditing

Possible disciplines that may provide the knowledge or experience required are listed as follows:

- System engineer
- Operating system support analyst
- Systems analyst
- System administrator
- Hardware analyst

A.2 Human/computer Interface Services Evaluators

Evaluators will be responsible for evaluating human/computer interface services including client-server operations, object definition and management, window management, dialogue support, user

interface security, and those parts of transition plans that apply to human/computer interface services. Hardware necessary to support these services will also be evaluated.

To effectively evaluate the offeror's proposal, these evaluators should collectively possess knowledge or experience in the following:

- *Client-server operations*
- *User interface services standards*
- *User interface toolkits*
- System security
- Existing organizational operating systems
- Network communications
- Operations and maintenance

Possible disciplines that may provide the knowledge or experience required are listed as follows:

- Systems analyst
- Programmer
- Hardware analyst

A.3 Data Management Services Evaluators

Data management services, including data dictionary/directory, database management system, distributed data, data management security, and supporting hardware will be evaluated by these evaluators. They will also be responsible for evaluating transition plans where data management services are concerned.

To effectively evaluate the offeror's proposal, data management services evaluators should collectively possess knowledge or experience in the following:

- *Logical data modeling*
- *Database administration*
- *SQL*
- *Database conversion*
- Data administration
- Database design
- Database security and integrity
- Operations and maintenance
- Database auditing

Possible disciplines that may provide the knowledge or experience required are listed as follows:

- Data administrator
- Database administrator
- Systems analyst
- Programmer
- Database designer

A.4 Combined Data Interchange and Graphics Services Evaluators

These evaluators will have responsibilities for data interchange services. These services include document, graphics data, product data, and data interchange security. Team members will also be responsible for the evaluation of transition plans to ensure that data interchange is explicitly managed and included in overall transition.

Graphics services including display element definition and management, and graphical object attribute definition and management for two- and three-dimensional graphics and interactive graphics will also be evaluated by these evaluators. They will evaluate transition plans and supporting hardware dealing expressly with graphics services.

To effectively evaluate the offeror's proposal, this group of evaluators should collectively possess knowledge or experience in the following:

- *Office automation*
- *Publishing and text processing*
- *Graphics programming*
- *Graphics and data interchange standards*
- Data administration
- Network communications
- Operations and maintenance

Possible disciplines that may provide the knowledge or experience required are listed as follows:

- Programmer
- Data administrator
- Systems analyst
- Publisher
- Documentation specialist

A.5 Software Engineering Services Evaluators

Software engineering services, including programming languages and language bindings, integrated software engineering environments (ISEE, in particular, individual tools and level of tool integration), programming security, and the proposed software development methodology will be the responsibility of these evaluators. The capabilities of supporting hardware will be evaluated on how well they match the requirements of applications and the tools proposed for a development environment. The evaluation of transition plans involving the installation and integration of programming services and software development methodology will also be the responsibility of this group.

To effectively evaluate the offeror's proposal, panel members should collectively possess knowledge or experience in the following:

- *Computer aided software engineering tools (CASE)*
- *Systems analysis and design*

- *Applied development methodologies*
- Application modeling
- Fourth generation languages (4GL)
- Standard programming languages

Possible disciplines that may provide the knowledge or experience required are listed as follows:

- Systems analyst
- Application designer
- Software engineer
- Programmer

A.6 Network Services Evaluators

These evaluators will concentrate on evaluating network and communications services proposed including data communications (protocols and programming interfaces), transparent file access (including directory services and network addressing), personal/micro computer support for interoperability, distributed computing, network security, network management, and supporting hardware. Team members will also pay particular attention to transition plans for moving to standards-based communications architectures.

To effectively evaluate the offeror's proposal, network services evaluators should collectively possess knowledge or experience in the following:

- *Network architectures and communications protocols*
- *Network administration*
- *Network design*
- Network security and auditing
- Communications standards (X.400, MHS, TCP/IP and associated protocols, etc.)
- Network conversion
- Operations and maintenance

Possible disciplines that may provide the knowledge or experience required are listed as follows:

- Network administrator
- System engineer
- Systems analyst
- Communications programmer

A.7 Security Services Evaluators

The security services evaluators will evaluate network and system security services proposed including data encryption mechanisms, identification and authentication, access control, reliability control, system logging, fault tolerance, audit facilities, and supporting hardware. Team members will also pay particular attention to security plans and transition plans for moving to secure architectures.

To effectively evaluate the offeror's proposal, members should collectively possess knowledge or experience in the following:

- *System security*
- *Network security and auditing*
- *Network design*
- System auditing
- Database security and integrity
- Database auditing
- Data administration
- Operations and maintenance

Possible disciplines that may provide the knowledge or experience required are listed as follows:

- Security analyst
- Physical security analyst
- Network administrator
- System engineer
- Systems analyst
- Network analyst

A.8 Management Services Evaluators

These services provide the mechanisms to monitor and control the operation of individual applications, databases, systems, platforms, networks, and user interactions with these components.

Evaluators will evaluate proposed mechanisms to monitor and control the operation of individual applications, databases, systems, platforms, networks, and user interactions with these components. Team members will also pay particular attention to transition plans for managing the move to the OSE.

To effectively evaluate the offeror's proposal, management services evaluators should collectively possess knowledge or experience in the following:

- *Operations and maintenance*
- *Configuration management*
- Capacity planning and management
- Chargeback systems
- Network conversion

Possible disciplines that may provide the knowledge or experience required are listed as follows:

- Network administrator
- System engineer
- Systems analyst
- Project manager

A.9 Adjunct Technical Support Team

Organizational and other agency experts in open system environments, the APP, and system architecture requirements should be available as needed to assist in investigating technical questions and providing expert assistance in determining if specific offeror claims are warranted, and in establishing the technical soundness of proposed methods. These consulting services will be available through liaison with the OSE evaluators. The composition of this team will vary according to needs. Large acquisitions, depending on the number of products and platforms proposed, may require a larger contingent of specialists.

Typical of the tasks assigned to this team will be investigating and providing background for technical inquiries by the OSE evaluators, evaluating hardware that is not specifically within the responsibilities of individual evaluators, and providing expertise that is not directly available within the group of OSE evaluators.

A.10 Proposal Evaluation Lessons Learned

Automated proposals and automated means of recording evaluations, questions, offeror responses, etc. can be used for productivity gains. Experience has taught that this is true only if the automation platforms provide high bandwidth capabilities, such as those available in a graphics-based workstation. In order to adequately display enough proposal text and diagrams, reference documents, word processing screens, etc. at one time, a workstation with a large, rapidly refreshed display is required. Otherwise, the user spends an inordinate amount of time flipping back and forth among paragraphs and documents to remember contexts and exact wording of proposal language.

A.11 Evaluation Criteria

Evaluation factors fall into two general categories: objective and subjective. Objective factors can be measured absolutely, usually through demonstration. Either the requirement is met fully, or it is not met at all. Evaluation of objective factors can be indicated by a yes or no answer. Subjective factors, on the other hand, require a qualitative or quantitative indication of how well they fulfill the requirements. Weighted scores can be used to achieve this. They indicate a sort of "goodness of fit" for meeting specifications. Both objective and subjective categories are included in the following evaluation criteria (more correctly referred to as evaluation standards in procurement terminology.) Users of this report must decide which criteria to include as objective and which to include as subjective. No differentiation is made in this report.

The combination of objective and subjective evaluation criteria, and weights is affected through the use of a checklist that lists evaluation criteria in detail and assigns a weight to each of the optional evaluation criteria. Additional scoring information may be added to the optional evaluation criteria to guide evaluators in how to respond to individual factors. The evaluation factors listed in this report are not aggregated in any particular order other than to reflect the order of requirements in the SOW. The list of evaluation factors may be distributed to evaluators as a complete list, or it may be split up into sub-lists for individual service areas and given to specialists who evaluate only the specified service areas. At least two sets of evaluations should be performed for each proposal to ensure a minimum basis for consensus-building on the final score.

A.12 Example Evaluation Factors for Operating System Services

Kernel operations are based on FIPS 151-2, and the current Validated Products List (VPL) contains an entry for validation. . . . . ____
Kernel operations validation was carried out on the proposed platforms. . . . . ____
Commands and utilities are based on IEEE 1003.2-1993. . . . . ____
Offeror has demonstrated conformance to the IEEE 1003.2-1993 specification. . . . . ____
Offeror has demonstrated interoperability with at least one other standard-based product required in this contract.. . . . . ____
Operating system security services are based on IEEE P1003.1e. . . . . ____
Offeror has demonstrated conformance to specification. . . . . ____
Offeror demonstrated interoperability with NCSC-STD-020-A. . . . . ____
Offeror demonstrated interoperability with NCSC-STD-002-85. . . . . ____
Offeror has submitted documentation on bounded operating system service completion times. . . . . ____
Offeror has demonstrated the ability of an application to reconfigure according to operating system resources. . . . . ____
Offeror has demonstrated the ability of an application to request and act on operating system services within a specified timespan. . . . . ____
Offeror has demonstrated the ability of an application to continue processing in the absence of resources that were available at application execution start. . . . . ____

A.13 Example Evaluation Factors for Human/computer Interface Services

The system shall be easy to use and understand by providing the following:

Written and programmed guidance and assistance to users in a simple, easy to understand, nontechnical manner. . . . . ____
Screens and function keys that are used in a consistent manner by any executive and other software within the system, and that do not conflict with style guidelines as required above. . . . . ____
Screens and function keys that allow users to customize the operating environment and to save customization information in a user profile that can be invoked at any time. . . ____
Features and functionality that aid novice, intermediate, and experienced users in learning and mastering the basic operation of any hardware or software with which users are expected to function. These features shall include the ability for the user to adjust the level of detail for messages, prompts, and screens, as a minimum. . . . . ____
System manuals with comprehensive levels appropriate to the type and experience of users (e.g., user manuals for novice users shall contain extensive graphic presentations [pictures, diagrams, and charts] to aid in rapid learning of and familiarization on system features). . . . . ____

The system shall provide a help facility including the following:

An on-line help facility that provides clear, precise, and accurate instructions that help a user correct the problems at hand. . . . . ____

Software and hardware features that resist, accommodate, and recover from user errors while providing clear and complete guidance for proper use. Such features shall be designed to minimize the amount of help needed by avoiding user errors that can be anticipated from extensive experience with previous systems. . . . . _____

Error messages that provide options and default suggestions when commands are invoked in incorrect syntax. . . . . _____

Manuals and on-line help sequences that are available in various levels of detail (e.g., complete, a limited subset of frequently used features, a quick reference guide, etc.) and allow the user flexibility in obtaining assistance quickly. . . . . _____

On-line help instructions that include references to appropriate user manuals and system documents in addition to help text provided. . . . . _____

User interface operations are based on FIPS 158-1 . . . . . _____

Object definition and management services, window management services, and dialogue support services offered conform to IEEE P1295.1. . . . . _____

Offeror has demonstrated conformance of implementation with P1295.1 specification . . . _____

Offeror has submitted a toolkit based on FIPS 158-1 components. . . . . _____

Offeror has submitted transition plan for human/computer interface services. . . . . _____

Transition plan contains offeror certification that transition will be complete within 12 months of FIPS acceptance. . . . . _____

Offeror has demonstrated conformance to style implementations that use the user interface toolkit specification as defined in (insert title of style guide) . . . . . _____

Written system guidance is provided in a grammatical style that is readable and understandable by a person who has completed the eighth grade. . . . . _____

System screens and function keys are consistent and do not conflict with style guidelines defined in (insert title of style guide). . . . . _____

A.14 Example Evaluation Factors for Programming Services

Offeror has demonstrated that software developed or acquired for this procurement is portable at the source code level. . . . . _____

Ada processors offered conform to FIPS 119 and offeror has submitted a NIST Certification of Validation and Validation Summary Report for each different processor. . . . . _____

Offeror has submitted ACEC test results for each different processor. . . . . _____

Without going into detail, there are many factors to be considered as a result of ACEC tests: performance, tool functionality, error messages, etc. Subjective evaluation of these tests may require more factors in this section.

A.15 Example Evaluation Factors for Network Services

Context- and time-sensitive alarms. Alarms that will warn automatically or at periodic intervals, that the network has exceeded predefined limits. . . . . _____

Fault detection, fault accounting, and fault isolation. . . . . _____

Security functions. Password protection will allow network administrator to encrypt the passwords to network servers, or to ensure that only authorized personnel can have access to network configuration information. . . . . _____

Performance management functionality. Administrator needs to know whether the network is working at optimum levels, and that can help identify bottlenecks (and other potential problem spots) that can cause network slowdowns. . . . . _____

An integrated display. Administrator needs to know at a glance what is going on with the network, and that means a single graphical view of the entire network, showing all devices. . . . . _____

Report generation functionality. Reports can provide performance summaries, for example all the errors that may have occurred in a specific network segment over a period of time. . . . . _____

The ability to update and distribute software throughout the network from a central management console. . . . . _____

Remote control functionality. . . . . _____

Further examples are not included. The above examples are provided only to illustrate the level of detail necessary to perform a complete evaluation of proposals that will stand up to scrutiny.

ANNEX B. EXAMPLE OF SOW REQUIREMENTS

This annex contains an example set of general informational items (not to be evaluated) and mandatory (denoted by the keyword *shall*) and non-mandatory (denoted by the keyword *should*) requirements derived from this report for a *fictitious* office automation environment. This is not a recommended set of requirements. It is used only to illustrate the concept of extracting requirements from the report.

The paragraph numbering used in this annex does not refer to section B of an RFP or any significant placement or importance of the requirements. It refers only to the structure of the text in this annex. In many RFPs that have been reviewed, the OSE requirements are spelled out in an annex such as this. The annex is referenced in section C of the RFP with a statement similar to the following: *Open System Environment (OSE) requirements are specified in Annex [OSE] and are included by reference.* The symbol *[OSE]* represents the annex letter or number in which the OSE requirements actually occur.

B.1 This statement of work (SOW) describes the requirements for an office automation (OA) environment consisting of components that are defined by standards for the most part. The use of standards stems from the Open System Environment (OSE) described as follows.

B.1.1 The National Institute of Standards and Technology (NIST) has developed an Open System Environment (OSE) framework that is directed at supporting a broad range of Federal applications. This framework is called the Application Portability Profile (APP) and is defined in NIST Special Publication 500-210.

B.1.1.1 The APP describes the component interfaces, protocols, and supporting data formats necessary to provide the services required by applications. A profile, or selected list of specifications, options, and parameters defines specific interfaces, protocols, and data formats that have been recommended by NIST for use by Federal agencies and are included in the APP.

B.1.1.2 The main purpose of establishing an OSE is to provide a stable environment in which interoperability, portability, and scalability of applications are the major focus. These terms are described as follows:

B.1.1.2.1 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 (defined below) 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.

B.1.1.2.2 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.

B.1.1.2.3 Interoperability—The capability of systems to communicate with one another and to exchange and use information including content, format, and semantics.

B.1.2 The systems and applications affected by this contract include the following:
Time and Attendance System (TAS)
Local Area Network (LAN)
Electronic Mail (E-mail)
Accounting System

The current operating environment does not include wide area networks (WANs), but remote offices shall be incorporated within the environment.

B.1.2.1 Time and Attendance System (TAS)

TAS currently consists of fourth generation language (4GL) programs and databases executing on desktop computers using single-user, single-tasking operating systems. They are generally operated in standalone mode, but they are connected in a divisional LAN. The platforms on which the application executes are character-oriented and have internal hard disks with 80 megabytes of storage capacity. TAS shall remain functionally unchanged and shall operate in a new environment, the OSE, as proposed by the contractor.

B.1.2.2 Local Area Network (LAN)

The software used in the division LAN is _____, Version ___. All platforms are connected via this LAN and can communicate in chat mode and through e-mail with other LANs that are connected to the division LAN through an installation server. The LAN shall be upgraded to provide higher throughput of transactions and messages. The current capacity is fully used and wait times are significant during peak loads.

B.1.2.3 Electronic Mail (E-mail)

The e-mail package in use is _____. The contractor shall provide the same functionality as is currently available, plus the capability to send and receive messages through Internet.

B.1.2.4 Accounting System

Much of the information generated on the current platforms with TAS is used as input to the installation accounting system. This is performed through transfer of batch data through diskettes to a collection point located in the accounting division. The contractor shall provide the means to transmit information directly to the accounting division and the accounting system through the OA system. No connections currently exist.

B.1.3 Organizational Requirements

All of the OA facilities are located in two adjacent buildings that are connected. Offices are located on several floors of one building and one floor of the other. The installation server is located in the basement of a third building, the administration building. Over 250 personnel are involved, of which 75 are now connected to networks outside the LAN. The contractor shall transfer these connections to the LAN and provide access to external networks as before.

B.2 Requirement for Open System Environment (OSE)

All information technology (IT) products and services offered in response to this solicitation shall operate in and execute upon platforms that provide an open system environment as described in the National Institute of Standards and Technology's (NIST) Special Publication 500-210 and modified in this solicitation. The contractor shall provide evidence to show that these products and services conform to the standards and specifications cited elsewhere in this contract. In addition, the contractor shall provide evidence showing that products, in fact, interoperate and are portable in the proposed OSE and within the constraints identified by these specifications.

B.3 The contractor shall provide information for each product proposed for use in the OSE as follows:

B.3.1 Contract Line Item Number (CLIN)

B.3.2 Name and identification of each product including version or release number that identifies the implementation explicitly from all other versions or configurations

B.3.3 Name and identification of the platforms upon which the products identified above are to be executed

B.3.4 Validation identifier, Validated Products List (VPL) date and page number; capability demonstration report date; or trademark/branding certificate identifier and issuing organization

B.3.5 Description of the product (e.g., applicability, manufacturer identification, commercial availability date, product interoperation requirements, product errors reported in the VPL, etc. In short, include information that will differentiate this product from all other similar products and manufacturers.)

B.3.6 Reference document identifiers that support contractor product claims as required, and cross-references to section numbers as described in [Hardware Components][5]

B.3.7 A text description of each product and platform proposed for use in the OSE shall be provided and included as subparagraphs of this section.

B.3.8 This table and descriptions shall be updated for each intermediate target implementation.

B.4 Validation of FIPS implementations shall be required when the following conditions are met:
a) A FIPS exists and is required by this contract.
b) An official conformance test suite exists.

---

[5]See footnote 2.

c) A FIPS testing procedure has been defined.
d) NIST-accredited or CSL-recognized testing laboratories exist.

B.5 Unless otherwise specified, all standards-based validation testing shall be conducted by CSL, or by testing laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) of NIST, or by testing laboratories that are officially recognized by CSL as the sole validation authority for specific standards, or by organizations named specifically in this contract.

B.5.1 Derived Validation: Where a FIPS is specified and a validation test suite is available and CSL validation testing procedures are in place, only validated implementations shall be used. The implementations shall implement all of the requirements of the FIPS and test results shall contain no failures. Proof of conformance shall be submitted in the form of an entry for the validated product in the current CSL Validated Products List (VPL). A currently valid base validation certificate may be submitted as proof of derived validation or validation by registration, as long as the implementation submitted is essentially the same as the implementation cited on the base certificate (i.e., errors may have been corrected, or performance changes may have been implemented, but no significant capabilities shall have been changed), and the platform configuration cited on the base certificate is the minimum when compared to the platform configuration proposed under this contract, and the proposed platform is binary compatible (i.e., uses the same CPU instruction set in native mode) with the base certificate platform. Final assessment of the acceptability and suitability of any implementation changes shall be the sole decision of the acquiring authority. The test results shall have been generated during the period that the base certificate is valid.

B.6 Interoperability among implementations shall be proven through current registration of offered products and test results with a CSL-approved interoperability registration service, where such service exists. Proof of registration shall be in the form of a reference to a current listing of the proposed product on the interoperability registration list.

B.7 Where CSL-approved interoperability registration service does not exist, the contractor shall demonstrate interoperability by executing demonstration tests on the proposed platforms as required by this contract for each individual specification affected.

B.8 A Government-provided application program in source code form shall be compiled and executed on one or more of the proposed platforms selected at random. The application program shall be moved to another platform that is not of the same model and the program shall be compiled and executed on this platform. A detailed report of the modifications made to the source code to achieve successful compilation and execution shall be submitted.

B.9 The above test may be executed with contractor-provided application programs that have been approved by the Government.

B.10 Two or more references in the current Validated Products List (VPL) shall indicate that the same implementation of the proposed software (i.e., same version and release) has been validated on at least two other manufacturer's platforms.

B.11 Two or more certificates from industry-recognized trademarking or branding organizations shall indicate that the same implementation of the proposed software (i.e., same version and release) has been validated on at least two different contractors' platforms.

B.12 A Government-provided application program in source code form shall be compiled and executed on one or more of the proposed platforms selected at random. The application program shall be moved to another platform that is not of the same model nor architecture (i.e., multiple processors versus single processor, different CPU instruction set, etc.) and the program shall be compiled and executed on this platform. A detailed report of the modifications made to the source code to achieve successful compilation and execution shall be submitted. This test and report may be combined with the application portability proof defined above, as long as the individual tests and results can be identified in the report.

B.13 The above test may be executed with contractor-provided application programs that have been approved by the Government.

B.14 In cases where capability demonstration is the required form of validation testing, the following instructions shall apply:

B.14.1 Capability demonstration: Where a FIPS is not the required specification, or where a FIPS is required and a validation test suite is not available or a CSL validation testing procedure has not been established, or where official CSL-recognized test laboratories do not exist, the contractor shall demonstrate conformance to the specification in order to allow the acquiring organization to assess the proposed implementation's suitability under this contract. The contractor shall demonstrate the implementation in a manner that exhibits the implementation's portability, scalability, and interoperability characteristics.

B.14.2 A Government-provided application shall be installed and executed on two of the proposed platforms selected at random. (If only one platform is proposed, then a second platform of different model supplied by the Government/contractor shall be temporarily used for the execution of this test.)

B.14.3 A data file of Government-provided information shall be transmitted through network communications directly (i.e., using a null modem or other similar connection) from one platform to the other. Both applications shall then be executed and a report printed of the file's contents on external storage, such as diskette or magnetic tape.

B.14.4 A second test shall be executed to replicate the first test, but without direct platform connection (i.e., communications shall be routed through an independent electronic routing or bridging device before connection shall be complete.) Transmission of data shall proceed at a communications speed different from that used in the first test (e.g., 19K bits per second [bps] versus 56K bps). A detailed report of the modifications

made to the source code to achieve successful compilation and execution shall be submitted along with machine-readable file contents generated by both platforms during both tests. This test and report may be combined with the application portability and scalability proofs defined above, as long as the individual tests and results can be identified in the report.

B.14.5 The above tests may be executed with contractor-provided data files that have been approved by the Government.

B.15 In addition to the standard implementation requirements specified elsewhere in this contract, all implementations of Federal Information Processing Standards (FIPS) that are brought into the Federal inventory as a result of this contract for which validation is specified, and those implementations used by contractors to develop programs or provide services shall be validated using the official Validation System specified by the National Institute of Standards and Technology's (NIST) Computer Systems Laboratory (CSL). Validation shall be in accordance with CSL validation procedures for the individual FIPS concerned. The results of validation shall be used to confirm that the implementation meets the requirements of the applicable FIPS as specified in this contract.

B.16 If a specification becomes a FIPS, and upon availability of a test suite, established testing procedures for the FIPS, and accredited testing laboratories, the contractor shall submit proof of conformance according to the testing requirements of the FIPS involved. As a minimum, validation shall be required within 12 months of the availability of the FIPS, an official CSL test suite, established testing procedures, and one or more CSL-recognized validation test laboratories.

B.17 If an interpretation of the FIPS is required that will invoke the procedures set forth in FIPS 29-3, "Interpretation Procedures for Federal Information Processing Standards for Software," U.S. Department of Commerce, October 29, 1992, such a request for interpretation shall be made within 30 calendar days after contract award. Any corrections that are required as a result of decisions made under the procedures of FIPS 29-3 shall be completed within 12 months of the date of the formal notification to the contractor of the approval of the interpretation. Proof of conformance for correction testing shall be submitted.

B.17.1 The implementation shall be tested using a test suite provided by the acquiring agency, such test to be witnessed by approved Government representative [most rigorous testing]; or

B.17.2 The implementation shall be tested using a test suite provided by the contractor and acceptable to the acquiring agency, such test to be witnessed by approved Government representative [less rigorous testing]; or

B.17.3 The implementation shall be tested using test suites provided by industry-recognized branding organizations and the contractor shall submit proof of conformance in the form of a certificate or license awarded by the branding organization [least rigorous testing].

B.18 In any of the capability demonstration cases, the contractor shall obtain the approval of the contracting officer to use the proposed test suites and testing methods. The contractor shall provide the test suites, test results, and environment configuration parameters in the form of a test report containing this information. The test report shall provide other appropriate information to allow the acquiring agency to assess the demonstration.

B.19 The contractor shall provide operating system services including the specified interfaces, protocols, and supporting data formats for implementing portable applications at the application-operating system interface. These services shall include kernel operations, commands and utilities, system management, and operating system security as prescribed in the following:

B.19.1 Operating System Services Requirements Reference Specifications

B.19.1.1 POSIX-like operating system environments for kernel operations offered as a result of this and other requirements in this contract shall implement FIPS 151-2, as a minimum, and shall require validation in accordance with provisions contained in FIPS 151-2.

B.19.1.2 Commands and utilities offered in support of FIPS 151-2 implementations shall implement IEEE 1003.2-1992, "POSIX Shell and Utility Application Interface for Computer Operating System Environments," as a minimum, and shall require capability demonstration.

B.19.1.3 Realtime operating system services offered in support of FIPS 151-2 implementations shall implement the functionality defined in IEEE 1003.4-1993, "Amendment 1: Realtime Extension [C Language]," and shall require capability demonstration.

B.19.1.4 As standards and other specifications required in this contract evolve, the contractor shall provide upgrades for implementations based on the current standards within 12 months of the publication of these standards.

B.19.1.5 Technology based on emerging standards that are not specifically referenced in this contract may be proposed by the contractor when such specifications achieve a high degree of stability and the benefit to the Government can be clearly documented when compared to older technologies and their cost bases.

B.19.2 Operating System Services Additional Technical Requirements Specifications

B.19.2.1 Operating system services shall support the prediction of operating system service completion times. These completion times shall be bounded and shall be documented by the contractor.

B.19.2.2 Operating system services shall provide applications with the ability to configure the implementation for optimal processing as required by the application.

B.19.2.3 Operating system services shall provide applications with the ability to specify response timing constraints for bounded services and determine from system responses whether or not this timing constraint can be met.

B.19.2.4 Operating system services shall allow processes that are not affected by lost services to continue processing.

B.20 The contractor shall provide human/computer interface (HCI) services including the specified interfaces, protocols, and supporting data formats for implementing portable applications at the application/user interface, and for communicating between the application/platform and the external environment. These services shall include client-server operations, object definition and management, window management, dialogue support, and HCI security and management as described in the following. These services shall be provided for both graphical and character-based display platforms.

B.20.1 Human/computer Interface Services Requirements Reference Specifications

B.20.1.1 Client-server operations offered as a result of this and other requirements in this contract shall implement FIPS 158-1, and shall require capability demonstration.

B.20.1.2 Object definition and management services, window management services, and dialogue support services offered as a result of this and other requirements shall implement the IEEE P1295.1 interface as defined in Draft "Standard for Information Technology—X Window System Graphical User Interface—Part 1: Modular Toolkit Environment," as a minimum, and shall require capability demonstration.

B.20.2 User Interface Services Additional Technical Requirements Specifications

B.20.2.1 User interface implementations offered as a result of the requirements of which this is a part shall implement the style guidelines defined in _____ and shall require capability demonstration.

B.20.2.2 User interface implementations based on character-oriented displays offered as a result of the requirements of which this is a part shall provide a means for replacing such interfaces with graphics-oriented displays and shall support the transition to graphics-oriented displays.

B.21 Contractors shall propose standard programming languages and language bindings for use in developmental applications provided as required in this contract. Integrated software engineering environments (ISEE) shall also be proposed that support the development of applications in standard programming languages and shall support integrated software engineering methods from initial inception of an application through development and retirement/replacement of the application. Such ISEEs shall operate on one or more proposed platforms within the operating environment required in this RFP.

B.21.1 Software Engineering Services Requirements Reference Specifications

B.21.1.1 When computer application programs are developed or acquired as a result of the requirements of which this is a part, and one of the FIPS programming languages is specified elsewhere in this contract, only the language elements of that FIPS, as well as any additional language elements specified in this contract shall be used. In these cases, processors used in developing such programs shall be validated as specified in the following requirements.

B.21.1.2 C language processors offered as a result of this and other requirements in this contract shall conform to FIPS 160 C. These processors shall implement all of the language elements of FIPS 160 C, and shall implement any additional language elements specified elsewhere in this contract. Such processors shall require validation.

B.21.1.3 COBOL language processors offered as a result of this and other requirements in this contract shall conform to FIPS 21-3 COBOL. These processors shall implement all of the language elements of the subset and optional modules of FIPS 21-3 COBOL as specified elsewhere in this contract and shall require validation.

B.21.1.4 When computer application programs are developed or acquired as a result of this and other requirements in this contract, and one of the FIPS programming languages is used as the implementation language for such programs, only the language elements of that FIPS, as well as any additional language elements specified in this contract shall be used. In these cases, processors used in developing such programs shall require validation.

B.21.1.5 Very high-level languages, such as fourth generation language (4GL) processors and application generators offered shall be required to provide the functionality described in sections 4.1 through 4.9 of NIST Special Publication 500-184, "Functional Benchmarks for Fourth Generation Languages." Contractors shall demonstrate that individual tasks described in the cited publication can be accomplished by the proposed implementation. Such 4GL processors shall be based on and compatible with the pending Xbase specification under development by Standards Committee X3J19.

B.21.1.6 When computer programs are developed or acquired as a result of the requirements of which this is a part, then the contractor shall provide a list of the methods, tools, and techniques used to verify and validate the computer programs during development.

B.21.1.7 Software verification and validation plans provided with these computer programs shall comply with the requirements in FIPS 101, "Guideline for Life Cycle Validation, Verification, and Testing of Computer Software," and FIPS 132, "Guideline for Software Verification and Validation Plans."

B.21.2 Contractors shall propose data management services including specified interfaces, protocols, and supporting data formats for application level interfaces to data dictionary/directory services, relational database management systems (RDBMS), distributed data services, and data management security as described in the following.

B.21.3 Data Management Services Requirements Reference Specifications

B.21.3.1 Data dictionary/directory implementations offered as a result of this and other requirements in this contract shall conform to FIPS 156 Information Resource Dictionary System (IRDS) and shall implement all of the functions defined, and shall require validation.

B.21.3.2 Application program interfaces (API) to the FIPS 156 implementation shall implement ANSI Standard X3.185-1992 IRDS Services Interface as a minimum and shall require validation.

B.21.3.3 An export-import facility in support of the FIPS 156 implementation shall implement ANSI Standard X3.195-1991 IRDS Export-Import File Format as a minimum and shall require validation.

B.21.3.4 SQL language processors offered as a result of this and other requirements in this contract shall conform to FIPS 127-2 Database Language SQL and FIPS 127-2 Change Number 1. These processors shall implement all of the required language elements of FIPS 127-2, all of the FIPS 127-2 options specified elsewhere in this contract, as well as all default options required by Section 13 of FIPS 127-2, New FIPS SQL Requirements, and additional requirements as specified in Section(s) [14.1, Transitional SQL, 14.2, Intermediate SQL, 14.3 Full SQL (choose none or one). Integration with RDA as defined in Section 14.4 shall also be required.] Validation shall be required.

B.21.3.5 Distributed database services offered as a result of this and other requirements in this contract shall implement "Remote Database Access (RDA)," ISO/IEC 9759:1993; "Part 1: Generic Model, Service, and Protocol," and "Part 2: SQL Specialization"; and shall require capability demonstration.

B.21.3.6 Distributed database services offered as a result of these and other requirements in this contract shall interoperate with the proposed ISEE, database implementations, and other tools as appropriate, and shall require capability demonstration.

B.21.4 Data Management Services Additional Technical Requirements Specifications

B.21.4.1 The contractor shall provide a database management system (DBMS) to implement logical data views independent of the physical underlying data model. The DBMS shall conform to FIPS 127-2.

B.21.4.2 The DBMS/data dictionary shall maintain and store database descriptions separate from, but available to, applications through an appropriate API. The information stored in this implementation shall be accessible to the IRDS implementation proposed.

B.21.4.3 The DBMS proposed shall ensure that the full range of tools needed to perform database administration and management, as well as support end-user application generation functionality is provided. As a minimum, such tools shall provide database integrity checking; allocating, initializing, and deallocating physical storage; loading,

unloading, reorganizing, and reloading files and parts of files; repairing damaged information; and logging all transactions selectively before or after the data is updated.

B.22 Contractors shall provide implementations of data interchange services for supporting data formats that provide interchange of documents, graphics data, and product description data between applications as described in the following.

B.22.1 Data Interchange Services Requirements Reference Specifications

B.22.1.1 Standard Generalized Markup Language (SGML) systems offered as a result of this and other requirements in this contract shall implement the requirements in FIPS 152 SGML and shall implement all of the language elements of SGML, and shall require capability demonstration.

B.22.1.2 All computer graphics metafiles (CGM) acquired to store, and/or communicate graphical information among different applications, devices, and computer systems shall conform to FIPS 128-1 CGM and shall require validation.

B.22.1.3 Electronic Data Interchange (EDI) services offered as a result of these and other requirements in this contract shall conform to FIPS 161-1 EDI and shall require capability demonstration.

B.22.1.4 Standard Page Description Language (SPDL) services offered as a result of these and other requirements in this contract shall conform to ISO/IEC DIS 10180 and shall require capability demonstration.

B.22.2 Data Interchange Services Additional Technical Requirements Specifications

B.22.2.1 The contractor shall provide word processing, spreadsheet, personal information manager, personal database, presentation graphics, and other office automation software that imports and exports information in a mix of the formats required in subsections relating to data interchange.

B.22.2.2 Word processors shall import and export text and page information in SGML form as a minimum.

B.22.2.3 Word processors shall print text in properly constructed SPDL form as a minimum.

B.22.2.4 Presentation graphics processors shall import and export text and graphics information in CGM or SPDL format, or both.

B.23 Contractors shall include computer networking and communications services that provide data communications, transparent file access, personal/micro computer support, distributed computing, and network security functionality as specified in the following.

B.23.1 A general requirement is that communications shall execute transparently to the users and shall provide programming interfaces at the application layer where appropriate

as a minimum. Additional requirements may augment these requirements as specified elsewhere in this contract.

B.23.2 Computer Network Services Requirements Reference Specifications

B.23.2.1 Transparent file access (TFA) services offered as a result of these and other requirements in this contract shall conform to IEEE P1003.8, "Transparent File Access (TFA)," and shall require capability demonstration.

B.23.2.2 In addition, such products offered shall interoperate with and support FIPS 151-2 POSIX, and shall require capability demonstration of this interoperability as specified elsewhere in this contract.

B.23.3 Network planning functionality shall be provided as follows:

B.23.3.1 Data monitored by various LAN components shall be aggregated into a database of time-correlated data.

B.23.4 OSI APIs for File Transfer, Access, and Management (FTAM) proposed shall provide the functionality defined in IEEE P1238.1 and shall require capability demonstration.

B.23.5 Software interfaces for accessing and administering Integrated Services Digital Network (ISDN) services proposed shall provide the functionality defined in Application Software Interface (ASI) Version 1.

B.23.6 Integrated video, voice, and data communications proposed shall implement the protocols defined in FIPS 182, "Integrated Services Digital Network."

B.23.7 Electronic mail/message handling programming interfaces proposed shall implement the functionality defined in X.400 Based Electronic Messaging Application Program Interface (API) IEEE P1224.1 and shall require capability demonstration.

B.23.8 Directory services programming interfaces proposed shall implement the functionality defined in Directory Services Application Program Interface (API) IEEE P1224.2 and shall require capability demonstration.

B.23.9 Computer Network Services Additional Technical Requirements Specifications

B.23.9.1 The contractor shall provide, deliver, install, and test communications software to implement intersite and intrasite communications requirements, via appropriate infrastructure components, common carrier, and other transmission media. Traffic volumes to be accommodated by the communications software will be identified in a baseline inventory (see [Baseline Inventory]). The communications software shall provide the following:

B.23.9.2 Detection, isolation, and correction of faults; monitoring usage; and recording significant events at the installation, system, network, and subnetwork levels.

B.23.9.3 Multiprocessing and multitasking in order to exchange information with remote computers or application systems while the operator concurrently performs application processing.

B.23.9.4 Operating in an unattended mode (e.g., where no operator is present) to exchange information with other computers or application systems.

B.23.9.5 Interfacing with the communications software employed by applications that are outside the scope of this contract but which exist within the organization or are required for communicating with the organization's external environment.

B.23.9.6 Interfacing and interoperating with contractor-provided and organizational telecommunications hardware as described in the baseline inventory.

B.23.9.7 Security features shall be provided through the use of network access control software and system security software in accordance with security guidelines of the National Security Administration (NSA) and NIST. (Draft security guidelines are available through CSL's Security Division.)

B.23.9.8 Network management software shall be provided for network and security monitoring and managing the network infrastructure, allowing systems personnel to administer the network effectively. Further functionality shall include the following:

B.23.9.9 Transferring files between any organizational platforms using standards-based communications products.

B.23.9.10 Assisting the network administrators in installation and configuration of the network, operating and maintaining the network, managing performance, and planning for network growth and evolution.

B.23.9.11 Use both the existing protocol suites (as described in the baseline inventory) and the standards-based protocol suite with the following options and additions:

B.23.9.11.1 A Simple Network Management Protocol (SNMP).

B.23.9.11.2 A Common Management Information Protocol (CMIP) and Common Management Information Services (CMIS) protocol using described managed objects in accordance with ISO/IEC 10165-4.

B.23.9.11.3 Fault detection and isolation.

B.23.9.11.4 Centralized network configuration.

B.23.9.11.5 Monitoring and testing without disruption where possible.

B.23.9.11.6 Continuous monitoring.

B.23.9.11.7 Flow and congestion control.

B.23.9.11.8 Maintenance of a centralized file of registered network object names and associated networks.

B.23.9.11.9 Gathering and analyzing usage data for all managed objects within the network and subsequently making this data available for charge-back or usage accounting on a user, account, and group basis.

B.23.9.11.10 Software to calculate subnetwork channel utilization and traffic flow among subnetworks in frames and bytes per second shall be provided and shall execute on the proposed platforms.

B.23.9.11.11 Remote access to all network management system functions by authorized users across the network.

B.23.9.11.12 Network initialization.

B.23.9.11.13 Identify the functionality for consumer and server relationships.

B.23.9.11.14 Identify changes to logical Internet Protocol (IP) addresses for individual network nodes.

B.23.10 Wide area network (WAN) functionality shall be provided using Government long haul networks, such as FTS 2000.

B.23.11 Local and wide area networks (LAN/WAN) products offered shall use existing infrastructure where feasible. Where existing infrastructure cannot be used, the contractor shall provide rationale for this decision.

B.23.12 Network functionality shall support data transfer synchronously and asynchronously at the program's discretion between a host computer and attached terminals.

B.23.13 Network functionality shall support existing communications that are based on the TCP/IP protocol suite, including the following specifications:

B.23.13.1 "Internet Protocol" RFC 791, "Internet Standard Subnetting Procedure" RFC 950, "Broadcasting IP Datagrams" RFC 919, and "Broadcasting Internet Datagrams in the Presence of Subnets" RFC 922.

B.23.13.2 "Internet Control Message Protocol" RFC 792.

B.23.13.3 "Host Extensions for IP Multicasting" RFC 1112.

B.23.13.4 "User Datagram Protocol" RFC 768.

B.23.13.5 "Transmission Control Protocol" RFC 793.

B.23.13.6 "TELNET Protocol Specification" 854 and "TELNET Option Specifications" RFC 855.

B.23.13.7 "File Transfer Protocol" RFC 959.

B.23.13.8 "Simple Mail Transfer Protocol."

B.23.13.9 "Standard for the Format of ARPA Internet Text Messages" RFC 822.

B.23.13.10 "Content Type Header Field" RFC 1049.

B.23.13.11 "Network Time Protocol (Version 2)" RFC 1119.

B.23.13.12 "Domain Names—Concepts and Facilities" RFC 1034 and "Domain Names—Implementation and Specification" RFC 1035.

B.23.13.13 "Mail Routing and the Domain System" RFC 974.

B.23.13.14 "A Simple Network Management Protocol (SNMP)" RFC 1157.

B.23.13.15 "Structure and Identification of Management Information for TCP/IP-based Internets" RFC 1155.

B.23.13.16 "Concise MIB Definitions" RFC 1212.

B.23.13.17 "Management Information Base-II (MIB)" RFC 1213.

B.23.13.18 "Exterior Gateway Protocol" RFC 904.

B.24 Security Services Requirements Reference Specifications

B.24.1 Operating system security services offered in support of FIPS 151-2 implementations shall implement the functionality defined in IEEE P1003.1e, "Security Interface for the Portable Operating System Interface for Computer Environments," and shall interoperate with and support security measures specified for access control as defined in National Computer Security Center Standard NCSC-STD-020-A, and password management as defined in NCSC-STD-002-85, and shall require capability demonstration. Additional security requirements may be specified elsewhere in this contract.

B.24.2 Network security features shall be provided in accordance with the selected guidelines in NIST Special Publication 800-4 "Computer Security Considerations in Federal Procurements."

B.24.3 The selected security requirements from NIST Special Publication 800-4 include the following:

B.24.3.1 The data/message authentication provided by [the system or specific part of the system as defined in the statement of work] shall be accomplished using message authentication codes as defined by FIPS 113, "Computer Data Authentication," and shall require validation.

B.24.3.2 The electronic signature capability provided by the system or specific part of the system as defined in the statement of work shall be accomplished in accordance with FIPS 113 and shall require validation.

B.24.3.3 The key management provided by the system or specific part of the system as defined in the statement of work shall be accomplished in accordance with FIPS 171, "Key Management Using ANSI X9.17."

B.24.3.4 The design, implementation, and use of the cryptographic module provided by the system or specific part of the system as defined in the statement of work shall conform to FIPS 140-1, "General Security Requirements for Equipment Using the Data Encryption Standard," Level [insert level] and shall require validation.

B.24.4 Security Services Additional Technical Requirements Specifications

B.24.4.1 Contractor multi-user systems used to process data under this contract shall use the following pre-logon warning message:

```
THIS COMPUTER IS OPERATED BY/FOR THE U.S. GOVERNMENT.
UNAUTHORIZED ACCESS TO AND/OR USE OF THIS COMPUTER SYSTEM IS A
VIOLATION OF LAW AND PUNISHABLE UNDER THE PROVISIONS OF 18 USC
1029, 18 USC 1030, AND OTHER APPLICABLE STATUTES.
```

B.24.4.2 After contract award, the Contractor shall examine sensitive and critical databases and files, and shall develop a list of data security techniques and methods for review. At a minimum, this list shall include:

B.24.4.2.1 Access control, integrity controls, and backup procedures

B.24.4.2.2 Data element documentation

B.24.4.2.3 Sensitive data procedures and implementation

B.24.4.2.4 Existing privacy policies and protections

B.24.4.2.5 Data access including authorization and implementation

B.24.4.2.6 Application software and how applications are moved into production

B.24.4.2.7 Written user responsibilities for management of data and applications

B.24.4.2.8 Direct access storage device (DASD) management techniques and the impact on user file integrity

B.24.4.3 After contract award, the Contractor shall examine the specific operating systems proposed and required in this contract. This examination shall, at a minimum, include:

B.24.4.3.1 Review of the operating system and its installation

B.24.4.3.2 Review of identification and authentication techniques

B.24.4.3.3 Backup and restore procedures

B.24.4.3.4 Review of system exits

B.24.4.3.5 Verification of audit trails

B.24.4.3.6 Review of handling and availability of system logs

B.24.4.3.7 Identification of change control procedures (installation of new software releases)

B.24.4.3.8 Procedures which ensure that software patches are kept current

B.24.4.3.9 Review of installation for integrity

B.24.4.3.10 Review of interfaces to access control package (if installed)

B.24.4.3.11 Identification of primary access control software and files and procedures for ensuring that all software runs under its control

B.24.4.3.12 Review of access authorizations for appropriateness and completeness

B.24.4.3.13 Review of interfaces with the access control package for integrity.

B.25 A system administration facility shall be provided and shall implement system administration functions to allocate the use of system resources by individual user, by class of users, and by application. As a minimum, the resources that shall be available for allocation are CPU time available, disk space available, relative priority for CPU access, input and output time available, and input and output volume available.

B.26 In instances where services, protocols, program interfaces, or data formats are required, but specifications have not been explicitly defined in this contract, the contractor shall propose specific implementations and cite the specifications used. In addition, the contractor shall provide a transition plan for moving to the proposed implementations (if different from existing implementations), a risk/cost/benefit analysis of each proposed implementation, and rationale for proposing a specific implementation as opposed to other available implementations. The contractor shall explain and document what effects such transition will

have on the long-term implementation of an OSE and how the contractor shall transition from the proposed implementation to an OSE when a standard specification becomes available.

B.27 Hardware Requirements

B.27.1 All monitors on user platforms shall provide 256 colors and a 14 inch diagonal viewing area measured from the upper left-most pixel to the lower right-most pixel, as a minimum.

B.27.2 All monitors on non-user platforms (e.g., network servers, test equipment, etc.) shall provide black-and-white, or amber-and-black, or green-and-black screens with a 14 inch diagonal viewing area as defined above, as a minimum.

B.27.3 All user and development platforms shall provide 3-key mouse, trackball, or thumbball for controlling cursors and human/computer interfaces. Such devices shall provide functionality for changing operating parameters, such as tracking speed, sensitivity, cursor form, etc.

B.27.4 The contractor shall consider satisfying hardware requirements from Government-Owned Equipment (GOE) and interfaces to existing GOE. The use of this equipment will be at the option of the Government.

B.27.5 Accessibility of systems shall be provided to prevent discrimination against users who have abilities other than average, such as individuals who are sight-impaired or who are impeded by other physical impairments.

B.27.6 Voice input and output devices and braille output devices shall be provided to implement accessibility for sight- and hearing-impaired operators and users.

B.28 After contract award, the contractor shall provide transition plans for accomplishing the move from the current environment to the OSE in an orderly and controlled manner. In particular, where nonstandard specifications are referenced, such as draft standards and other public specifications, contractors shall provide a method and plan for transitioning from the proposed implementation to a future FIPS implementation when such FIPS has been accepted, and shall certify that transition shall be implemented and complete within 12 months from the date of acceptance of such FIPS, unless otherwise specified elsewhere in this contract. Validation testing shall be accomplished by the contractor according to the requirements in section [Validation].

B.29 In general, transition plans shall include tasks for development and use of a baseline environment definition and analysis; specification of an objective OSE architecture; development of an overall strategy for schedule, milestones, and deliverables during transition; and development of implementation plans for intermediate targets. The Transition Plan shall address each of the following goals and shall describe how the contractor will implement and manage the transition process in light of these goals.

B.29.1 Eliminate unnecessary dedicated systems and emphasize common user systems and services.

B.29.2 Provide for management and control visibility, and accountability.

B.29.3 Provide data management support and data standardization as a separate and independent entity. Promote the use of standard data elements in all automated systems and maintain data dictionaries as a management and standardization tool.

B.29.4 Identify the proper technical approach and architecture with which all automation and application systems will be designed as the environment evolves over time from its current baseline to the objective environment.

B.29.5 Consolidate existing organizational data processing installations where feasible.

B.29.6 Develop the procedures required to incorporate technology insertions and deletions as they occur and are appropriate.

B.29.7 Minimize user disruptions.

B.29.8 Minimize operational impacts resulting from communications service failure.

B.29.9 Ensure that security is an integral part of the architecture.

B.30 After contract award, the contractor shall define, through appropriate measures, such as site visitation and inventory, and analyze the baseline configuration of current systems to determine how best to proceed with transition to the OSE, and shall provide specific recommendations based on this analysis.

B.31 After contract award, the contractor shall develop the complete baseline inventory of items including all platforms, communications, and other hardware used in the support of current systems; all software installed, and all data managed by any system within any current configuration; external system interfaces that produce information used by, or use information produced by, the baseline systems; and organizations responsible for each item. Appropriate characteristics of these inventory items, such as transaction volumes, usage statistics, capacities, error histories, maintenance histories, and other measures of software usability and maintainability, shall be included in the baseline. Problem areas, enhancements to existing systems, redundancy (planned or otherwise), and plans for new systems shall be identified in the analysis and recommendations for changes, additions, and deletions to the baseline.

B.32 After contract award, the contractor shall develop a schematic diagram of major components of the baseline environment. The schematic shall contain examples of the major types of installations and organization of hardware, software, and communications and how they are related to one another.

B.33 An overview schematic diagram shall be produced for the entire organization, as well as separate diagrams for each installation, down to local area network (LAN) levels. At the LAN

level, individual users do not have to be identified, but inclusion of the numbers of users and types of platforms supported by each LAN segment shall be required. (See fig. 6.)

B.34 Contractors shall provide a table of information describing the individual platform product configurations proposed as the baseline infrastructure. The table shall contain elements as listed in table 3. (See page 66.) Each column shall contain the name and release information of specific implementations of the required specifications for all platforms that are proposed. If a specific class of platform is not proposed, then that column may be omitted.

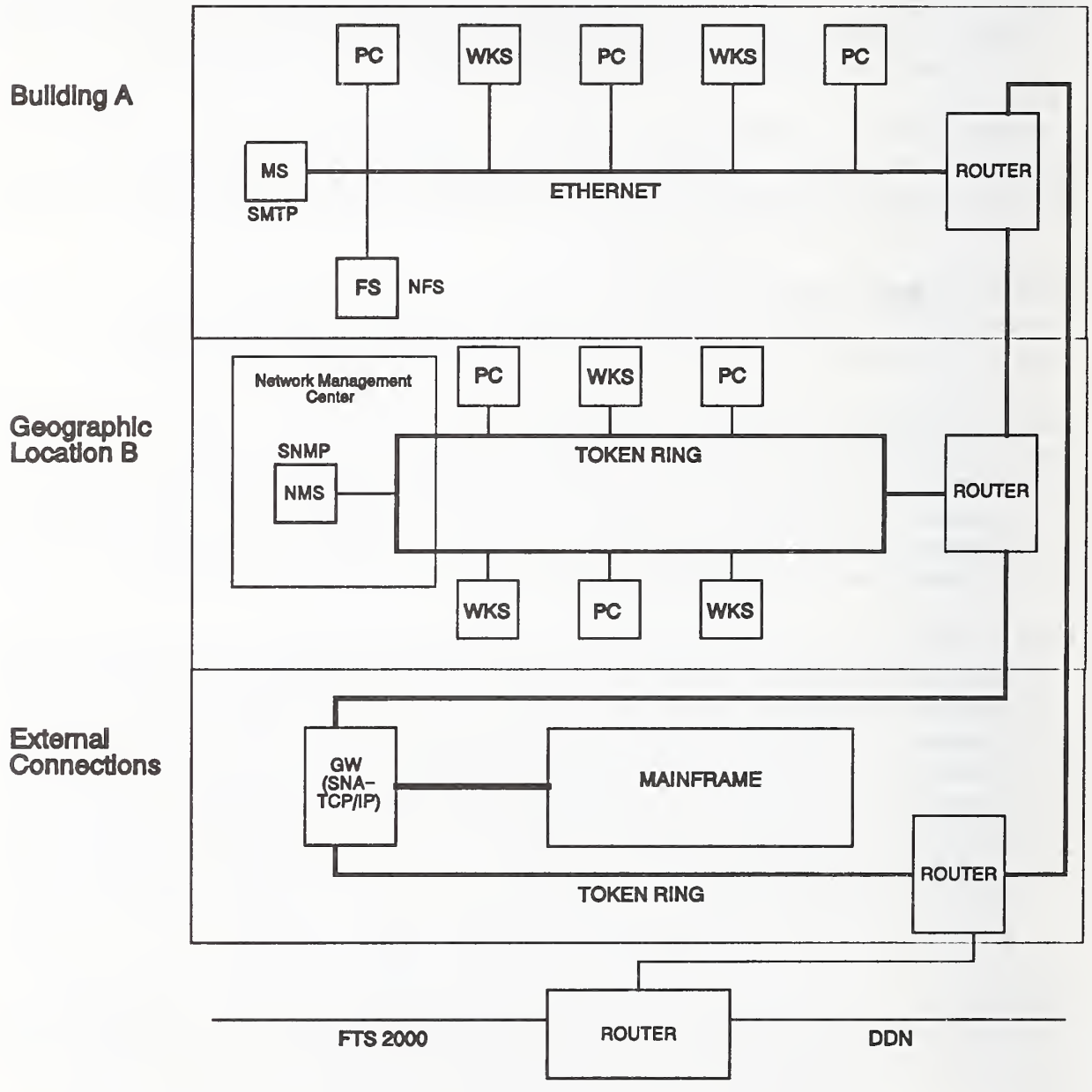


Figure 6. Sample Baseline Configuration Diagram.

B.35 The objective architecture shall define an open system environment based on the computing requirements defined in this contract, and shall provide OSE services using a building-block approach for evolution to proven future technology developments that may be useful. This architecture shall include identification of components for supporting OSE services, applications, and the user community as specified in this contract, among which are the hardware and software infrastructure proposed to meet these requirements. Rationale for the inclusion of each component and the relationship of each component to other components in the architecture shall be provided by the contractor.

B.36 After contract award, the contractor shall maintain the organizational OSE profile, including nonstandard specifications, as specified by the objective architecture. The profile shall be continually reviewed for modifying and extending to fit immediate, long-term, and unique requirements. These modifications shall entail evaluating specifications based on their stability, maturity, and the availability of products that implement the specified interfaces.

B.37 After contract award, the contractor shall provide a transition strategy for determining the best course of action necessary to implement the transition from the current baseline environment to the objective environment. The strategy shall identify planned actions and provide cost/benefit and risk analyses for each specific action. A master schedule depicting the events, deliverables, milestones, and event dependencies shall be provided by the contractor. The strategy shall also provide a means for maintaining flexibility in changing the schedule to take advantage of targets of opportunity as they arise, with minimal impact on future events and schedules. In addition, the contractor shall submit the items described in the following sections:

B.37.1 Approach for data element standardization.

B.37.2 Transition of the current baseline application services to the OSE within the scheduled timeframe.

B.37.3 Testing functionality.

B.37.4 Data and software distribution.

B.37.5 Local area network and wide area network functionality.

B.37.6 Training requirements.

B.37.7 Interactive processing functionality.

B.37.8 Functional and system requirements definition functionality.

B.37.9 Design, development, and evaluation functionality.

B.37.10 Incorporation of emerging technologies.

B.38 Transition to the OSE

B.38.1 The contractor shall prepare and provide a description of the transition process as part of this section. The process shall describe generally how transition planning, phasing, staffing, conversion, testing, operation, and maintenance of systems shall be accomplished throughout transition. The contractor shall provide information in sufficient detail for the Government to determine the adequacy and thoroughness of this process for accomplishing the proposed tasks.

B.38.2 In particular, the transition process shall describe the following:

B.38.2.1 Management and control of the process.

B.38.2.2 Data management support and data standardization.

B.38.2.3 Technical approaches and architecture design principles to be used.

B.38.2.4 Methods for consolidating existing organization data processing installations.

B.38.2.5 Methods and procedures for incorporating/replacing technology

B.38.2.6 Minimizing user disruptions.

B.38.2.7 Ensuring that security is an integral part of the architecture.

B.38.2.8 Providing for continuity of operations.

B.38.3 The contractor shall recommend tasks or processes that need to be accomplished in addition to those already stated.

B.38.4 Because not all specifications are supported by implemented products, intermediate targets that provide incremental functionality and transition to the objective environment shall be identified. Intermediate targets shall be defined by the contractor and fully described including changes from the baseline. Detailed plans for managing and implementing the intermediate targets shall be included. Each intermediate target shall include a description of the intermediate target environment, major changes from the baseline, and identification of schedules, deliverables, milestones, and organizational resource requirements, as a minimum.

B.38.5 Additional functionality shall be proposed and described that enable organizational management to maintain flexibility to reevaluate and reallocate resources based on targets of opportunity. Targets of opportunity will typically allow the agency to reduce costs and provide more efficient use of resources in implementing the transition to open systems. The contractor shall provide a methodology and procedures for applying resources to take advantage of these targets of opportunity. Examples of such situations may include a reduction in staffing levels available to perform tasks during transition, the loss of contract funding due to unforeseen externally defined requirements, or the addition of new equipment or technology that was not available during initial evaluation of the existing systems and infrastructure.

B.38.6 After contract award, the contractor shall develop a schematic diagram of major components of each transition architecture to be implemented. The schematic shall contain examples of the major types of installations and organization of hardware, software, and communications and how they are related to one another.

B.38.7 The contractor shall provide a table of information describing the individual platform configurations proposed in each transition architecture to be implemented. The table shall contain elements as listed in the example illustrated in section [Baseline Definition and Analysis]. Each column shall contain the name and release information of specific implementations of the required specifications for all platforms that are proposed. If a specific class of platform is not proposed (e.g., mainframe), then that column may be omitted. Each of the services in the first column shall be addressed by entries in one or more of the adjacent columns.

Additional requirements are necessary to define the full functionality required in this statement of work. The essence of the OSE requirements are here, albeit this example represents only a small portion of those requirements in general. The establishment of an OSE does not have to incorporate every aspect of an organization at one time. The goals and assumptions are stated, the appropriate requirements are distilled, and the statement of work is refined. The overriding consideration to be given is that this and any other statements of work to be formed for inclusion in an organizational OSE should mesh within the framework of the OSE.

Follow-on acquisitions for other aspects of the organizational OSE, such as software development, integrated database and communications, file and network server hardware, etc. should all flow from the original concept of an OSE. That is, to provide portability, scalability, and interoperability of applications across an environment of heterogeneous platforms and communications.

ANNEX C. REFERENCES

Source addresses for these documents are included at the end of this annex.

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

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

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

Draft ISO 10303, "Standard for the Exchange of Product Model Data (STEP)."

Emerging Technologies Group, Inc., "An Analysis of Application Environments," Dix Hills, NY, 19890.

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

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

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

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

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

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

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

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

FIPS 127-2, "Database Language SQL," DOC, June 2, 1993.

FIPS 128, "Computer Graphics Metafile," DOC, October 15, 1993.

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

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

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

FIPS 151-2, "Portable Operating System Interface (POSIX)—System Application Program Interface [C Language]," DOC, October 15, 1993.

FIPS 153-1, "Programmer's Hierarchical Interactive Graphics System (PHIGS)," DOC. (Undated as of this report's publication date.)

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

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

FIPS 179, "Government Network Management Profile (GNMP), Version 1.0," DOC, December 14, 1992.

FIPS 182, "Integrated Services Digital Network," DOC, October 5, 1993.

Galitz, Wilbert O., *User-Interface Screen Design*, QED Publishing, Wellesley, Massachusetts, 1993.

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

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

IEEE Working Group P1295.1, Draft "Standard for Information Technology—X Window System Graphical User Interface—Part 1: Modular Toolkit Environment."

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

ISO 9945-2:1993, "POSIX Shell and Utility Application Interface for Computer Operating System Environments."

ISO/IEC 9759:1993, "Remote Database Access (RDA) Part 1: Generic Model, Service, and Protocol, Part 2: SQL Specialization."

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

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

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

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

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

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

NIST Special Publication 500-210, "Application Portability Profile (APP), The U.S. Government's Open System Environment (OSE) Profile OSE/1 Version 2.0," DOC, June 1993.

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

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

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

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

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

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

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

RFC 768, "User Datagram Protocol."

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

RFC 791, "Internet Protocol."

RFC 792, "Internet Control Message Protocol."

RFC 793, "Transmission Control Protocol."

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

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

RFC 854, "TELNET Protocol Specification."

RFC 855, "TELNET Option Specifications."

RFC 904, "Exterior Gateway Protocol."

RFC 919, "Broadcasting IP Datagrams."

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

RFC 950, "Internet Standard Subnetting Procedure."

RFC 959, "File Transfer Protocol."

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

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

RFC 1035, "Domain Names—Implementation and Specification."

RFC 1049, "Content Type Header Field."

RFC 1112, "Host Extensions for IP Multicasting."

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

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

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

RFC 1212, "Concise MIB Definitions."

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

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

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

U.S. General Services Administration (GSA), "Standard Solicitation Documents for Federal Information Processing (FIP) Resources" (Software, Equipment, Maintenance, Systems, and modifications based on changes in Federal regulations).

DOCUMENT SOURCES

The following organizations are responsible for distributing standards for various standards-making organizations. Ordering and fee information for specific standards may be obtained directly from the addressees.

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

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

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

Department of Defense
Defense Printing Service Detachment
Standardization Documents Order Desk
700 Robbins Avenue
Philadelphia, PA 19111-5094
Phone: (215) 697-1187
Any Federal organization or DoD contractor can order numerous types of standards, including FIPS PUBs and MIL-STDs from the Defense Printing Service.

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

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

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

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

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

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

IEEE (for draft standards)
1730 Massachusetts Avenue, N. W.
Washington, DC 20036-1903
Phone: (202) 371-0101
Ask for the name and address of the editor of the draft standard for specific working groups.

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

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

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

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

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

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

ELECTRONIC DOCUMENT SOURCES

Various standards and associated documents are available from NIST through electronic means such as electronic mail or remote file access. The Computer Systems Laboratory (CSL) operates three electronic bulletin boards for information exchange:

INFORMATION ABOUT DATA MANAGEMENT ACTIVITIES AND APPLICATIONS

With a modem, dial (301) 948-2048

INFORMATION ABOUT THE NORTH AMERICAN INTEGRATED SERVICES DIGITAL NETWORK (ISDN) USERS' FORUM (NIUF)

With a modem, dial (301) 869-7281
or
telnet to 129.6.53.11

Users can reach the bulletin boards by dialing the numbers listed above. Terminal modems should have the following capabilities: ASCII, 300, 1200, or 2400 baud, 8 bits with no parity or 7 bits with even parity, 1 stop bit.

If a connection is not established at the end of two rings or if the line is busy, hang up and try again. After the word "CONNECT" appears, press the carriage return twice and the system will be accessed. The system will now guide you through the bulletin board by asking key questions and providing helpful menus.

COMPUTER SECURITY RESOURCE CLEARINGHOUSE (CSRC)

Dialup Access

Dialup access to the CSRC requires a standard ASCII terminal or personal computer with serial communications capability. The terminal/workstation must be configured to support the following communications parameters:

Modem Speed: 28.8 KBPS-300 BPS
Data Bits: 8 bit- no parity, or 7 bit - even parity
Stop Bits: 1
Default Terminal type = VT100

1. Dial 301-948-5717 and wait for the system to answer. If the line is busy or is not answered in two rings, hang up and try again.

2. When the CONNECT message is displayed, you are automatically connected to the CSRC system. Press the "ENTER" key to access the initial system screen.

NOTE: To ensure that the screen characters are correctly formatted for your display, visually verify that your terminal emulation setting (this parameter is set in your communications software program) matches the default terminal type setting shown at the bottom of the screen.

3. The CSRC provides you with on-line help and various choices of documents. The user mode of operation (for the session) can be set to "NOVICE", "INTERMEDIATE", OR "ADVANCED" by selecting the "OPTIONS" menu option. Key stroke commands are available via the "H" (HELP) key.

4. If you are using a personal computer, you may download files to your PC using various download protocols, such as ASCII, kermit, xmodem, ymodem, and zmodem.

From any screen, press the "d" key to access the screen that allows you to download a file.

Internet Access

The CSRC system can be accessed via the Internet (http, gopher, and ftp). To connect via gopher and ftp, use the following:

gopher csrc.ncsl.nist.gov or 129.6.54.11

ftp csrc.ncsl.nist.gov or 129.6.54.11

To download CSRC files, Internet users can use *ftp* as follows:

Type "ftp csrc.ncsl.nist.gov" or "ftp 129.6.54.11"
Log in to account anonymous, using your Internet ID as the password
CSRC files are located in directory *pub*.

To access the clearinghouse via an http client, such as Mosaic, use the following Uniform Resource Locator (URL):

http://csrc.ncsl.nist.gov/

ANNEX D. OSE DECISION TABLE

The following table contains an abstract decision table for assisting in the process of developing an organizational OSE profile. The questions in the first column are all answered by the user as either "yes" or "no." The entry in the second column indicates an applicable reference specification to review should the answer be "yes." The third column points to a section within this report for further information on the reference specification.

The questions are not presented as absolute indicators of the right choices; they signify only that further information contained in the references may be needed to make a final decision.

The decision model assumes that multiple applications and databases are included within the requirements of the system. It also assumes that novice, knowledgeable, and expert users will be interacting with the system and various applications.

REQUIREMENT	REF. SPEC.	SECTION NO.
1. Are platforms from more than one contractor used in the current or planned system?	See FIPS 151-2 POSIX	4
2. Is there a mix of platforms (i.e., one or more microcomputers, mainframes, workstations, and personal computers)?	See FIPS 151-2 POSIX	4
3. Are embedded or process control applications part of the current or planned system?	See IEEE 1003.4 POSIX Realtime	4
4. Are transaction processing monitors part of the current or planned system?	See IEEE 1003.4 POSIX Realtime	4
5. Are platforms to be multi-tasking?	See FIPS 151-2 POSIX; IEEE P1003.1e POSIX Security API	4, 11
6. Will platforms support multiple simultaneous users?	See FIPS 151-2 POSIX; IEEE P1003.1e POSIX Security API	4, 11
7. Do all existing systems use the same proprietary operating system?	See FIPS 151-2 POSIX	4
8. Will client/server operations be part of the system architecture?	See FIPS 158-1 X Window System	5
9. Will graphical user interfaces be available within the system?	See FIPS 158-1 X Window System and IEEE P1295.1 X Toolkit	5
10. Will the organization develop software on the proposed platforms?	See FIPS 119, FIPS 160, FIPS 21-3, FIPS 69-1, FIPS 109, and NIST SP 500-184	6
11. Will computer-aided software engineering (CASE) environments or automated tools be used in developing software?	See ECMA-149 PCTE and NIST SP 500-211 SEE	6
12. Is a data dictionary planned as part of the system?	See FIPS 156 IRDS	7
13. Is a relational database system required?	See FIPS 127-2 SQL	7

	REQUIREMENT	REF. SPEC.	SECTION NO.
14.	Will remote database access requirements be included?	See FIPS 127-2 SQL and ISO/IEC 9759:1993 RDA	7
15.	Will the system be used to produce documents for public distribution?	See ISO 8613:1989 ODA	8
16.	Will these documents require the same appearance on all output devices?	See ISO 8613:1989 ODA	8
17.	Will document processing within the system allow both printing on output devices and viewing on a windowing system?	See ISO/IEC DIS 10180 SPDL	8
18.	Will content rather than appearance be more important in document development?	See FIPS 152 SGML	9
19.	Will computer graphics data be transmitted from one platform to another?	See FIPS 128-1 CGM	7
20.	Will the computer graphics data be used to generate CAD/CAM types of drawings?	See FIPS 177 IGES	8
21.	Will the computer graphics also be used to drive process control equipment?	See ISO 10303 STEP	9
22.	Will the computer graphics also be used in printed technical documentation?	See ISO 10303 STEP	8
23.	Will the system be connected to other organizational components for transactions and payments of bills?	See FIPS 161-1 EDI	8
24.	Will 2-dimensional graphics capabilities be required?	See FIPS 120-1 GKS	9
25.	Will 3-dimensional or interactive graphics be required?	See FIPS 153-1 PHIGS	9
26.	Will transparent access to local and remote files, including databases and other files, be required?	See IEEE P1003.8 TFA; RFC 959 FTP	10
27.	Will electronic mail messaging be used?	See Planned FIPS 146-2 (X.400); RFC 821 SMTP, RFC 822 Internet Text Messages, RFC 987 X.400 to RFC 822 Mapping, RFC 1112 IP Multicast	10
28.	Will programs be developed to provide X.400 messaging?	See IEEE P1224.1 X.400 API	10
29.	Will electronic mail be routed through the system, both from internal and external system sources?	See Planned FIPS 146-2 (X.500); RFC 1034 Domain Names, RFC 1035 Domain Names Spec.	10
30.	Will programs be developed to provide X.500 directory services?	See IEEE P1224.2 X.500 API	10
31.	Will users have remote login capability through the network?	See Planned FIPS 146-2; RFC 854 Telnet, RFC 855 Telnet Option	10

REQUIREMENT	REF. SPEC.	SECTION NO.
32. Will similar networks be centrally managed?	See RFC 1155 Management Information, RFC 1157 SNMP, RFC 1119 Network Time; ISO/IEC 10165-4 CMIS/CMIP	10
33. Will dissimilar networks be centrally managed?	See RFC 1155 Management Information, RFC 1157 SNMP, RFC 1213 MIB, RFC 1212 MIB Def.	10
34. Will wide area networks (WAN) be part of the system?	See Planned FIPS 146-2; CCITT X.25, ISO 7776:1993 DLCP/LAPB, EIA 232-D Serial Interchange, EIA 530 25-position DTE Interchange	10
35. Will local area networks (LAN) be part of the system?	See Planned FIPS 146-2; ISO 8802-2:1989-12 LLC, RFC 826 ARP, RFC 903 RARP, RFC 1042 IP/ARP over IEEE 802	10
36. Will CSMA/CD networks be part of the system?	See Planned FIPS 146-2; ISO 8802-3:1992-03 CSMA/CD, ISO 8802-2:1990 10 MBPS Baseband/Twisted-pair/10 Base T	10
37. Will transport services be required across different networks and subnetworks?	See Planned FIPS 146-2; RFC 791 IP, RFC 950 Subnet, RFC 919 Broadcast Datagrams, RFC 922 Datagrams over subnets, RFC 972 ICMP, RFC 768 UDP, RFC 793 TCP	10
38. Will video communications be required in the system?	See FIPS 182 ISDN	10
39. Will the system require data or message authentication?	See FIPS 113 Authentication	10
40. Is an electronic signature capability to be part of the system?	See FIPS 113 Authentication	11
41. Will data encryption be required in the system?	See FIPS 140-1 DES	11
42. Is classified material to be used within the system?	See DoD 5200.28-STD "Orange Book"	11

GLOSSARY

The information in this glossary came from various sources including the U.S. Army's Sustaining Base Information Services (SBIS) Request for Proposals, the "American National Standard Dictionary for Information Systems" (ANSI X3.172-1990, FIPS 11-3), the draft "POSIX Guide" (IEEE P1003.0), and others.

3GL: *3rd Generation Language* - High-level programming languages that provide generalized functions for building applications and functional components of applications. Examples include Ada, C, COBOL, and FORTRAN.

4GL: *4th Generation Language* - High-level programming languages that are usually domain-specific and provide functional components for database query, database management, user interface development, system interface management, and an integrated language for providing functionality that is not contained in the other components.

5GL: *5th Generation Language* - Very high-level programming languages that generally consist of declarative, function-based, or logic-based constructs and are usually associated with artificial intelligence applications.

A

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

Acquisition Life Cycle: Five phases, each proceeded by a milestone or other decision point, during which a system goes through research, development, test and evaluation, and production. The five phases of the defense acquisition process are: Concept Exploration/Definition, Concept Demonstration/Validation, Full Scale Development, Full Rate Production and Deployment and Operations Support.

Acquisition Plan: A document that records program decisions, contains the requirements, provides appropriate analysis of technical options and the life cycle plans for development, production, training, and support of material items.

Acquisition Strategy (AS): The conceptual framework for conducting systems acquisition, encompassing the broad concepts and objectives that direct and control the overall development, production, and deployment of a system. It evolves in parallel with the system's maturation. It must be stable enough to provide continuity but dynamic and flexible enough to accommodate change. It is tailored to fit the needs for developing, producing, and fielding the system.

Administrative Contracting Officer: The Government Contracting Officer, often at an installation other than the one which made the contract, who performs the business administration of the contract.

ADPE: *Automatic Data Processing Equipment* - Any computer or communications hardware used in a computing system.

ADPR: *Automatic Data Processing Resource* - Any hardware, software, or communications equipment used in a computing system.

Application: 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 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.

Application Software: All computer programs of a given system that directly support the process of a functional application (for example, calculate payroll, produce reports, etc.).

ASCII: *American Standard Code for Information Interchange* - A coded character set consisting of 7-bit coded characters (8-bits including parity check), used for information interchange among data processing systems, data communications systems, and associated equipment.

Asynchronous: Occurring without a regular or predictable time relationship to a specified event (for example, the transmission of characters one at a time as they are keyed).

B

BAFO: *Best and Final Offer* - The final offer received in an acquisition effort.

Baseline: Defined quantity or quality used as a starting point for subsequent efforts and progress measurement.

Baseline Configuration: The baseline configuration consists of the information resources currently in the inventory and their interrelationships. The baseline configuration contains the following architectural building blocks: baseline information model, baseline data architecture, baseline applications architecture, and baseline geographic/technical architecture.

Beta Testing Process: For the purpose of an acquisition, operational testing of the system by and at a site selected by the Government. Any problems encountered during testing shall be corrected by the Contractor prior to Government acceptance.

Bridging Software: In programming, software employed to enable a set of application programs, developed on one computer system, to run on another. It is often employed in the transition phase of changing computer systems.

Business Case: A study which provides expected financial results and operating measures prior to the decision to invest in technology or business practice changes. It quantifies functional area costs, benefits, and risks; adjusts for the time value of money; and offers a uniform basis for analyzing and comparing alternatives. By comparing baseline costs to the costs of various alternatives, it

provides key quantitative financial ratios and management indicators for management decision making and control of Department investment opportunities.

C

CAE: *Contractor Acquired Equipment* - Hardware acquired by the Contractor in support of a Government project.

CASE: *Computer Aided Software Engineering* - An engineering database information system using analysis, design, code, and testing) to create a software engineering environment for hardware.

Centralized Data Processing: A concept by which an organization maintains all computing equipment at a single site (host), and the supporting field-office(s) have no effective data processing capabilities.

Certification: The issuance of a document attesting that a product or service is in conformance with specific standards or technical specifications as determined through the use of a specified test method.

CICA: *Competition in Contracting Act* - The policy that ensures full and open competition in all Government acquisition efforts.

Client/Server: The client/server model states that a client (user), whether a person or a computer program, may access authorized services from a server (host) connected anywhere on the distributed ADP system. The services provided include database access, data transport, data processing, printing, graphics, electronic mail, word processing, or any other service available on the system. These services may be provided by a remote mainframe using long haul communications or within the user's workstation in realtime or delayed (batch) transaction mode. Such an open access model is required to permit true horizontal and vertical integration.

CLIN: *Contract Line Item Number* - An identification number assigned to each integral component of a contract.

CM: *Configuration Management* - A procedure for applying technical and administrative direction and surveillance to (1) identify and document the functional and physical characteristics of an item or system, (2) control any changes to such characteristics, and, (3) record and report the change, process, and implementation status. The CM process must be carefully tailored to the capacity, size, scope phase of the life cycle, maturity, and complexity of the system involved.

Commercial Communications System: Any communications system developed by a Contractor for commercial use, although the primary users may be Government Agencies.

Commercial Equipment and Software: Equipment and software that is regularly used for other than Government purposes and sold or traded to the general public in significant quantities in the course of normal business operations.

Competition: Part of an acquisition strategy whereby more than one Contractor is sought to bid on performing a service or function, with the winner being selected on the basis of criteria established by the party for whom the work is to be performed.

Competitive Range: The competitive range is determined by the Contracting Officer. Generally, this will be determined on the basis of price or cost, technical and other salient factors.

Compiler: A software facility that converts source code (programmer written) into object code (operational) for a specific programming language (i.e., COBOL compiler, FORTRAN compiler.)

Computer: A machine capable of accepting, performing calculations on, or otherwise manipulating and storing data. It usually consists of arithmetic and logical units, a control unit, and input/output and storage devices.

Conceptual Feasibility: The reasonableness of the proposed concept and its suitability to the Government requirement.

Configuration: A collection of an item's descriptive and governing characteristics, which can be expressed in functional terms and in physical terms.

Configuration Item: An aggregation of hardware/computer programs or any of its discrete portions which satisfies an end use function and is designated by the Government for configuration.

Configuration Management (CM): A procedure for applying technical and administrative direction and surveillance to (1) identify and document the functional and physical characteristics of an item or system, (2) control any changes to such characteristics, and (3) record and report the change, process, and implementation status. The CM process must be carefully tailored to the capacity, size, scope, phase of the life cycle, maturity, and complexity of the system involved.

Conformance: The state of an implementation satisfying the requirements and specifications of a specific standard as tested by a test suite.

Contract: An agreement between two or more legally competent parties, in the proper form, on a legal subject matter or purpose, for a legal consideration.

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

Cost/Benefit: A criterion for comparing programs and alternatives when benefits can be valued in dollars. Also referred to as a benefit-cost ratio, which is a function of equivalent benefits and equivalent costs.

Cost Estimate: The resulting product of an estimation procedure which specifies the expected dollar cost required to perform a stipulated task or to acquire an item. A cost estimate may constitute a single value or a range of values.

Cost Reimbursement Contracts: In general, a category of contracts whose use is based on payment by the Government to a Contractor of allowable costs as prescribed by the contract.

Cost Risk: The risk associated with possible unforeseen costs incident to the procurement process.

COTS: *Commercial Off The Shelf* - A full developed product that is available on the commercial market.

CPAF: *Cost Plus Award Fee* - A type of Government contract under which the Government reimburses the Contractor for all allowable costs and may or may not pay an award fee based on the Contractor's performance.

CPFF: *Cost-Plus-Fixed-Fee* - A type of Government contract under which the Government reimburses the Contractor for all allowable costs and pays a fixed fee based on a percentage rate agreed to in the contract.

Critical Issues: Questions relating to a system's operational and technical support or capability that must be answered before the system's worth can be evaluated. They are of primary importance to the decision authority in allowing the system to advance to the next acquisition phase.

Critical Success Factor: A significant or key aspect of the organization's mission which must occur for a manager or organization to be successful.

Current Production: To be in current production, the equipment must 1) be created from all components specified by the manufacturer for that equipment, 2) may contain new or used parts providing that the used parts are warranted as being equivalent to new in performance, and 3) the equipment is not out-of-date, nor is it a prototype or developmental model.

D

Data: Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities, to which meaning is or might be assigned.

Data Architecture: The framework of organizing and defining the interrelationships of data in support of an organization's Information Architecture.

Database (DB): A generalized integrated collection of data that fulfills the data requirements of the applications that use it. The collection is structured to model the actual relationships within the organization. A database is typically shared by many applications, and its existence is independent of the execution of any particular application program.

Database Management System (DBMS) Data processing system that provides the means to store, organize, and access the information in a database.

Database Transaction: Any operation which alters the contents of a data base or returns data from the data base.

Data Communications: Information exchanged between end-systems in machine-readable form.

Data Dictionary: A centralized repository of information about data, such as meaning, relationships to other data, origin, usage, and format.

DBA: *Database Administrator* - An individual or organizational unit generally responsible for all physical activities relating to maintenance, control, and modifications of databases.

Detail Specification: A specification that covers all requirements for one or more types of items or services so as not to require preparation of and reference to a general specification for the common requirements.

Detailed Test Plan: An internal document of the organization conducting the testing that provides detailed instructions for the conduct of tests and sub-tests. Identifies test control, data collection, data analysis, and the administrative aspects of the tester's operations.

Distributed Data: Data stored in more than one location over a network or several interconnected computers.

Distributed Database: A database that is not stored in a central location, but is dispersed over a network of interconnected computers under the overall control of a central database management system whose storage devices are not all attached to the same processor.

Distributed Data Processing (DDP): Data Processing in which some or all of the processing, storage, input/output, and control functions are dispersed among data processing stations.

E

Economic Life: The period of time over which the benefits to be gained from a project may reasonably be expected to accrue.

EFT: *Electronic Funds Transfer* - The capability of transferring funds electronically from one account into another at the same or different financial institutions.

E-MAIL: *Electronic Mail* - A message transfer system that uses the Multichannel Memo Distribution Facility (MMDF II (B)) used by the Government.

Embedded: Refers to software that must operate within a strongly coupled complex of hardware, software, regulations, and operational procedures such as an electronic funds transfer system or air traffic control system.

Encryption: The process of systematically encoding a bit stream before transmission so that an unauthorized party cannot decipher it.

Engineering Change Proposal (ECP): A proposal to the responsible authority recommending that a change to an original item of equipment be considered, and the design or engineering change be incorporated into the article to modify, add to, delete, or supersede original parts.

Environment: A geographic area, area of decision making, or an area defined by resources required to fulfill a mission.

Executive Software (ES): (1) The operating system software and tools purchased to enable hardware and/or communications configuration to process in a pre-defined manner and to support the development and processing of application systems. (2) System software, utilities, software interfaces, and support software and tools.

Evaluation Criteria: Standards by which achievement of required technical and operational effectiveness and suitability characteristics, or resolution of technical or operational issues, may be evaluated.

Extensible: The capability of being expanded or customized. For example, with extensible programming languages, programmers can add new control structures, statements or data types.

F

Facsimile: A method of transmitting graphic images by means of analog or digital signals. Also called fax.

FAR: *Federal Acquisition Regulation* - The Government regulation detailing federal acquisition requirements and procedures.

FD: *Functional Description* - A detailed description of the functions and functional requirements of a new or proposed system.

Federal Information Processing Standard (FIPS): Publications, organized into major service categories, that define the Government's Federal Information Processing Standards as issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), as amended by Public Law 100-235, the Computer Security Act of 1987.

FED-STDS: *Federal Telecommunications Standards* - The standards set by the Government for telecommunications.

Fiber Optics: A technology that uses light as a digital information carrier. Fiber optic cables (light guides) directly replace conventional coaxial cables and wire pairs. The glass-based transmission facilities occupy far less physical volume for an equivalent transmission capacity and are immune to electrical interference.

Firm-Fixed-Price: *Firm-Fixed-Price* - A type of contract that generally provides for a firm price or, under appropriate circumstances, may provide for an adjustable price for the supplies or services being procured. Fixed price contracts are of several types so designed as to facilitate proper pricing under varying circumstances.

Fixed Price Contract: In general, a category of contracts whose use is based on the establishment of a firm price to complete the required work. Includes: (1) firm-fixed price, (2) fixed price with escalation, (3) fixed price redeterminable, and (4) fixed price with incentive provisions contracts.

Fixed Price Incentive (FPI): A type of contract with the provision for the adjustment of profit and price by a formula based on the relationship that final negotiated total cost bears to negotiated target cost as adjusted by approved changes.

FOUO: *For Official Use Only* - A security classification.

FTS 2000: *Federal Telecommunications System 2000* - A Government-contracted commercial telecommunications network which allows the Government to select from a wide array of voice, data, and video services.

Full and Open Competition: All responsible sources are eligible to compete. The standard for competition in contracting.

Functional Requirements Document (FRD): A document that identifies the requirements that must be supported and/or fulfilled by an acquisition effort. This document includes user locations, application systems, site and system specific processing requirements, workload data, etc. as a minimum.

G

Gateway (GW): The means of communicating between networks. Designed to reduce the problems of interfacing different networks or devices. The networks involved may be any combination of local networks which employ different level protocols or local and long-haul networks.

GFE: *Government Furnished Equipment* - Government property which may be incorporated into or attached to an end item to be delivered under a contract or which may be consumed in the performance of a contract. It includes, but is not limited to, raw and processed materials, parts, components, assemblies, and tools and supplies. See FAR 45.101.

GFS: *Government Furnished Software* - Software owned or leased by the Government which is provided to the Contractor to support a project.

GO/CO: *Government Owned/Contractor Operated* - Facilities and/or equipment owned by the Government for which the Government has acquired Contractor support in provided operations personnel.

GO/GO: *Government Owned/Government Operated* - Facilities and/or equipment which is owned and operated by the Government.

GOE: *Government Owned Equipment* - Computing hardware, equipment, and infrastructure that is owned by the Government and may be applied for use within the scope of a contract. The Government retains ownership and full rights as specified in titling documents.

GOSIP: *Government Open Systems Interconnection Profile* - Defines and describes a set of protocols that enable systems developed by different vendors to interoperate and enable users of different applications to exchange information. (See reference to POSIT, Planned FIPS 146-2.)

H

Hardware (H/W) (HW): The physical equipment which makes up a computer system, for example, terminals and storage devices, as opposed to programming software.

Human Factors Engineering: Human Factors Engineering (HFE) is defined as a comprehensive technical effort to integrate human factors qualitative and quantitative information into doctrine, development and acquisition to ensure operational effectiveness.

I

IAW: *In Accordance With* - A reference to a document that defines specific requirements.

IFB: *Invitation For Bid* - A Government request for contractor bid on an acquisition effort.

Independent Evaluation: The process used by independent parties to determine if the system satisfies the stated requirements. It renders an assessment of data from all sources, simulation, and modeling; and an engineering or operational analysis to evaluate the adequacy and capability of the system.

Independent Evaluation Plan (IEP): An internal plan which addresses program evaluation responsibilities relative to the system throughout its acquisition cycle. This plan serves as a source of issues for other evaluation documents and includes issues, a description of evaluation methodology, support requirements, and data sources.

Independent Evaluation Report (IER): A report that provides a systems evaluation based on test data, reports, studies, and other appropriate sources in the areas of technical performance, safety, operational effectiveness and suitability, and the adequacy of testing to that point in the development of the item or system.

Information Model: A model that represents the processes, information classes, information flow, and elements of an organization and all relationships among these factors, based on the Information Requirements Study. It supports an organization's Information Architecture.

Information System (IS): The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures. An organized assembly of resources and procedures designed to provide information needed to execute or accomplish a specific task or function. Activities and resources concerned with the creation, gathering, manipulation, classification, storage, display, retrieval, security, transmission, dissemination, or removal of elements of information. Information may be in visual, audio, or electronic form.

Installation: A contractor- or Government-owned and operated facility for providing Government information services.

Installation Communications: Any communications requirements not supplied by long haul communications. These include office, building, inter-building, and other installation Local Area Networks (LANs). LANs may be connected to a larger network and may be connected into community, command, or regional area networks through long haul communications.

Installation Processing Transition Plan: A study conducted to identify the extension schedule and OSE platforms required to support specific applications at an installation.

Installation Service: Printing and publications, records management, visual information, and library services supplied by installations to the installation residents, tenant organizations, and requesting users with no other source of support.

Integrated Computing: The concurrent use of data by two or more software packages.

Integrated Database: A database that has been consolidated to eliminate redundant data and that may support multiple applications.

Integrated Data Processing: A systematic approach to all aspects of data capture and data processing in order to maximize overall system efficiency.

Integrated Services Digital Network (ISDN): In communications, an integrated digital network in which the same digital switches and digital paths are used to establish different types of services (for example, data, video, and voice communications.)

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

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

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

IV&V: *Independent Verification and Validation* - An independent review of the hardware configuration or software product for functional effectiveness and technical sufficiency. A third party responsible for the verification and validation of a project.

J

K

Kbps: *Kilobits Per Second* - A measurement of information throughput speed.

KO: *Contracting Officer* - Any officer or civilian designated with the authority to enter into, administer, or terminate contracts for the Government.

L

LAN: *Local Area Network* - A user-owned, user-operated, high volume data transmission facility connecting a number of communicating devices (computers, terminals, word processors, printers, mass storage units, etc.) within a single building or several buildings within a physical area.

Life Cycle Cost (LCC): The total cost to the Government of acquisition and ownership of a system over its useful life. It includes the cost of development, acquisition, extension, support, and, where applicable, disposal.

Life Cycle Cost Estimate (LCCE): A cost estimate that considers all costs incurred during the projected life of the system, subsystem, or component being evaluated.

Life Cycle Management: The process for administering an automated information system or hardware support system over its entire life, with emphasis on strengthening early decisions which shape costs and utility.

M

Maintainability: Ability of an item to be retained in or restored to a specified condition when maintenance is performed, using prescribed procedures and resources, at each prescribed level of maintenance and repair.

Memorandum of Understanding (MOU): Agreements that are generally recognized by all partners as binding even if no legal claim could be based on the rights and obligations laid down in time.

Migration: The process of moving from one environment (Operating System or Platform) to another.

MIPS: *Million Instructions Per Second* - A measurement of CPU speed.

MIS: *Management Information Systems* - Those computer systems used to process information to support the management of a specific mission.

MOA: *Memorandum of Agreement* - A internal Government agreement signed by two or more organizations which states the functions and responsibilities of each organization involved in a project.

Modular Hardware: ADPE capable of adding discrete elements of capacity, thereby allowing for growth.

N

Network: A composition of a communications media and components attached to that medium whose responsibility is the transfer of information. Such components may include automated information systems, packet switches, telecommunications controllers, distribution centers, and technical management and control devices.

Network Architecture: The philosophy and organizational concept for enabling communications among data processing equipment at multiple locations. The network architecture specifies the processors and terminals, and defines the protocols and software that must be used to accomplish accurate data communications.

Network Management Software: Software to provide the capabilities for network and security monitoring and managing the network infrastructure, allowing systems personnel to administer the network effectively from a central location.

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

NIST: *National Institute of Standards and Technology* - An organization of the U.S. Department of Commerce that develops standards and guidelines for Federal computer systems under the provisions of Public Law 100-235.

Nonproprietary: Computing environments that define their capabilities and specifications and are available to any vendor for use in developing commercial products.

O

Object Types: Object types are classes of persons, places, things, concepts, events, or activities about which the organization wants to keep data. These are the objects of the information model and information architectures.

Objective Configuration: The optimum capability needed to support a mission. It provides an objective for planning purposes and, therefore, is not restricted by resource availability. The objective configuration is a logical structure. The objective configuration contains the following architectural building blocks: objective information model, objective data architecture, objective applications architecture, and objective geographic/technical architecture.

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

Original Equipment Manufacturer (OEM): A manufacturer that sells equipment to a reseller. The term is also used to refer to the reseller, as well. OEM customers typically purchase hardware from a manufacturer and resell it under their own brand names. They may combine units from several vendors as well as add software. Often used synonymously with VAR.

Offer: A response to a solicitation that, if accepted, would bind the offeror to perform the resultant contract.

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

Off-the-Shelf: Existing systems or equipment without a research and development program or with minor development to make the system suitable for Government needs. May be commercial system/equipment or one already in the Government's inventory.

Online System: A system with a direct interface between applications programs stored in the computer and terminals for data entry and output.

Operational Test and Evaluation: The field test, under realistic conditions, of any item or key component to determine the effectiveness and suitability of the equipment for use by typical users; and the evaluation of the results of such test.

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

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

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

P

PC: *Personal Computer* - A piece of equipment capable of storage, retrieval, and manipulation of data.

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

Portability: The ability of application software source code and data to be transported without significant modification to more than one type of computer platform or more than one type of operating system. An indirect effect of portability combined with interoperability (defined above)

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.

POSIT: "Profiles for Open Systems Internetworking Technologies." (See Planned FIPS 146-2 in reference section and GOSIP in this glossary.)

Program Management: The process whereby a single leader and team are responsible for planning, organizing, coordinating, directing, and controlling the combined efforts of participating/assigned civilian and military personnel and organizations in accomplishing program objectives.

Program Manager (PM): The individual chartered to manage a system acquisition program.

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

Prototyping: In system development, the process of building and refining a working model of the final operational system during the development phase. The main purpose of prototyping is to refine inputs, outputs and functions during the design phase rather than having to await the final development of the system. Prototyping can take one of three forms. At the simplest level, the prototype merely comprises a mockup of system outputs, sample reports, screen layouts, etc., produced in hard copy and reviewed with the user. A more elaborate form is a simulation of the final system where users can sit at a terminal and experience the system as it would be after development. This method is useful for demonstrating the system and giving user feedback. The third form of prototyping is the evolutionary system made possible by the development of fourth-generation languages. In this case the prototype system can evolve into the final system.

Q

Quality Assurance (QA): A planned and systematic pattern of all actions necessary to provide confidence that adequate technical requirements are established, that products and services conform to established technical requirements, and that satisfactory performance is achieved.

Quality Control (QC): The system or procedure used to check on product quality throughout the acquisition process.

Quantifiable Benefit: A benefit which can be assigned a numeric value such as dollars, physical count of items, or percentage change.

Query Language: A high level Data Manipulation Language used in a stand alone interactive processing manner.

R

Remote Access: Pertaining to communications over a common carrier facility or other external data link.

Request for Proposal (RFP): Solicitation document used in negotiated procurement actions with which the Government reserves the right to award without further oral or written negotiations. Only the acceptance of the Government is required to create a binding contract. The Government can choose to negotiate further at its option.

Requirement: (1) The need or demand for personnel, equipment, facilities, other resources or services, by specific quantitative for specific periods of time or at a specified time. (2) For use in budgeting, item requirements should be screened as to individual priority and approved in the light of total available budget resources.

Response Time: The time period between a terminal operator's completion of an inquiry and the receipt of a response. Response time includes the time taken to transmit the inquiry, process it by the computer, and transmit the response back to the terminal. Response time is frequently used as a measure of the performance of an interactive system.

RFC: *Request for Comment* - A formal request for an independent organization to review and comment on a proposed contractual document or portions thereof.

Risk Assessment: An evaluation of a risk in terms of mission loss should a hazard result in an accident.

Risk Management: A method of management which concentrates on identifying and controlling the areas of events that cause unwanted change.

S

Safety: Freedom from the conditions that can cause death, injury, illness, damage to, or loss of, personnel, equipment, or property.

SAT: *System Acceptance Test* - The test, usually a 30-90 day test period, to ensure that a system and all of its components function as designed.

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.

SDP: *System Design Plan* - A plan that details the design of a system or program.

Security Features: The security-relevant functions, mechanisms, and characteristics of automated information system hardware and software (for example, authentication, access control, confidentiality, and integrity).

Shared Databases: Use of a stable subject area database by multiple applications. The databases are organized in accordance with a model independent of organization structure and software applications.

Site Plan: A document detailing the hardware, software, communications, environmental requirements, user training, software transition, and Contractor services required to install and support one geographic location.

Site Survey: The physical walk-through of a location to identify requirements and environmental shortfalls.

Software (SW): Computer program instructions and data. May be either executive or application software.

Software Enhancements: Functional changes in software made to improve existing software performance, maintainability, or reliability, and changes required in response to changing doctrine, techniques, or threats.

Software Interface: The languages, codes, and messages that programs use to communicate with each other. This includes the implementation of language bindings and other programming language-specific interfaces.

Software Maintenance: The technical changes needed to correct errors and defects which reduce the effectiveness or operability of the system.

Sole Source Acquisition: A contract for the purchase of supplies or services entered into or proposed to be entered into by an agency after soliciting and negotiation with only one source.

Solicitation: In contracting, the term means to go out to prospective bidders and request their response to a proposal.

Source Selection: The process where requirements, technical evaluations, costs, commendations, and policy relevant to an award decision of a competitive Government procurement are examined and the decision is made as to the source to supply the required system and services.

Source Selection Authority: The official designated to direct the source selection process, approve the selection plan, select the source(s), and announce the contract award.

SSAC: *Source Selection Advisory Council* - Senior Government functional area personnel involved in a procurement who make recommendation to the SSA based upon the conclusions of the SSEB.

SSEB: *Source Selection Evaluation Board* - Government functional and technical personnel charged with providing a detailed evaluation of technical, management, logistics, and cost proposals submitted by the offerors.

Standardization: The most efficient use of research, development, and production resources; and to adopt on the broadest possible basis the use of (1) common or compatible operational, administrative, and logistics procedures and criteria; (2) common or compatible technical procedures and criteria; (3) common, compatible, or interchangeable supplies, components, or equipment; and, (4) common or compatible tactical doctrine with corresponding organizational compatibility.

Statement of Work (SOW): That portion of a contract which describes the actual work to be done by means of specifications or other minimum requirements, quantities, performance data, and a statement of the requisite quality.

Support Software: All software that indirectly supports the operation of a computer system and its functional applications, for example, MACRO instructions, call routines, read and write routines, etc.

System Software: A major category of programs used to control the computer and process application programs, such as secure operating systems, communications control programs, and database managers. Contrasts with applications software, which comprises the data entry, update, query, and report programs that process an organization's data.

T

Technical Evaluation: Addresses the technical issues and criteria; acquisition and fielding of an effective, supportable and safe system; engineering design and development; verifying technical performance specifications, objectives, producibility, adequacy of the Technical Data Package, and supportability; determining safety, health hazards, and human factors aspects. The evaluation makes use of models, simulations, testbeds and prototypes, or full-scale models.

Testbed: A system representation consisting of actual hardware, computer models or prototype hardware.

Test method: A specified method of performing tests, such as the procedures and specific test cases used to test a product for conformance to a specification or standard.

Test Report: A formal document of record which reports the data and information obtained from the conduct of, and describes the conditions which actually prevailed during, test execution.

Transaction: A unit of work which is carried on to completion and is characterized by ACID properties (Atomicity, Consistency, Isolation, and Durability).

Transition Plan: Describes how the organization plans to move from the baseline configuration through the current target configuration, to achieve the objective configuration.

Trusted Computer System: A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information (Department of Defense 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria").

Trusted Database: Relating to the interpretive guidance as stated in Department of Defense 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria."

Trusted System: A collection of interdependent components that can be considered as a unified whole, for example, a networked collection of computer systems, a compiler or editor, a memory

unit and so on believed and demonstrated to enforce a given set of attributes to a stated degree of assurance (confidence.) (Handbook of Information Security and Computers at Risk, source documents).

U

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

User Test: A generic term which encompasses testing and requires the use of user representatives for development tests, innovative tests, concept evaluation program, operational tests, follow-on operational test and evaluation, on-site user tests, and joint user tests.

Utilities: A program that supports the operation of the computer. Utility programs, or simply "utilities," provide file management capabilities, such as sorting, copying, archiving, comparing, listing, and searching, as well as diagnostic routines which check the health of the computer system. Compilers or software that translates a programming language into machine language.

V

V&V: *Verification and Validation* - The process of verifying and validating that a system or function meets or exceeds its stated requirements.

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

W

Waiver: (1) A written authorization to accept a configuration item or other designated items, which during production or after having been submitted for inspection, are found to depart from specified requirements, but nevertheless are considered suitable "as is." (2) A decision to not require certain criteria to be met for certain reasons.

Window: (1) A separate viewing area on a display screen as provided by the software. Operating systems can provide multiple windows on screen, allowing the user to keep several application programs active and visible at the same time. Individual application programs can provide multiple windows as well, providing a viewing capability into more than one document, spreadsheet or data file. (2) a reserved area of main memory. (3) a period of time in which an event can or must occur.

Workstation (WS): A piece of computer hardware that is operated by a user to perform an application. Provides users with access to the distributed information system or other dedicated systems; input/output via a keyboard and video display terminal; or, any method that supplies the user with the required input/output capability. Computer power embodied within the workstation may be used to furnish data processing capability at the user level.

WP: *Word Processing* - An information processing system for the printed word that allows storage, retrieval, and manipulation of information.

X

X.21: A technical specification recommended by the CCITT that describes the interface used in the CCITT X.25 packet switching protocol and in certain types of circuit-switched data transmissions.

X.25: A standard for packet switching procedures developed by CCITT.

Y

Z

INDEX

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.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

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 bi-monthly 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.

Consumer Information Series—Practical information, based on NIST research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NIST publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

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 non-government). 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