

U.S. Department
of Transportation

United States
Coast Guard



Commandant
United States Coast Guard

2100 Second St. S.W.
Washington, DC 20593
Staff Symbol G-SIA
Phone: (202) 267-1272

COMDTINST M5230.45A
APR 22 1996

COMMANDANT INSTRUCTION M5230.45A

Subj: INFORMATION SYSTEMS TECHNOLOGY ARCHITECTURE

1. PURPOSE. To provide technical architecture guidance for commands implementing systems which use Information Technology (IT).
2. ACTION. Area and District Commanders, Commanders of Maintenance and Logistics Commands, Commanding Officers of Headquarters Units, and Directors of Headquarters Directorates and Chiefs of Headquarters Staffs and Offices shall ensure compliance with the provisions of this instruction.
3. DIRECTIVES AFFECTED. COMDTINST 5230.45 is cancelled.
4. BACKGROUND. The Director of Information and Technology is committed to providing quality leadership and management in developing and supporting computer, telecommunication, electronic, and information management systems. To this end, information systems technology architecture will provide the needed standards and help shape the Coast Guard's IT focus. This focus will guide the fundamental decisions and actions of systems developers and improve communications with, and provide support for, customers.
5. DISCUSSION. This document publishes the Information Systems Technology Architecture (ISTA). It introduces and promotes:
 - a. the ability of two or more systems to use and exchange information (interoperability),
 - b. the ease with which a system or component can be transferred from one hardware or software environment to another (portability), and
 - c. the ability to use the same application software on many

personal computers to super computers (scalability). This version of the ISTA is a first step toward "open systems" and will provide interoperability and portability of applications and data. Commandant (G-SI) will provide additional near-term guidance as required by systems developers on specific standards.

6. OBJECTIVE. The objective of the Coast Guard ISTA is to develop a common vision of the future USCG Information Technology environment and to provide near-term guidance and long-term direction for the development and deployment of information technology resources. Critical policy and procedures for the planning and approval of Federal Information Processing (FIP) resources are described.
7. RESPONSIBILITIES.
 - a. The Office of Architecture and Planning (G-SIA) specifies the Coast Guard Information Systems Technology Architecture and focuses on maintaining a framework to guide the development, deployment, and operation of information technology (i.e., communications, computers, and electronics) based on international, national, federal, industry, and Coast Guard standards. All AIS system proposals and budget requests will be reviewed for architectural compliance with the standards as described herein.
 - b. Area and District Commanders, Commanders of Maintenance and Logistics Commands, Commanding Officers of Headquarters Units, and Chiefs of Headquarters Directorates and Directors shall ensure that appropriate staff members are cognizant of the contents of this instruction and that future information technology systems are designed, engineered, developed, and implemented according to the Information Systems Technology Architecture.

/s/ D. E. CIANCAGLINI
Director of Information & Technology

EXECUTIVE SUMMARY

The USCG Information Systems Technology Architecture (ISTA) defines a target framework for Information Systems (IS) development. The ISTA is not intended to be a specific system architecture, however, it does contain specific policy and procedures for the planning and approval of FIP resources. It identifies specific standards that are required to be implemented in any IS procurement (mandatory standards), and it identifies other standards that **may** be required depending on the intended use of the system. All of these standards are designed to enable portability (ability to transfer a system from one hardware or software environment to another), scalability (ability to use the same application software on many different classes of hardware/software platforms from personal computers to super computers), and interoperability (ability of two or more systems or components to exchange and use application data). Implementing these standards creates an open systems environment that is important for inter-agency and intra-agency operations.

All Coast Guard information system developments will use the standard application software suite (e.g. database, development tools, user interface, operating system) and will: 1) apply the mandatory standards when appropriate (SQL, POSIX, etc.), and 2) consider the use of the non-mandatory standards (Ada, X-Windows, etc.) for interoperability, portability, and scalability as needed to meet long term goals. For example, end-user applications for internal Coast Guard use are only required to be programmed in C or Ada if the application requires a third generation language, but a fourth or fifth generation language may be used if the 4GL/5GL is the standard software development tool obtained from the Coast Guard Standard Workstation III (SWIII) contract and the application needs no interoperability with other agencies. Similarly, personal databases can be developed using the SWIII personal database application, but databases using the high end SWIII database application program require the use of the SQL2 standard. Depending on the application being developed, the affect of implementing the standards could have no impact or could have significant impact on information system development. Commandant (G-SIA) will evaluate program requests for waivers to the standards in instances where the standard increases time and/or development costs and appears to add no apparent value.

To develop the ISTA, the staff consulted with the National Institute of Standards and Technology (NIST), the DOD, the Defense Information Systems Agency (DISA) Center for Information Management (CIM), the Architecture Methodology Working Group (AMWG), and others. In particular, the USCG acknowledges the work accomplished by NIST in developing the Application Portability

Profile (APP), the Institute of Electrical and Electronic Engineers (IEEE) in developing the guide to the POSIX open System Environment (OSE), and the DOD in their development of their Technical Architecture Framework for Information Management (TAFIM), version 3.0. The ISTA is based heavily on the TAFIM, which mandates IS standards for the Department of Defense community.

The architecture will evolve as new technologies and standards emerge. Commandant (G-SIA) will assess these technologies and standards and the architecture will be updated. Other areas to be addressed in future editions of the architecture include services and standards for tactical systems, imagery, and multimedia data transfer. Commandant (G-SIA) will assist users in choosing extensions to the current standards in those areas where standards do not exist, or where consensus has not been achieved. Other changes to the architecture can be made by following the procedures described in Chapter 4 of the ISTA.

The associated standards profile identifies standards and guidelines in terms that can be tailored and applied to meet the needs of specific mission areas (i.e. mission or functional areas). The reference architecture and standards profile define the target technical environment for the acquisition, development, and support of USCG information systems. Areas of the architecture where approved standards are not yet available, or where multiple competing standards exist, represent technical issues and gaps to be resolved. Successful implementation will require that the guidance provided in the ISTA be followed when designing, developing, engineering and implementing Information Systems.

The ISTA is not intended to hasten the obsolescence of the legacy and proprietary systems we use. Alternatives to convert a proprietary system to an open systems environment to meet information systems requirements should be considered on a business case basis. Implementing activities should consider the degree to which the new open system/subsystem must co-exist or be interoperable with legacy systems during transition. A total "grand design" conversion from an existing proprietary system to an open system may exceed the operational or technical capabilities of the organization. A transition strategy that plans for the expeditious replacement of inefficient, proprietary subsystem/components with products conforming to standards may be the best solution, from both an operational and technical perspective. Part of this strategy will require that Project Managers (PM's) perform an economic analysis with trade-offs for technologies. Lastly, PM's must also ensure compliance with the Strategic Information Resource Management Plan (SIRMP) and other applicable directives.

TABLE OF CONTENTS

CHAPTER 1 - INTRODUCTION.....	1-1
A. Background.....	1-1
B. Purpose and Objectives.....	1-1
C. Standardization Efforts.....	1-2
D. Approach.....	1-3
E. Document Organization.....	1-3
CHAPTER 2 - USCG TECHNICAL REFERENCE MODEL.....	2-1
A. Overview.....	2-1
B. Principles.....	2-2
C. Generic CG Technical Reference Model.....	2-5
D. Detailed CG Technical Reference Model.....	2-6
E. Application Software Entity.....	2-6
F. Application Program Interface.....	2-9
G. Application Platform.....	2-9
H. External Environment Interface (EEI).....	2-10
I. External environment.....	2-11
CHAPTER 3 - USCG PROFILE OF STANDARDS.....	3-1
A. Overview.....	3-1
B. Process and Criteria.....	3-1
C. Specific Standards by Service Area.....	3-3
D. Software Engineering Services - C, Ada.....	3-3
E. User Interface Services - WIN32, X-Windows.....	3-5
F. Data Management Services - SQL, RDA.....	3-7
G. Data Interchange Services - SGML, EDI.....	3-9
H. Graphics Services - PHIGS, GKS.....	3-14
I. Network Services - POSIT, TCP/IP.....	3-15
J. Operating System Services - POSIX.....	3-20
K. Security and System Management Services.....	3-22
L. Communications, Information Interchange, and Users.....	3-26
M. Assessment of Standards Availability.....	3-28
CHAPTER 4 - IMPLEMENTATION GUIDANCE.....	4-1
A. Challenges.....	4-1
B. Standards Gaps.....	4-1
C. Implementation.....	4-1
D. Conversion.....	4-3
E. Implementation Planning.....	4-3
F. Tailoring.....	4-5
G. Additional Implementation Guidance.....	4-5
H. Waiver/Waiver Procedures.....	4-6

APPENDICES

A. References.....A-1
B. Acronyms.....B-1

CHAPTER 1. INTRODUCTION

- A. **Background.** The goal is to transition the U.S. Coast Guard's present Information Systems to a communications and computing infrastructure transparent to the user. This goal will be achieved by implementing the USCG Information Systems Technology Architecture. The development of a technical reference model and the selection of associated standards are the first steps toward executing this strategy.
- B. **Purpose and objectives.** **The architecture, populated with specific standards, defines a profile of technical standards that are mandatory for all USCG information systems, except systems specifically exempted by Commandant (G-SIA).** *Note: Systems that are currently operational or budgeted for development are exempt from this instruction.* The purpose of this is to enable our systems to work together. It provides a common conceptual framework, defines a common vocabulary, and specifies a base of standards so that the USCG can better coordinate acquisition, development, and support of USCG information systems and associated infrastructure systems. The architecture also provides a high-level representation of the domain showing major service areas. USCG components are required to apply the architecture to increase commonality and interoperability across the USCG and with DOD and other Government agencies. Areas of the architecture where approved standards are not yet available, or where multiple competing standards exist, represent technical issues and gaps to be resolved. The architecture is not a specific system architecture. Rather, it establishes a common vocabulary and defines a set of services and interfaces common to USCG Information Systems. The associated standards profile identifies standards and guidelines in terms that can be tailored and applied to meet the needs of specific mission areas (i.e. mission or functional areas). The reference architecture and standards profile define the target technical environment for the acquisition, development, and support of USCG information systems. The ultimate objectives of the architecture are to:
- o Improve user productivity
 - o Improve IS development efficiency
 - o Improve portability and scalability
 - o Improve interoperability
 - o Reduce reliance on single vendors
 - o Reduce life cycle costs
 - o Improve security

Principles. IRM improvements will be realized by applying the following principles:

- (1) When there is consistency (a set of standards) in how to manage information resources throughout their life cycle, there is considerable improvement in product quality and uniformity.
- (2) Establishing controls and measurements for project monitoring, evaluation, management decisions, tracking, and auditing provides better information resource management and reduces system life cycle costs.

C. **Standardization efforts.** There is increasing standards activity in the Federal Government, industry, and the international community. The National Institute of Standards and Technology (NIST) is responsible for promulgating Federal Information Processing Standards (FIPS). NIST actions and decisions will significantly affect the USCG for two major reasons. First, the USCG is required to adhere to the standards promulgated by NIST, and second, USCG customers desire to interact and exchange data with other Government and industry organizations that will be adhering to the same standards. Clearly, NIST and DOD standardization activities are the logical starting point for developing an architecture and standards profile for the USCG.

NIST is currently pursuing the definition of an Open System Environment (OSE), which encompasses (1) the functionality needed to provide easier transfer of a system or component from one hardware or software environment to another, (2) the ability to use the same application software on many different classes of hardware/software platforms from personal computers to super computers, and (3) the ability of two or more systems or components to exchange and use information across networks of different hardware/software platforms.

In April 1991, NIST published the first version of the Application Portability Profile (APP), which defines a reference model and outlines a suite of selected specifications (i.e., standards) that defines the interfaces, services, protocols, and data formats for implementation of an OSE within the U.S. Government.

In September 1991, the DOD published the first edition of the DOD Technical Reference Model. Subsequent versions have been produced. The U.S. Coast Guard Technical Reference Model (USCG TRM) is adopted from the NIST APP and DOD TRM models to meet the requirements of the USCG, and conforms to NIST and DOD recommendations wherever possible. As NIST and DOD

continue to evolve their models, changes will be considered for incorporation into this document. As USCG requirements evolve, changes to the APP will be forwarded to NIST and the Defense Information Systems Agency (DISA) Center For Standards (CFS).

- D. **Approach.** Commandant (G-SIA) has the responsibility for developing an information technology architecture and educating appropriate parties on the architecture and its value to the Coast Guard. Commandant (G-SIA) prepares the architecture based on standards, including international, federal, industry, and Coast Guard standards. The staff will promote systems interoperability, sharing of resources, and systems stability by facilitating consensus on information technology and will continue to work with NIST and other national and international standards organizations to ensure that the NIST APP and emerging standards meet or are compatible with the needs of the USCG.

- E. **Document organization.** The ISTA consists of four chapters. Chapter 1 provides an introduction to the ISTA. Chapter 2 provides an overview of the USCG Technical Reference Model, the principles upon which the model is based, and the services to be provided. Chapter 3 presents the profile of standards, discusses the criteria for the selection of standards, summarizes each of the selected standards, and discusses related standards. Chapter 4 provides implementation guidance, including principles for the transition planning to migrate existing systems into compliance with the standards profile defined in Chapter 3 and concepts for tailoring the architecture to a specific mission area. References and acronyms are identified in appendices A and B, respectively.

CHAPTER 2. USCG TECHNICAL REFERENCE MODEL

- A. **Overview.** Within the context of information systems, a reference model is defined to be a generally accepted representation that allows people to agree on definitions, build common understanding, and identify issues for resolution. A technical reference model is necessary to establish a context for understanding how the various technologies required to implement information management relate to each other. The model also provides a means for identifying the key issues associated with applications such as providing easier transfer of a system or component from one hardware or software environment to another, the ability to use the same application software on many different classes of hardware/software platforms from personal computers to super computers, and the ability of two or more systems or components to exchange and use information across networks of different hardware/software platforms. The USCG Technical Reference Model is not a specific system design. Rather it establishes a common vocabulary and defines a set of services and interfaces shared by USCG information systems.

The USCG Profile of Standards identifies standards and guidelines associated with the USCG Technical Reference Model services and interfaces. For example, the standards associated with Data Interchange Services in Figure 2-2, USCG Technical Reference Model, are identified in Figure 3-1, USCG Profile of Standards, as Electronic Data Interchange (EDI), Initial Graphics Exchange Specification (IGES), and others. These standards and guidelines can be applied in the design, development, acquisition, installation, operation, and maintenance of information systems and tailored to meet specific mission area requirements. The USCG Technical Reference Model will serve to facilitate interoperability between mission area applications, portability across mission areas, and cost reductions through the use of common services.

The development of the USCG Technical Reference Model is critical to the successful implementation of the USCG Information Systems Technology Architecture. By adopting the USCG Technical Reference Model and the standards associated with it in the USCG Profile of Standards, we can move towards constructing an Open Systems Environment (OSE) for our Information Systems. It is then we can move from today's many vertical stovepipe systems and programs to tomorrow's integrated end-to-end systems.

It should be noted that the USCG Technical Reference Model is evolutionary in nature. Standards will continue to emerge and evolve as the state-of-the-art is continually advanced. Future needs and contexts need to be defined. Nevertheless,

the USCG must begin moving in this direction if it is to satisfy the requirements of the 1990's.

B. **Principles.** The USCG Technical Reference Model was devised to permit the Coast Guard to take advantage of the benefits of open systems and the new technologies available in the commercial market. USCG-wide application of the model will result in long-term cost savings. Chapter 1, paragraph B, outlines the Information Systems Technology Architecture objectives. The principles that support these objectives and that will be used to refine and implement the architecture are as follows:

1. **Objective 1: Improve user productivity.** User productivity improvements will be realized by applying the following principles:
 - a. **Consistent user interface.** A consistent user interface across all applications will ensure that all user accessible functions and services will appear and behave in a similar, predictable fashion regardless of the application or the site. This simplifies training, facilitates the development of future applications, improves the ease of use across applications, and promotes the ease with which a system or component can be transferred from one hardware or software environment to another.
 - b. **Integrated applications.** Applications available to the user will behave in a logically consistent manner across user environments. Support applications, such as office automation and electronic mail, will be developed as an integrated set.
 - c. **Data sharing.** Concepts and tools that promote data sharing include adherence to standard data base development rules, the use of USCG corporate data dictionary and reuse of existing software components, and strong USCG commitment to resource sharing. Databases will be shared across the service, considering security and operational aspects.
2. **Objective 2: Improve IS development efficiency.** The efficiency of development efforts will be improved by applying the following principles:
 - a. **Common development.** Applications that are common to multiple mission areas can be centrally developed or acquired.
 - b. **Common Operating Environment.** A standards-based common operating environment, which accommodates the injection of new standards, technologies, and

applications on a USCG-wide basis, will be established. This standards-based environment will provide the basis for development of common applications and facilitates software reuse.

- c. **Use of commercial products.** Hardware-independent, commercial-off-the-shelf (COTS) products will be used to satisfy requirements to reduce the dependence on custom developments and to reduce development and maintenance costs.
 - d. **Software reuse.** Software reuse is the application of reusable components in multiple domains, systems, or product lines. Incorporating a reuse methodology into the development process, can, over the system life cycle, save time and money, reduce development time, and improve product reliability.
 - e. **Resource sharing.** Data processing resources (hardware, software, and data) will be shared by all users requiring the services of those resources. Resource sharing will be accomplished in the context of security and operational considerations.
3. **Objective 3: Improve portability and scalability.** The portability and scalability of applications will be improved by applying the following principles:
- a. **Portability.** Applications which conform to the architecture will be portable, allowing for movement across heterogeneous computing platforms with minimal or no modifications. With portable applications, implementing activities will be able to upgrade their hardware base as technological improvements occur with minimal impact on operations.
 - b. **Scalability.** Applications which conform to the architecture will allow operation on the full spectrum of computer platforms depending on user requirements.
4. **Objective 4: Improve interoperability.** Interoperability improvements across applications and mission areas can be realized by applying the following principles:
- a. **Common infrastructure.** The USCG will develop and implement a communications and computing infrastructure based on open systems and systems transparency including, but not limited to, operating systems, database management, data interchange, network services, network management, and user interfaces.
 - b. **Standardization.** By implementing standards from the USCG Profile of Standards (see Chapter 3),

applications will be provided and will be able to use a common set of services that improve the opportunities for interoperability.

5. **Objective 5: Reduce reliance on single vendors.** Single vendor reliance will be reduced by applying the following principle:
 - a. **Interchange components.** Hardware and software supporting or migrating to open systems compliance will be acquired or implemented so that upgrades or the insertion of new products will result in minimal disruption to the user's environment.
 - b. **Non-proprietary specifications.** Capabilities will be defined in terms of non-proprietary specifications that support full and open competition and are available to any vendor for use in developing commercial products.
6. **Objective 6: Reduce life cycle cost.** Life cycle costs can be reduced by applying most of the principles discussed above. In addition, the following principles directly address reducing life cycle costs:
 - a. **Reduced duplication.** Replacement of "stovepipe" systems and "islands of automation" with interconnected open systems, which can share data and other resources, will dramatically reduce overlapping functionality, data duplication, and unneeded redundancy.
 - b. **Reduced software maintenance costs.** Software complexity may increase with increased user demand for services such as distributed processing and distributed database services. However, if the principles described above are implemented, reductions in software maintenance will be realized because there will be less software to maintain. In those cases where the number of USCG users is small, increased use of standard COTS software will further reduce costs since COTS vendors distribute their product maintenance costs across a much larger user base.
 - c. **Reduced hardware and software acquisition costs.** A common set of hardware and software capabilities and requirements allows for clear identification of system needs and possible solutions. This results in lower costs and more effective systems acquisition.
 - d. **Reduced training costs.** A reduction in training costs will be realized as users rotating to new organizations will already be familiar with the common systems and Human Computer Interfaces (HCIs).

7. **Objective 7: Improve security.** Security improvements across applications and missions can be realized by applying the following principles:
- a. **Uniform security policy.** Consistent policy across the USCG will facilitate the evolution to an integrated environment. For example, uniform accreditation procedures will enhance security interoperability as the information systems become more closely coupled or interconnected.
 - b. **Consistent security interface.** Security features will have similar characteristics across mission area applications. Not all mission area applications will need the same suite of security features, but any features used will be consistent across applications. Users will see the same security labels in a common format and manage them in the same way. User login will be consistent across applications.
- C. **Generic USCG Technical Reference Model.** The generic USCG Technical Reference Model is a set of concepts, entities, interfaces and diagrams that provides a basis for the specification of standards. It is intended to provide guidance to managers and project leaders responsible for developing, integrating and maintaining USCG information systems and their infrastructure. To a large extent, the USCG Technical Reference Model adopts the foundation work of the Institute of Electrical and Electronic Engineers (IEEE) Portable Operating System Interface (POSIX) P1003.0 Working Group as reflected in their Draft Guide to the POSIX open System Environment. The POSIX Guide has reached a degree of maturity and is undergoing the IEEE balloting process to be sanctioned as an official IEEE document.

The basic elements of the generic USCG Technical Reference Model are those identified in the POSIX Open System Reference Model and are presented in Figure 2-1. As shown, the model includes three classes of entities and two types of interfaces as follows:

- o Application Software Entity
- o Application Program Interface
- o Application Platform Entity
- o External Environment Interface (EEI)
- o External Environment

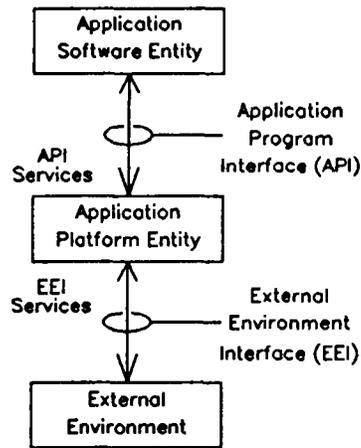


Figure 2-1. Generic USCG Technical Reference Model

Generic USCG Technical Reference Model

This model has been generalized to such a degree that it can accommodate a wide variety of general and special purpose systems. More detailed information is presented in subsequent chapters; however, the service specifications allow for subsets or variations as needed. Standards address only the interface between entities and include the definition of services as well as the supporting format across the interface. From the perspective of the application software, these services are provided by the application platform whether the particular services are provided from the local platform or from remote platforms which may comprise one or more nodes of a larger distributed system. This view of providing services to an application software entity may be characterized as "platform-centered."

- D. **Detailed USCG Technical Reference Model.** Figure 2-2 expands upon Figure 2-1 to present the USCG Technical Reference Model's entities and interfaces including the service areas of the Application Platform entity and related services.
- E. **Application software entity.** In the past, custom systems were developed for specific hardware platforms using proprietary systems software (i.e., operating system, text editor, file management utilities, etc.). Such customization was necessary because USCG requirements were often more sophisticated than those of the commercial marketplace. These systems were not designed to interoperate with other systems nor to be portable to other hardware platforms.

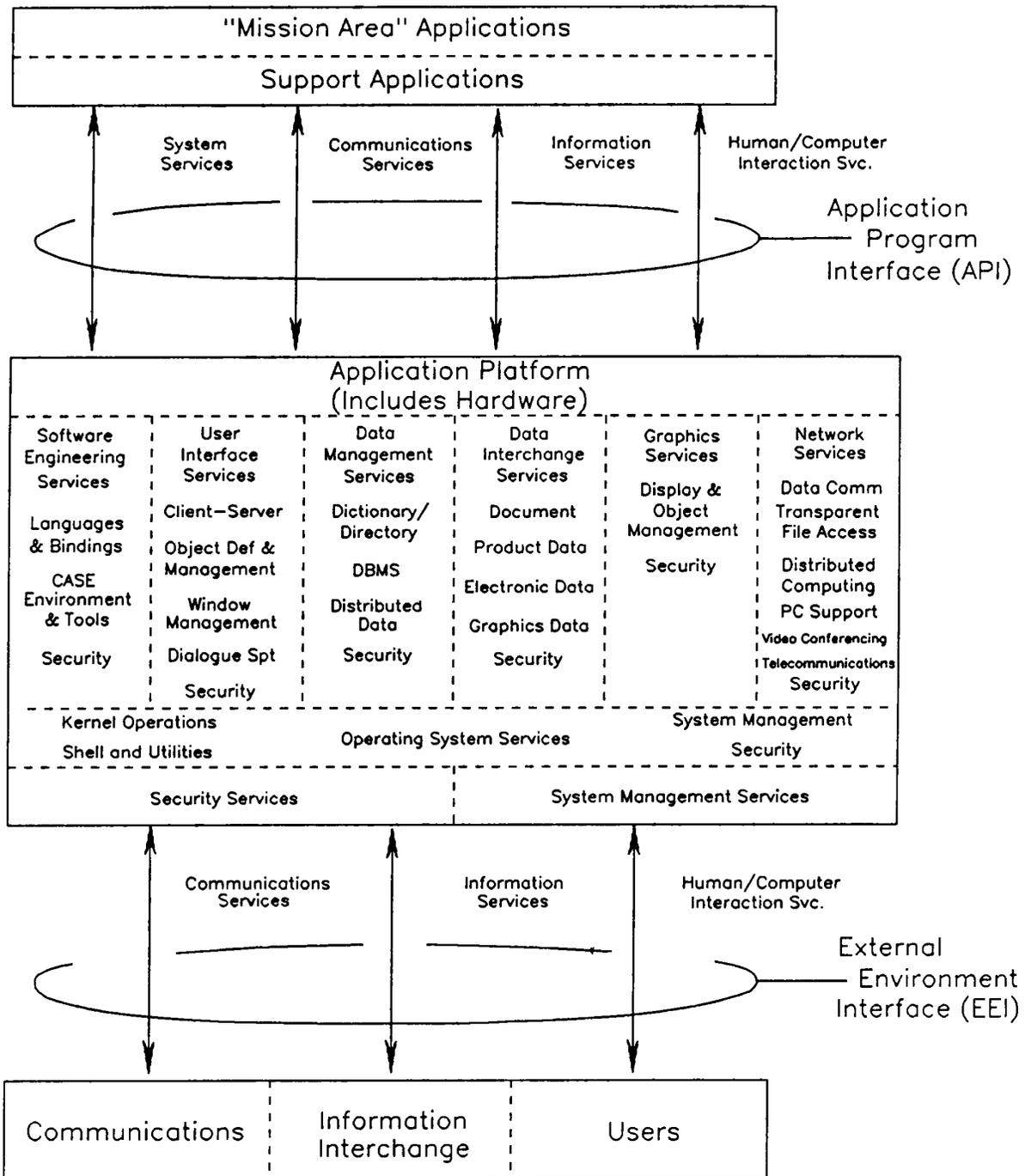


Figure 2-2. Detailed USCG Technical Reference Model

Detailed USCG Technical Reference Model

In addition, different systems were developed to perform similar functions for organizations at different levels (national, district, and unit) and to interface with different service components (Navy, Army, Air Force). As a result, many of the systems that were developed duplicated functions of other applications and often hindered systems evolution toward greater interoperability, data sharing, portability, and software reuse.

The USCG Technical Reference Model emphasizes the goals of developing modular applications and promoting software reuse to support the broad range of activities that are integral to any organization. To satisfy these goals, functional (mission area) applications development will, in many respects, become an integration activity. Application development will be accomplished by dividing and/or consolidating common functional requirements into discrete modules, identifying already developed reusable components, or Government-off-the-shelf (GOTS) applications that could satisfy some, if not all, of the new functional requirements, then integrating or interfacing such reusable code/applications, to the extent possible, to form a baseline from which to build the software pieces necessary to complete the mission and/or support applications that will satisfy all of the requirements.

In the USCG Technical Reference Model, applications are divided into mission area applications and support applications. A common set of support applications forms the basis for the development of mission area applications. Mission area applications should be designed and developed to access this set of common support applications. The following mission area and support applications are not to be confused with the Coast Guard's operating and support missions.

1. **Mission area applications.** Mission area specific applications support particular mission area needs (e.g., payroll, accounting, materiel management, personnel, command and control). The application software can be COTS, GOTS, custom-developed, or a combination of all of these. Each mission area application includes data (user data, reports, application parameters, screen definitions, diagnostics, etc.), online documentation, and online training (context-sensitive help, tutorials, etc.), as well as application software (source code, command/script files).
2. **Support applications.** Support applications are common applications (e.g. E-mail, word processing, spreadsheets) that must be standardized across individual or multiple mission areas.

Support applications can be used to develop mission area specific applications or they can be employed directly at the user level. For example, the Defense Logistics Agency (DLA) has developed a general-purpose, reusable information management system that provides access to commonly-used government-developed applications and COTS products. DLA's Information Exchange (INX) system is a generic support application that manages the storage, distribution, and presentation of information created by application processes. Through control data stored in its directory, INX invokes the appropriate platform services to archive, format, and transmit data.

F. **Application Program Interface (API).** The API is defined as the interface between the application software and the application platform across which all services are provided. It is defined primarily in support of application portability, but system and application software interoperability also are supported via the communication services API and the information services API. The API specifies a complete interface between the application and the underlying application platform and may be divided into the following groups:

- o System Service API (including API's for Software Engineering Services and Operating System Services)
- o Communications Services API (including API's for Network Services)
- o Information Services API (including API's for Data Management Services and Data Interchange Services)
- o Human/Computer Interaction Services API (including API's for User Interface Services and Graphics Services)

The first API group, System Services, is required to provide access to services associated with the application platform internal resources. The last three API Groups (Communications Services, Information Services and Human/Computer Interaction Services) are required to provide the application software with access to services associated with each of the external environment entities (i.e., communications, information interchange, or users). API's for Security Services and System Management Services are included among all groups where applicable.

G. **Application Platform.** The Application Platform is defined as the set of resources that support the services on which an application or application software will run. It provides interface services that, as much as possible, make the implementation-specific characteristics of the platform transparent to the application software.

In order to assure system integrity and consistency, application software entities competing for application software platform resources must access all resources via service requests across the API. Examples of application platform services may include an operating system, a realtime monitor program, and all hardware and peripheral drivers. The application platform implementations that use the USCG Technical Reference Model may differ greatly depending upon the requirements of the system and its intended use. It is expected that application platforms defined to be consistent with the USCG Technical Reference Model will not necessarily provide all the features discussed here, but will use tailored subsets (profiles) for a particular set of application software.

H. **External Environment Interface.** The External Environment Interface (EEI) is the interface between the application platform and the external environment across which information is exchanged. It is defined primarily in support of system and application software interoperability. User and data portability are directly provided by the EEI, but application software portability is indirectly supported by reference to common concepts linking specifications at both interfaces. The EEI specifies a complete interface between the application platform and the underlying external environment, and may be divided as shown in the USCG Technical Reference Model into the following groups:

- o Communication Services EEI
- o Information Services EEI
- o Human/Computer Interaction Services EEI

The Communication Services EEI provides access to services for interaction between internal application software entities and application platform external entities, such as application software entities on other application platforms, external data transport facilities, and devices. The services provided are those where protocol state, syntax, and format all must be standardized for application interoperability.

The Information Services EEI defines a boundary across which external, persistent storage service is provided, where only the format and syntax is required to be specified for data portability and interoperability.

The Human/Computer Interaction Services EEI is the boundary across which physical interaction between the human being and the application platform takes place. Examples of this interface include CRT displays, keyboards, mice, and audio

input/output devices. Standardization at this interface will allow users to access the services of compliant systems without costly retraining.

- I. **External Environment.** The External Environment contains the external entities with which the application platform exchanges information. These entities are classified into the general categories of communications entities, information interchange entities, and human users. Communication entities include telephone lines, local area networks, and packet switching equipment. Information interchange entities include, for example, removable disk packs, floppy disks, and security badges.

Chapter 3. USCG Profile of Standards

- A. **Overview.** The USCG Technical Reference Model, populated with approved standards, is shown in Figure 3-1 and is described in Sections D through L of this chapter. The USCG Technical Reference Model standards were based on the DoD Technical Reference Model; however, the USCG Technical Reference Model is tailored to the Coast Guard. The Information Systems Technology Architecture is intended to be a living document which will be updated to reflect the standards added, changed, or deleted in the USCG Technical Reference Model.

Implementing activities are required to use the standards specified in this document to meet the needs of specific missions. When several standards are given in an area, implementing activities may select the most appropriate standard to meet mission needs. A waiver from Commandant (G-SIA) is needed to deviate from these standards.

A detailed discussion of the process and criteria used to select the standards is provided in Section B. The standards profile is not entirely complete. Although this situation will be rectified over time, implementing activities need guidance now to plan for migrating systems and future upgrades. This architecture is intended to be a starting point. Sections 3.D. through 3.L. describe in detail the applicable standard(s) for each of the USCG TRM service areas where consensus standards have been identified. Information is provided to assist in evaluating these standards for inclusion in application and/or organizational profiles. Section M provides additional information so that implementing activities can evaluate the risk of implementing the various standards within certain time frames.

- B. **Process and criteria.** The methodology developed by NIST in Special Publication 500-187 (Application Portability Profile) was followed in choosing standards for the architecture. Every future USCG document relating to architectures, reference models, frameworks, and standards should use the NIST APP as a baseline from which to start. In deciding to evaluate standards for incorporation into the architecture, the following criteria were used for assessing standards and supporting products by NIST:

- o Level of consensus
- o Product availability
- o Completeness
- o Maturity
- o Stability
- o De facto usage
- o Problems/limitations
- o Conformance testing

"Level of consensus" was considered the most important factor, since the standards included in the architecture have to accommodate user needs across the USCG. For example, in determining the level of consensus for standards in the APP, NIST prefers to use international standards as a basis. The process through which these international standards have evolved requires a very high level of consensus. A number of FIPS specified in the APP are based on approved international standards. The use of international standards has significant military and commercial utility for the USCG.

GOSIP is no longer mandatory. POSIT (Profiles for open Systems Internetworking Technologies) is the new standard. In general, it retains the open systems stack that GOSIP touted but now includes TCP/IP as an additional standard.

The architecture is a target towards which the USCG must be moving. The MIL-STD-187/188 series is applicable when addressing the evolution of network and telecommunication services. Additional study is required to resolve technical issues on the maturity of several approved and emerging standards before they are added to the architecture. Resolution of several conflicting standards must be accomplished. The implementation guidance provided in outlines procedure for implementing activities to submit changes and nominate new standards or services for inclusion in the architecture.

C. **Specific standards by service area.** Figure 3-1 summarizes the USCG Technical Reference Model standards. Each service area is addressed in the following sections.

D. **Software Engineering Services.** Software engineering services cover all OSE services related to the support of information systems development. These services include, but are not limited to, Computer Aided Software Engineering (CASE), programming languages, and related language bindings.

1. **Software Development environments.** +-----+

A software development environment refers to	:	Software	:
a complete, workbench-oriented environment	:	Engineering	:
for a set of integrated software development	:	Services	:
tools that spans the entire software life	:		:
cycle and integrates many functions. It	:		:
includes a set of automated tools, firmware	:	C	:
devices, and hardware necessary to test	:		:
software. Prior to the selection of an	:	Ada	:
environment or set of tools, application	:		:
system requirements and the accompanying set	:	PCTE	:
of required services should be identified.	:		:
To ensure uniformity and consistency of	:		:

+-----+

service definitions between vendors, contractors, tools, integrators, etc., the NIST SP 500-211 (Reference Model

for Frameworks of Software Engineering Environments) should be consulted.

2. **Programming Languages and Binding.**

a. Languages

Ada is a general purpose, systems programming language designed with an emphasis on reliability, readability, and maintainability. Originally intended for embedded, real-time systems development, use of Ada has extended into the Management Information Systems (MIS) community and is appropriate for a broad range of application areas. Ada is a language that enforces modern software engineering principles of data abstraction, information hiding, and modularity. The Ada-95 standard (**FIPS 119-1 or ISO/IEC 8652-95**) brings the language into line with newer software engineering concepts including extensions to improve support for real-time systems, object oriented features, and mega-programming. Ada does not allow any extensions to the language and thereby has exceptional portability. Ada is also a "strongly typed" language and supports structured programming. Ada has a strongly supported DoD certification program. Many DoD systems use Ada and the USCG can benefit from reusable Ada source code and object libraries.

C is a systems programming language which has been adopted for widespread use as a general purpose language in developing commercial applications. C is a relatively "low level" language which deals with basic computer objects, such as characters, numbers, and addresses, and does not inherently provide operations to handle composite objects, such as strings, sets, and lists. C does not support structured programming and portability as well as the Ada language. C is also not supported by a certification program.

All USCG-maintained application software that needs interoperability with other agencies shall be written in C or Ada per the standards. If the application software is unique to the Coast Guard, it may also be written in any 4GL or 5GL that is part of the standard software development suite as established by the SWIII contract. A waiver from Commandant (G-SIA) is required to develop a USCG-maintained application in any language not covered above.

b. Bindings

Language bindings are interfaces to operating systems, network software, graphical user interfaces,

database management systems, and other system software specific to a programming language. Bindings define conventions for accessing functionality of the specified subsystem. Although many standards exist or are in development for Ada bindings to OSE component subsystems, few Ada bindings are currently implemented.

C has been the language of choice among commercial software developers over the past decade for development of interface bindings for SQL, communications, windowing systems, and operating systems. This "choice" has been formalized by the explicit generation of C binding standards for various aspects of POSIX.

E. User Interface Services. The recently-awarded Coast Guard Standard Workstation III contract designated Windows NT as the standard operating system for the organization. With the Coast Guard in an NT environment, procurements should stipulate the WIN32 standard, wherever practicable. However, if interoperability is needed with an agency or organization that uses X-Windows e the procurement must consider the X-Windows standard. FIPS PUB 158-1 addresses layers 0, 1, and 2 of the User Interface System Reference Model (UISRM) which is based on the Massachusetts Institute of Technology's X Window system. Work is still in progress on Layers 3, 4, 5, and 6 and has not progressed enough to include specifications in this model on those layers. The Graphical User Interface (GUI), or Presentation issue, is being addressed.

1. **User Interface Component - FIPS PUB 158-1** +-----+
MIT X Window System). Client-server : User :
operations define the relationships between : Interface :
client and server processes operating within : Services :
a network, in particular, graphical user : :
interface display processes. In the : MS WINDOWS :
X-Windows case, the program that controls each : :
display unit is a server process, while : FIPS 158-1 :
independent user programs are client : OSF/MOTIF :
processes that request display services from : (X Windows) :
the server. The functions that constitute : :
this service area are included in Layers 0, : IEEE P1295 :
1, and 2 of the UISRM. : :
: IEEE P1201 :
+-----+

The specification for FIPS PUB 158-1 defines the primitives, intrinsic functions based on these primitives, and some of the lower-level library specifications for user interface services. It does not specify any of the "look and feel" or style services that will be accessible at higher levels of abstraction nor does it contain a full complement of utilities and services required to allow application programmers to easily program user interfaces.

The specification for FIPS PUB 158-1 is comprised of the following documents from the X Consortium, X Window System, Version 11, Release 5:

- o X Window System Protocol, X Version 11
- o Xlib - C Language X Interface
- o X Toolkit Intrinsic - C Language Interface
- o Bitmap Distribution Format 2.1

The computer program source code contained in Version 11, Release 5, is not part of the specification for the FIPS PUB. The Xlib and X Window System Protocol documents are fairly stable. X Toolkit Intrinsic will achieve a large measure of stability with the next release. Changes in these specifications are expected to include minor modifications. X Version 11, Release 4 is available from most major vendors now and can be specified as an enhancement to the FIPS PUB. Conformance to this FIPS shall be considered whether the network-based bit-mapped graphic system applications are: (1) Developed internally, (2) acquired as part of an ADP system procurement, (3) acquired by separate procurement, (4) used under an ADP leasing arrangement, or (5) specified for use in contracts for programming services.

2. **User Interface Component - IEEE P1201.** IEEE Working Group P1201 is preparing documents to address the drivability of user interfaces (e.g. the general location of symbols on the screen, what happens when a mouse click is detected, standard menu items). They have already agreed on IEEE Motif as the X-Window user interface standard. The IEEE Recommended Practice for GUI, P1201.2 specifies elements and characteristics that must be consistent to permit GUI users to easily transfer from one application to another with minimal difficulty or retraining. The standard will include recommendations for keyboards, pointing devices, menus, buttons, controls, windows, user guidance, and common user actions.

There are several human-computer interface specifications to use in developing user interfaces. One is the Draft Standard for Information Technology - X Window System Graphical User Interface - Part 1: Modular Toolkit Environment (IEEE P1295.1) which is the API to Motif. Another is the DoD published Human-Computer Interface (HCI) Style Guide which is published as Volume 8 of the Technical Architecture Framework for Information Management (TAFIM). DoD policy is to use the HCI Style Guide to tailor user interfaces along standard guidelines.

The Inter-Client Communications Convention Manual (ICCCM) from the MIT X Consortium which defines how user interface application programs communicate with each other in a system will be included in a future update of FIPS PUB 158-1. ICCCM should be used in all USCG development efforts and system procurements using a client-server computing architecture with a graphical user interface in a networked environment.

F. **Data Management Services.** The Data Management service area includes the data dictionary/directory service for accessing and modifying data about data (i.e., metadata), the database management system service for accessing and modifying structured data, and the distributed data service for accessing and modifying data from a remote database.

1. **Data Base Management System Component** -- +-----+
Structured Query Language (SQL) FIPS : Data :
PUB 127-2. Data Base Management Services : Management :
(DBMS) include the definition, management, : Services :
query, and security of structured data : :
storage in a relational database management : :
system. The security interface for granting : SQL :
and revoking privileges does not specify a : :
secure DBMS, only its interface. FIPS : RDA(future) :
PUB 127-1 is obsolete and was based on the : :
ISO SQL 9075:1989 standard. That standard : :
had minimum functionality. Every vendor had : :
to add functionality necessary for real-world +-----+
environments, and did so differently, because there
were no standards for that functionality. Consequently, no
two SQLs were compatible. A new SQL standard, ISO SQL
9075:1992, commonly known as SQL2 was defined and approved
in November 1992. SQL2 has far more functionality than SQL
'89. It has so much functionality that it was necessary to
divide SQL2 into three levels - the Entry Level, the
Intermediate Level, and the Full Level. The Entry Level is
designed to be as compatible as possible with SQL '89,
although there is not a one-for-one match. Entry Level
SQL2 products became available in 1994. However, Entry
Level SQL2 is still inadequate for real-world production
environments. Intermediate and Full Level SQL2 products
are more functional, but these SQL2 levels will take much
longer for products to be available because there is so
much to implement, debug, optimize, and test. Meanwhile,
vendors will continue to implement proprietary extensions
to support needed functionality.

To alleviate the SQL2 functionality and incompatibility problems, FIPS 127-2 has defined a fourth level called "Transition Level SQL2." Transition Level SQL2, for the most part, is a hybrid of Entry Level and Intermediate

Level SQL2. It contains the most important parts of Intermediate Level SQL2 that users need for a real-world environment. Research shows that most vendors will first implement Entry Level SQL2, and second, implement the NIST's Transition Level SQL2. Transition Level SQL2 is easier to implement than the Intermediate Level SQL2. It also gives vendors the ability to bid on Federal procurements. Some Transition Level SQL2 products entered the market at the end of 1994 and the beginning of 1995.

Most DBMS vendors have no intention of conforming to the Intermediate or Full Level of SQL2 because SQL2 Intermediate and Full Levels are very large and complex. As a result, the time necessary to add the Intermediate and Full Level features will likely exceed the time needed for the SQL3 standard to be completed. To ensure portability, as well as functionality, Coast Guard users must specify the NIST FIPS PUB 127-2 Transition Level SQL2. Specifications for access to remote heterogeneous sites are under development in an emerging ISO Remote Database Access (RDA) specification (see following paragraph 3, "Distributed Data Component.")

Specifications for distributed database management are also under development. Tools for data management such as triggers, assertions, user-defined types, domain and table hierarchies, and stored procedures are under active consideration as follow-on enhancements to the SQL standard. FIPS 127-2 became effective December 3, 1993 and is mandatory for all federal procurements of relational model database management systems.

2. **Distributed Data Component - Remote Database Access (RDA), ISO/IEC 9579-1:1993 and ISO/IEC 9579-2:1993.** RDA is used to establish a remote connection between an RDA client, acting on behalf of an application program, and an RDA server, interfacing to a process that controls data transfers to and from a database. The goal is to promote the interconnection of applications with database systems within heterogeneous environments, with emphasis on an SQL server interface. Contrary to what most people believe, SQL is designed for standalone database environments. RDA is necessary for database access in client/server environments. The two-phase commit, which is needed for distributed transaction management and distributed databases, is specified in the ISO 9804-3 and 9805-3 Commitment, Concurrency, and Recovery (CCR) standards. The ISO CCR 2-phase commit is also included in X/Open's XA and XA+ specifications for communications between a transaction manager and resource manager and between remote transaction managers. It is necessary to check and see whether and how the 2-phase commit is a part of RDA. The ISO RDA is a protocol for bidirectionally

communicating requests about remote database data. At present, the ISO RDA is limited in scope. It has been extended, however, by the SQL Access Group. The SQL Access Group specifications are published jointly with X/Open as X/Open specifications. The Coast Guard is now a member of the X/Open international consortium and has easy access to these specifications. The X/Open-SQL Access Group (SAG) specifications include the ISO RDA Protocol. They also include a series of APIs and formats that are needed for portability. In addition, the X/Open-SQL Access Group specifies a Call Level Interface (CLI) for SQL programs. This CLI allows application programs to directly call an SQL program, instead of having to embed the SQL program in a third generation programming language and then use a pre-processor to convert the embedded SQL program into the third generation language used.

In summary, the ISO RDA is an international standard and is incontestable; X/Open-SQL Access Group's RDA contains APIs and formats, in addition to just a protocol; and the SQL Access Group's X/Open's (SAG) Call Level Interface (CLI) allows SQL programs to be called directly.

RDA services consist of dialogue management, association controls, resource handling, and data language services between a single client and a single server. Association control includes making a connection to a specific database at the server site. SQL statements are sent as character strings with a separate list of input parameters, and resulting data or exception conditions are returned. Transaction management services are also included for both one and two-phase commit protocols. Individual applications determine whether one and two phase commits are available.

- G. **Data Interchange Services.** The Data Interchange service area establishes data formats for the interchange of documents, graphics data, and product description data. The parent document is MIL-STD-1840C, which is currently in final review. A summary of CALS standards is shown in Table 3-1 at the end of this section.

1. **Document Component - Standard Generalized Markup Language (SGML) FIPS PUB 15.** +-----+
 SGML is a markup language for defining : Data :
 the logical structure of documents. It : Interchange :
 provides a means to specify on the : Services :
 particular markup what is allowed, what : SGML :
 is required, and how the markup is : :
 distinguished from the text. A high : CGM :
 percentage of SGML features are available : :
 in current implementations. SGML does not : Raster :
 deal with the meaning of the markup. : :
 Markup consists of the common sets of : IGES :
 document formatting codes used in classes : :
 of document types. For example, technical : EDI :
 manuals may use a different markup from : :
 management guideline documents, due to the : IETM :
 audience and content of the respective : :
 document types, and the types of : MILSTD-1840C :
 publishing layouts that are commonly used +-----+
 for each. Therefore, SGML does not specify what to do
 after the document has been processed by an SGML
 recognizing program. Additional specifications, such as
 Document Style Semantics and Specification Language
 (DSSSL), are needed to determine the markup's meaning.
 While consensus on the SGML standard has been reached to
 some degree, there is still a great deal of definition
 required on the particular markup, i.e., Document Type
 Definition (DTD's) to be employed. SGML defines
 requirements for all of the steps involved in automated
 publishing of page-oriented technical publications. For
 exchange of source data, it defines a common
 implementation of SGML. For composition functions, it
 defines an output specification of typographic tags and
 format rules. CALS SGML, MIL-PRF-28001, is a subset of
 SGML that specifies particular fonts, tags, etc. for DOD
 use.

Although SGML is oriented to technical weapons systems support documents, its capabilities and versatility also make it the preferred standard for our business office environments. In fact, archival backups of documents that are going to be stored for a long time would benefit from storage in SGML format so they would not be constrained to a particular word processor that may not be in service at a later date when the document needs to be retrieved.

2. **Vector Graphics Component - Computer Graphics Metafile (CGM) FIPS PUB 128-1, and CALS CGM MIL-PRF-28003.** Vector graphics data interchange is specified in terms of a file format suitable for the description, storage, and communication of graphical (pictorial) information that can be created independently of device requirements and translated into the formats needed by specific output

devices, graphics systems, and computer graphics installations. CGM contains capabilities to describe and format any type of picture or drawing. It defines the use of CGM for two-dimensional vector picture descriptions or illustrations which must be included in technical publications. This revised standard became effective October 15, 1993. The use of the CGM Application Profile became mandatory for all federal procurements beginning October 15, 1994.

The problem with CGM is that it must describe every pixel and part of a graphic. The result is that when files are converted to CGM, it is not unusual for a 6,000 byte file to grow to 3/4 of a Megabyte or an entire Megabyte. At this rate, it is easy to run out of disk storage space, even on a 350-600 Megabyte disk, depending on the amount of mixed text and graphics produced. If a large amount of graphics (and image) importing and exporting is expected, it may be more practical to use a filter that converts the file directly into the graphics format used by a word- or document-processing program.

3. **Raster Graphics Component - Raster Graphics Representation in Binary Format, Including FIPS PUB 150 and CALS Raster MIL-PRF-28002.** Raster graphics data interchange includes all digital raster graphics files complying with one of the two binary formats specifically addressed as follows: Type I raster graphics binary format consists of Group 4 Facsimile encoding as defined in FIPS PUB 150, Telecommunication Standardization Sector (TSS) (formerly called the International Telegraph and Telephone Consultative Committee (CCITT) Recommendation T.6; and Type II raster graphics binary format consisting of Abstract Syntax Notation One (ASN.1) and TSS (CCITT) Recommendation T.6 encoding. (Any references in the ISTA to the CCITT, now called the TSS, will remain CCITT until the next major revision to this instruction).

Raster is used in the DOD CALS initiative to specify interchange of optically scanned engineering drawings and pages of technical publications. MIL-PRF-28002 is the specified profile for implementation of raster graphics within DOD CALS. It defines requirements for raster graphics that have been compressed to reduce file size and transmission time. Two types of requirements are defined: Type I for non-tiled images, and Type II for document architectures which support both non-tiled and tiled graphics. FIPS PUB 150 and MIL-PRF-28002 are mandatory standards for procurements requiring raster graphics.

Product Data Interchange Component - FIPS PUB 177 for Initial Graphic Exchange Specification (IGES). 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, materials properties, and surfaces. The information typically associated with computer-aided design (CAD) and computer-aided manufacturing (CAM) can be described.

IGES does not cover the complete life-cycle of manufactured products; it addresses only the specification of products, not the manufacturing process relationships. IGES defines the representation of engineering data, but does not include all interfaces for use, such as the interface between the data specification and numerically-controlled machining tools.

MIL-PRF-28000 is the specified profile for implementation of IGES within DOD CALS and specifies application subsets and protocols regarding the ANSI IGES specification. It defines subsets for technical illustrations, engineering drawings, electrical/ electronic applications, and numeric control manufacturing.

Currently the USCG-selected technology for CAD/CAM systems must be those which are interoperable with AutoCad due to our current investments in these systems.

5. **Product Data Interchange Component - Planned FIPS PUB: Standard for The Exchange of Product Data (STEP).** The STEP will be based on the ISO 10303:1994 standard. ISO 10303:1994 is a set of inter-related standards that define the vocabulary and syntax for the exchange of product data, encompassing all aspects of product data that may be collected and exchanged for any product throughout the life cycle.

Two specific applications to be included in the initial version of STEP concern the exchange of 2-D drafting data and the exchange of configuration controlled 3-D design data. ANSI sponsors a U.S. Technical Advisory Group to the ISO. STEP is also actively supported by PDES Inc., which is an industrial consortium, and the Department of Commerce, which supports STEP through NIST.

6. **Electronic Data Interchange (EDI) Component - FIPS PUB 161-1.** Electronic Data Interchange provides a mechanism for the electronic exchange of data that would be traditionally conveyed on paper documents. The expected benefits to be achieved by implementing FIPS PUB 161-1

include reduced paperwork, fewer transcription errors, faster response time for procurement and customer needs, reduced inventory requirements and more timely payment of vendors. Electronic exchange of data using EDI is governed according to established rules and formats. The data that are associated with each type of functional document, such as a purchase order or invoice, are transmitted together as an electronic message. The formatted data may be transmitted between originator and recipient via telecommunications or physically transported on electronic storage media. Implementation of EDI requires a family of interrelated standards. The family includes types of messages (also called transaction sets), transmission envelopes, data elements, and short sequences of data elements called data segments. FIPS PUB 161-1 adopts, with specific conditions, the families of standards known as ANSI X12 standards and Electronic Data Interchange for Administration, Commerce and Transportation (EDIFACT). FIPS PUB 161-1 is applicable to the interchange of data between Federal agencies and other organizations if (1) the data are to be transmitted electronically and (2) X12 transaction sets or EDIFACT messages meeting the data requirements of the interchange have been developed and approved under the conditions of FIPS PUB 161-1.

Whenever FIPS PUB 161-1 specifies the use of GOSIP protocols to transmit EDI documents, substitute POSIT protocols. While POSIT specifications for EDI protocols mature, FIPS PUB 161-1 encourages the interim use of Message Handling System (MHS) implementations built in conformance with the CCITT **1984** MHS (X.400) Recommendations. However, for new starts, USCG components will conform to the CCITT **1988** MHS (X.400) Recommendations (as specified in the NIST Special Publication 500-202, Stable Implementation Agreements for Open Systems Interconnection Protocols, and avoid use of products that conform to the 1984 Recommendation. Note that the DoD has awarded their Defense Messaging System (DMS) contract as an X.400/X.500 based system. Coast Guard procurements for systems to interface to their system will need to be compliant with the X.400/X.500 standards.

X12 and EDIFACT are separate, although similar, families of standards. Efforts are being made to align the standards by the end of 1996. FIPS PUB 161-1 recommends the use of X12 standards for domestic applications and X12 or EDIFACT for international exchanges. Both families of standards may be employed to meet organizational needs. Coast Guard and DOD Components that implement EDI systems are required to conform to FIPS PUB 161-1. Coast Guard and DOD components that implemented EDI systems before September 1991, using

industry-specific standards, have until 30 September 1996 to convert to the standards specified in FIPS PUB 161-1.

7. **Interactive Electronic Technical Manuals (IETM)** -- Interactive electronic technical manuals are being developed by the Navy for use throughout DoD and are represented in the CALS standards as MIL-M-87268, MIL-D-87269, and MIL-Q-87270.
8. **CALS Specifications.** Table 3-1 summarizes the SGML, CGM, Raster, and IGES Standards and their associated CALS specifications mentioned in previous sections. In addition to the specifications included in the table, MIL-STD-1840C, Automated Interchange of Technical Information, acts as an umbrella document for the other CALS standards and specifications. It identifies the technologies and standards under CALS for the automated interchange of technical information.

Table 3-1. CALS Specifications

DATA INTERCHANGE COMPONENT	NIST STANDARD	CALS SPECIFICATION
Document Interchange	FIPS PUB 152 (SGML)	MIL-PRF-28001
Vector Graphics	FIPS PUB 128-1 (CGM)	MIL-PRF-28003
Raster Graphics	FIPS 150 (Group 4 FAX)	MIL-PRF-28002
Product Data Interchange	FIPS PUB 177 (IGES)	MIL-PRF-28000

- H. **Graphics Services.** The Graphics Services area provides the interfaces for programming two and three-dimensional graphics in a device-independent manner. The specification included in this are the Graphical Kernel System (GKS) FIPS PUB 120-1, and the Programmer's Hierarchical Interactive Graphics System (PHIGS) FIPS PUB 153. They are targeted at different types of users and applications. The apparent trend is to standardize in favor of PHIGS since a PHIGS extension to X Windows (PEXP) is included in FIPS 158-1.

1. **Graphical Kernel System Component - FIPS PUB 120-1.** This 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).

The standard includes library calls for virtually any kind of two-dimensional graphic image. GKS is well established, limited to two-dimensional graphics, and well supported by the computer industry, but it is minimal, and other capabilities are needed. Use of NIST FIPS PUB 153 and ISO/IEC 9592-4:1992 (PHIGS and PHIGS Plus respectively) is preferable to the use of GKS.

```

+-----+
: Graphics :
: Services :
:          :
:          :
: PHIGS    :
:          :
: PHIGS PLUS :
:          :
: GKS      :
: (legacy) :
:          :
+-----+

```

2. **Programmer's Hierarchical Interactive Graphics System (PHIGS) Component - FIPS PUB 153.** This specification fulfills the requirement for a language to program two and three-dimensional graphical objects that will be displayed or plotted on appropriate devices in interactive, high-performance environments, and for managing hierarchical database structures containing graphics data. PHIGS is a full-functioned specification for the development of interactive two-and three-dimensional graphics applications which manage hierarchical database structures containing graphics data. Bindings for the C language have been adopted.

A new standard called PHIGS Plus (ISO/IEC 9592-4:1992), adds shading, lighting, and other advanced graphics programming capabilities that were not included in PHIGS. Conforming PHIGS programs will be able to execute under PHIGS Plus with no change. Most implementations of PHIGS provide extra features that are not part of the PHIGS standard, but are often unnecessary. These features should be avoided if possible, since unique features limit portability. PHIGS Plus is preferable to PHIGS and GKS and should be specified in all Coast Guard procurements where graphical services are required.

I. **Network Services.** This service area includes telecommunications, data communications, transparent file access, personal/microcomputer support, and distributed computing support. Service areas related to telecommunications are voice, telephone, data transmission, facsimile, record traffic, and video support.

1. **Data Communications Component - Profiles for open Systems Internetworking Technologies (POSIT), FIPS PUB 146-2.** +-----+
 FIPS 146-1, the old GOSIP standard, is no longer supported by NIST and is NOT required for Federal information technology procurements. The new standard is POSIT, FIPS PUB 146-2. POSIT maintains the open system standard that GOSIP required but makes more protocols part of the open system specification, such as TCP/IP. In addition to FIPS PUB 146-2, MIL-STD-187-700A provides a broad profile of network services standards that can be used to meet POSIT requirements. Also, the Government Network Management Profile (GMMP) is in the process of being rewritten.

The primary objectives of these standards are to:

- o achieve interconnection and interoperability of computers and systems that are acquired from different manufacturers in an open systems environment;
- o reduce the cost of computer network systems by increasing alternative sources of supply;
- o facilitate the use of advanced technology by the Federal Government; and
- o provide guidance for the acquisition and use of networking products implementing open, voluntary standards such as those developed by the Internet Engineering Task Force (IETF), the ITU, and the ISO.

Periodic updates, upwardly compatible with current versions, are planned to coincide with maturing international standards and product availability. In a future revision of POSIT, NIST plans to offer additional guidance on the acquisition and use of Internet and OSI protocol suites.

2. **Telecommunications Component - Interoperability and Performance Standards for the Defense Information System (MIL-STD-187-700A).** This new planning standard ensures that end-to-end interoperability will be achievable between and among all users of the Defense Information System (DIS) in both the near and long term. MIL-STD-187-700A references mature-draft and approved standards.

It can be viewed as a "standard of standards", one that references those specific sections of commercial, federal, and military standards that are applicable to DIS. MIL-STD-187-700A also provides detailed technical information that relates to draft anticipatory standards, thus helping USCG and DOD acquisition authorities plan future systems that meet new DIS requirements. MIL-STD-187-700A contains the technical standards necessary to allow strategic and tactical users to exchange all forms of information digitally. It addresses those interoperability, performance, and interface standards that must be met by future USCG and DOD information systems to provide a wide variety of end-to-end digital subscriber services in an integrated network.

The development of MIL-STD-187-700A was influenced by several factors. Higher-performance processing systems and the provision of intelligent networks are new trends that will affect DIS. These trends will accompany the introduction of ISDN for base-level and long-haul systems, whereas the tactical systems will evolve to all digital systems based on Tri-Service Tactical Communication Systems (TRI-TAC) specifications. In the future, broadband-ISDN (B-ISDN) services will become part of DIS to provide switched broadband video service, switched multi-megabit data service (SMDS), flexible multi-party conference service, and bidirectional distribution service with subscriber control. Tactical assets have limited capability for broadband services, due to spectrum limitations. In the long-term, the tactical architecture will depend on the asynchronous transfer mode (ATM), thus it will move away from channel limitations caused by the present synchronous transfer mode (STM). MIL-STD-187-700 also provides guidance on how to handle the transition from existing data communications systems to POSIT compliant systems.

3. **Federal Building Telecommunications Wiring Standard - FIPS PUB 174.** This standard, by adoption of ANSI/EIA/TIA-568-1991, Commercial Building Telecommunications Wiring Standard, specifies minimum requirements for telecommunications wiring within a building and between buildings in a campus environment. It specifies a wiring system with a recommended topology and recommended distances.

It also specifies copper and optical-fiber transmission media by parameters that determine performance, and specifies connectors and their pin assignments to ensure interconnectability. This standard recognizes a background precept of fundamental importance: it is imperative that the telecommunications wiring design be incorporated during the preliminary architectural design phase. The purpose of this standard is to facilitate

interoperability and transportability among telecommunication facilities and systems of the Federal Government and compatibility of these facilities and systems at the computer-communications interface with data processing equipment (systems) of the Federal Government by specifying standard characteristics for building telecommunications wiring. This standard defines a generic, functional telecommunications wiring system for Federal buildings that will support a multiport, multivendor environment. The further purpose of this standard is to enable the planning and installation of building wiring with little knowledge of the telecommunications products that subsequently will be installed.

Adherence to a standard that specifies standardized building wiring contributes to the economic and efficient use of resources by avoiding the proliferation of local or vendor-unique standards, and is necessary to facilitate development of interoperable inter- and intra-building telecommunications systems. Specification of minimum acceptable values for basic performance parameters provides assistance to the user in multivendor systems. For the user requiring state-of-the-art systems performance, these values may serve as benchmarks for use in cost/performance analyses when evaluating alternative transmission media whose specifications exceed those of this standard. The use of this wiring standard by Federal departments and agencies is compulsory and binding for the construction of new buildings and the rehabilitation of existing buildings effective March 1, 1993.

4. **Video Teleconferencing Component - FIPS PUB 178.** This standard details video teleconferencing services at 56 to 1,920 kb/s, which supports the design and development of video teleconferencing systems. The referenced specifications for FIPS 178 are the CCITT recommendations H.320, H.221, H.242, H.261, and H.230, developed by CCITT with federal government assistance. Systems developed under this standard will be more cost effective and will facilitate the interoperability of products and services from different suppliers.
5. **Interoperability and Performance Standard for Video Teleconferencing - MIL-STD-188-331.** MIL-STD-188-331 is another video teleconferencing standard available for use which provides DOD with interoperability between video teleconferencing (VTC) terminals. This point-to-point video teleconferencing standard covers motion video, audio, still images, data, and security. This standard also includes video teleconferencing units (VTUs) and it also addresses cryptographic devices, but not

input/output equipment such as cameras, monitors, microphones, and speakers. Use of this standard assumes a network is operational to support communication between VTC terminals. This standard specifies the minimum requirements for DOD interoperability and also specifies optional features. If a requirement exists to interface and/or operate with cryptographic equipment for classified operation, this standard is mandatory. The capability to encrypt and decrypt unclassified sensitive information is optional. This standard is also recommended for DOD contractors and anyone else who needs to hold a video teleconference with DOD. It can be used in the design and installation of new VTC terminals and subsystems and in the authorized upgrading of existing VTC subsystems and equipment.

DOD and the Joint Staff have expressed an urgent need for a follow-on standard for multipoint conferencing (three or more sites connected in a single conference). Designated MIL-STD-188-331A, it will supersede MIL-STD-188-331 and include everything in MIL-STD-188-331 plus the multipoint features.

6. **Integrated Services Digital Network (ISDN) - FIPS PUB 182.**

This standard defines the generic protocols necessary to establish transparent ISDN connections among Government networks and between Government and conformant common carrier networks. The standard provides a minimal set of bearer services, and is based on international, national, and implementation agreements developed by the North American ISDN User's Forum (NIU-Forum). This standard supports a range of integrated services including voice, data, imagery, and video services. The standard is consistent with FIPS PUB 146-2, POSIT, which provides protocols for computer to computer data communications using ISDN as a lower layer network technology. The primary objectives of this standard are:

- o to achieve interconnection and interoperability of user and network equipment that are acquired from different manufacturers in an open systems environment;
- o to reduce the costs of acquiring user equipment for ISDN services;
- o to facilitate the use of advanced technology by the Federal Government;
- o to stimulate the development of commercial products compatible with ISDN standards.

This standard shall be used by USCG personnel for the acquisition of ISDN Customer Premise Equipment (CPE), switches, and ISDN services implementing the protocols specified within the standard. This standard became effective April 15, 1994 and should be cited in solicitations and contracts when the services or products to be acquired require the functionality specified in this standard, if conformant products and services providing the desired functionality are available, or are expected to be available, for delivery within the terms of the solicitation or contract. Acquisition agents may specify that a procurement request which is based on this FIPS require offerers to provide either evidence of conformance to the ISDN FIPS or to provide explicit evidence of the capability of a migration path towards conformance to the FIPS for the products and services offered in response to the procurement request. Even when conformant products and service provider offerings are not yet available, it is recommended to use this standard to the greatest extent possible, and to follow the recommendations of any subsequent user guidelines to this standard issued by NIST. Future versions of this FIPS will provide protocols for additional services, teleservices, and applications.

- J. **Operating System Services.** The operating System (OS) services area includes kernel operations, shell and utilities, system management, and security.

```

+-----+
: POSIX.1      POSIX.5 (Ada)                      POSIX.6 :
:              Operating System Services          :
: POSIX.2                      GNMP (future)     :
+-----+

```

- 1. **Kernel Operations Component - Portable Operating System Interface for Computer Environments (POSIX.1) FIPS 151-2.** The Portable Operating System Interface for Computer Environments (POSIX) consists of a family of related specifications which are intended to promote the source code portability of application programs across a heterogeneous platform environment often referred to as an open system environment. The different specifications within POSIX are at various degrees of maturity with POSIX.1 being the most mature.

POSIX.1 focuses upon kernel operations including low-level services necessary to create, manage, and terminate processes; execute programs; manage interprocess communication; manage files and directories; and control input and output. IEEE POSIX.1 now includes the real time extensions. The old POSIX.4 (P1003.4) real-time extension was formally approved and renamed IEEE 1003.1b.

The ISO numbering scheme has not been determined, but it will likely be similar. The rationale is to make all 1003.1 and 9945-1 interfaces refer to system programming interfaces. All 1003.2 and 9945-02 interfaces will refer to shell, commands, and utilities. All 1003.3 interfaces will refer to system administration (which are presently 1003.7). The present 1003.3 conformance testing services and standards have also been renamed as IEEE 2003. Existing kernel operations will not change, although additional operations are on the horizon. Related standards for other service components, such as system management, will be developed over the next several years.

FIPS 151-2 is a mandatory requirement in Federal information technology procurements. Further, NIST has established compliance testing for FIPS 151-2. Contractors should be required to provide proof of POSIX compliance through a NIST-approved voluntary compliance laboratory using the NIST developed conformance test suite. In addition, contractors shall be required to comply with upgrades to FIPS PUB 151-2 in accordance with directives in the revised FIPS. On 12 May 1993, NIST issued FIPS 151-2 that adopts International Standard (ISO/IEC 9945-1), Information Technology - Portable operating System Interface (POSIX) - Part 1: System Application Program Interface (API) (C Language) which define. a C programming language source interface to an operating system environment.

2. **POSIX.2 - Shell and Utilities Component - Portable Operating System Interface for Computer Environements - FIPS 189.** POSIX.2 defines a standard source code level interface to command interpretation or shell services and common utility programs for applications programs. The standard deals with the basic shell programming language and a set of utilities required for the portability of shell scripts. It also standardizes command line and function interfaces related to POSIX.2 utilities. A user portability utilities option standardizes user interaction for commands that are fundamental to any user's effective interaction with the operating system services. This standard is compulsory and binding for use in all solicitations and contracts for new operating systems and/or applications development where POSIX shell and utility interfaces are required and became effective April 3, 1995.
3. **System Management Component - FIPS PUB 179, Government Network Management Profile (GNMP).** The GNMP specifies the initial set of common management information exchange protocol and services, specific functions and services, and the syntax and semantics of the management information required to support monitoring and control of

the network and system components and their resources. System management includes the capabilities of defining and managing user access, devices, file systems, administrative processes (Job accounting), queues, machine/platform profiles, authentication (passwords), authorization of resource usage, and system backup on single platforms or in environments composed of heterogeneous networked platforms.

The GNMP specification (FIPS PUB 179) is based on the OSI Reference Model and is being revised. The revision is due out in late 1996 and will incorporate POSIT requirements as well as requirements from the Management Information Base for Internet Standards (MIL-STD-2045-17507-2 and -3) and the Internet Transport Profile (MIL-STD-2045-14502-1, and -3). The revised FIPS PUB 179 will be mandatory. Until then, the current FIPS PUB 179 along with the 5 MIL-STDS identified above should be used to specify the System Management component. The present versions of GNMP (Version 1 and Version 2) address network management only. Version 1 addresses OSI Layers 1 and 2 for local area network (LAN) communication standardization, and version 2.0 addresses OSI Layers 3 through 7. Version 3.0 (application services and operating system interface) will add functionality and include complete component descriptions. It is important to specify GNMP because GNMP includes the definition of many objects not specified by ISO or other organizations (e.g., for modems, routers, hubs) as well as security levels needed for government organizations.

- K. **Security Services and System Management Services.** These services include security services and system management services that relate to the overall Technical Reference Model.

+-----+	+-----+	+-----+
:	:	:
: Security Services	: System Management Services	:
:	:	:
+-----+	+-----+	+-----+

- 1. **Security Services.** Security services are relevant to most areas of the Technical Reference Model. Standards in the security services area address evaluation of software components to provide secure services, as well as interface standards and data formats. Evaluation criteria standards address the general functional characteristics and development constraints for software components. In 1985, DOD issued Standard 5200.28-STD, entitled: "DOD Trusted Computer System Evaluation Criteria (TCSEC)," also referred to as the "Orange Book". The Orange Book is intended to support the evaluation of trusted operating systems and computer subsystems and is

mandatory for DOD systems since DOD policy states that all systems must as a minimum comply with C2 criteria as defined by the TCSEC. The TCSEC was developed by the National Computer Security Center (NCSC) which also issued the Trusted Network Interpretation (TNI) (NCSC-TG-005) and the Trusted Database Interpretation (TDI) (NCSC-TG-021). These documents extend the Orange Book to include criteria in the network and database areas and are also mandatory.

Security standards related to national security systems must be approved in accordance with the National Policy for the Security of National Security Telecommunications and Information Systems (NSD-42). ISO 10745:1993 (OSI Upper Layer Security Model) and ISO GULS 11586-1:1994 (Generic Upper Layer Security, part 1 - Overview, Models, and Notation) are final ISO standards. In addition, ten specifications containing four protocols have been prepared to support the development of standards for security services. These have been published in three NIST publications: "Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols, NISTIR 90-4250; Secure Data Network System Access Control Documents, NISTIR 90-4259: and Secure Data Network System Key Management Documents, NISTIR 90-4262.

Two of the four protocols addressed in these documents are moving through ANSI and ISO toward international standards status. These address security services at Layer 3, Network Layer Security Protocol (NLSP) and Layer 4, Transport Layer Security Protocol (TLSP) of the OSI reference model. The IEEE has developed a security services protocol standard for interoperable LAN Security, IEEE 802.10B-1992. The Defense Intelligence Agency (DIA) and DOD Intelligence Information System (DODIIS) communities have adopted a minimal set of security standards to be compliant with the compartmented mode of operation requirements as specified in the Director for Central Intelligence Directive (DCID) 1/16. These standards and products are recommended for use in Coast Guard procurements and include:

- o DIA Document DDS-2600-5502-87, "Security Requirements for System High and Compartmented Mode Workstations (CMW)."
- o DIA Documents DDS-2600-6243-91 and -92, "Compartmented Mode Workstation Evaluation Criteria" an interpretation of the technical security requirements of DRS-2600-5502-87 above in terms of DOD 5200-28-STD. These documents describe the CMW requirements as a superset of the B1 TCSEC requirements found in DOD 5200.28-STD.

- o DIA Document DDS-2600-6216-91, "Compartmented Mode Workstation Labeling Encoding Format" which describes the Government developed code supporting the translation of security labels in both directions between human readable and bit-encoded forms necessary for well formed labels and accurate adjudication of label combinations.
2. **Secure Hash Standard - FIPS 180-1 on Computer Security.**
This standard specifies a Secure Hash Algorithm (SHA) which can be used to generate a condensed representation of a message called a message digest. The standard is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required for federal applications. The SHA may be used with the DSA in electronic mail, electronic funds transfer (EFT), software distribution, data storage and other applications which require data integrity assurance and data authentication. The SHA may also be used whenever it is necessary to generate a condensed version of a message. The SHA may be implemented in software, firmware, hardware, or any combination thereof. Only implementations that are validated by NIST will be considered as complying with this standard. This standard is applicable to all Federal departments and agencies for the protection of unclassified information that is not subject to section 2315 of Title 10, United States Code, or section 3502(2) of Title 44, United States Code.
3. **Automated Password Generator - FIPS 181 for Computer Systems, effective 25 March, 1994.** This standard specifies an algorithm for generating pronounceable passwords that can be remembered easily by users but that are more difficult to compromise than those passwords selected by users directly. The objectives of this standard are to:
- o improve the administration of password systems that are used for authenticating the identity of individuals accessing computer resources or files:
 - o provide a standard automated method for producing pronounceable passwords that have no association with a particular user;
 - o produce passwords that are easily remembered, stored and entered into computer systems, yet not readily susceptible to automated techniques that have been developed to search for and disclose passwords.

This standard is applicable to the development of procurement or design specifications for implementing an automatic password generation algorithm within a computer system and shall be used by all Federal departments and agencies when there is a requirement for computer generated pronounceable passwords for authenticating users of computer systems or for authorizing access to resources in those systems.

This standard does not require the use of passwords in a computer system, but establishes an automatic password generation algorithm for use in systems where an agency's computer security policy requires computer generated pronounceable passwords . The Automated Password Generator uses the Electronic Codebook (ECB) mode of the Data Encryption Standard (DES), FIPS PUB 46-2, as the random number generator. This mode of operation is specified in FIPS 81, DES Modes of Operation. This standard should be used in conjunction with FIPS PUB 112, Password Usage Standard, which specifies basic security criteria for the design, implementation, and use of passwords.

4. **Digital Signature Standard (DSS) - FIPS 186 for Digital Signature Generation and Verification, effective 1 December, 1994.** This standard specifies a Digital Signature Algorithm (DSA) appropriate for applications requiring a digital rather than written signature. The DSA digital signature is a pair of large numbers represented in a computer as strings of binary digits. The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified. The DSA provides the capability to generate and verify signatures. The DSA may also be used in proving to a third party that data was actually signed by the generator of the signature. The DSA is intended for use in electronic mail, electronic funds transfer (EFT), electronic data interchange (EDI), software distribution, data storage, and other applications which require data integrity assurance and data origin authentication. The DSA may be implemented in software, firmware, hardware, or any combination thereof. NIST is developing a validation program to test implementations for conformance to this standard.

This standard is applicable to all Federal departments and agencies for the protection of unclassified information that is not subject to section 2315 of Title 10, United States Code, or Section 3502(2) of Title 44, United States Code. This standard shall be used in designing and implementing public-key based signature

systems which Federal departments and agencies operate or which are operated for them under contract. Adoption of this standard is available to private and commercial organizations.

The DSS is efficient, compatible with the current mix of government applications, and suitable for future directions as well. From a security standpoint, the DSS provides the required protection without unnecessarily putting trust in processing components.

Use and compliance with the security standards identified in the Information Systems Technology Architecture do not constitute authorization to process classified data. COMDTINST M5500.13 (series), AIS Security Manual and other applicable USCG policy covering the accreditation process must still be adhered to in order to obtain approval for the processing of classified data.

5. **System Management Services.** Refer to Section J, Operating System Services, for a description of network management services.

L. **Communications, Information Interchange, and Users.** USCG communications whether land-based or mobile consists of:

- o Transmission means
- o Switching means
- o Network means

```
+-----+
:           :      Information      :           :
:   Communications   :      Interchange   :       Users   :
:           :      (Hardware)      :           :
+-----+
```

Transmission means may consist of cellular telephone, UHF/VHF/FM or satellite. For example, ship-shore-air communications will continue to use radio and satellite communications with the addition of cellular phone for close-to-shore communications.

Shore-to-shore voice will be supported primarily through the FTS-2000 and commercial networks. Switching means, which these rely on, are provided via Private Branch Exchanges (PBX's), bridges, routers, or gateways. Network means consist of our USCG Data Network, the X.25 Public Network, and others. Major consolidations of data networks will evolve with the future requirements supplied by the CGDN, Defense Data Network (DDN), and leased lines.

Our information interchange consists of:

- o Computers and workstations
- o Peripheral devices
- o Storage devices
- o Hardware components

In order for our information interchange to occur, USCG Computers and workstations currently employ the Unisys cluster workstations which uses the vendor's operating system. Where the number of connections, application size, or data integration needs make the Unisys cluster inadequate, minicomputers are a secondary option. Only if the Standard Workstation cluster cannot fulfill user requirements will the minicomputer platform be used.

The Super Minicomputer Program (SMP), formerly AFCAC - 300 joint procurement contract is the standard minicomputer solution. As always, future purchased peripheral, storage, and hardware components must all be interoperable with our Coast Guard Standard Workstations (CGSW).

M. **Assessment of standards availability.** Planning for migration to an open systems environment must include an evaluation of the availability of formally approved and stable standards and supporting products. Standards availability for the services of the architecture have been analyzed by G-SIA and fall into the following categories:

- o **NOW** - Standards that are reasonably mature with products that are available today or are expected to be available in the nearfuture. USCG users would be reasonably safe in making substantial investment and long-term plans covering mission critical systems and infrastructure needed to support them. Any changes to the standards are expected to be upwardly compatible.
- o **FUTURE** - Standards that are subject to change but appear to be headed for stability. Some of these standards are subject to change that may not be upwardly compatible. There are some long term risks involved.
- o **GAP-FILLER (GAP)** - Standards that are available as temporary gap-filler measures and are recommended for use only if the USCG is willing to take a moderate investment risk. These standards are indicators of the long term direction of the consensus building community, but no guarantee can be made that the final standard will conform to the current proposal.
- o **VOID** - There are no standards available in these service areas. The absence of standards translates into significant risk for long-term planning and investment.

A summary of standards availability by service and service area is shown in Table 3-2. This table is a combination of the USCG Profile of Standards and a number of other standards that may be incorporated into the profile by the G-SIA Staff at a later date.

Where multiple standards are noted for a given service, the Coast Guard preferred standard is indicated by an "*". A waiver is required from Commandant (G-SIA) to plan, procure, or implement a system which does not comply with the USCG Profile of Standards.

Estimated dates for availability of these additional standards are shown to assist acquisition, system upgrade, or system replacement planning. FUTURE or GAP standards that appear to be headed for approval by national or international standards bodies should be specified in all acquisition documents through a "technology insertion" clause. For example, in the specific case of operating systems, where applicable, contractors should be required to comply with the emerging POSIX standards, developed by the IEEE POSIX Working Groups, and subsequently published in draft or future FIPS.

Table 3-2. Summary of Standards Availability

Service Areas	Service	Stds Status	Standard(s)
Operating System	Kernel	Now	FIPS PUB 151-2 (POSIX.1)
	Shell and Utilities	Now	FIPS PUB 189
	Realtime Extensions	Future	FIPS PUB 151-2* IEEE 1003.1b:1993
	Security	Now	DoD 5200.28-STD (TCSEC)
	Communication of Mgmt Information	Future	Gvmt Network Mgmt Profile (GNMP, old FIPS 179)* MIL-STD-2045-38000
Programming Languages	Programming Languages	Now	FIPS PUB 160 (C) FIPS PUB 119-1 (Ada) ISO/IEC 8652-95 (Ada)
	Case tools	Emrg'g	NIST SP 500-211
	Security	Void	- - - -
User Interface	Client/server Operations	Now	WIN32 API* FIPS PUB 158-1 (X Window system)
	Object Definition & Management	Now	DoD Human Computer Interface (MCI) Style Guide (Vol 8 of TAFIM)
	Window Management	Now	WIN32 API* FIPS PUB 158-1 (X-Window system)
	Dialogue Support	Future	IEEE P1201.2
	Security	Void	- - - -

Table 3-2. Summary of Standards Availability

Service Areas	Service	Stds Status	Standard(s)
Date Management	Data Dictionary/Directory	Now	FIPS PUB 156 (IRDS)
	Date Management	Now	FIPS PUB 127-2 (SQL)
	Remote Date Access	Future	Remote Database Access (RDA) ISO/IEC 9579-1:1993 ISO/IEC 9579-2:1993
	Security	Void	- - - -
Date Interchange	Document Interchange	Now	FIPS PUB 152 (SGML)* MIL-PRF-28001 (CAL S SGML)
	Vector Graphics Data	Now	FIPS PUB 128-1 (CGM)* MIL-PRF-28003 (CAL S CGM)
	Raster Graphics Data	Now	FIPS PUB 150* MIL-PRF-28002 (CAL S Raster)
	Product Data Interchange	Now	FIPS PUB 177 (IGES)* MIL-PRF-28000 (CAL S IGES)
	Product Data Interchange	Now	ISO 10303:1994 (STEP)
	Electronic Data Interchange	Now	FIPS PUB 161-1 (EDI)
	Security	Void	- - - -
Graphic Services	Graphics	Now	ISO/IEC 9592-4:1992 (PHIGS+)* FIPS PUB 153 (PHIGS) FIPS PUB 120-1 (GKS legacy)

Table 3-2. Summary of Standards Availability

Service Areas	Service	Stds Status	Standard(s)
Network Services	Data Communication	Now	FIPS PUB 146-2 (POSIT)
	Video		FIPS PUB 178*
	Tele-conferencing	Now	MIL-STD-188-331
	Transparent File Access	Future	IEEE P1003.8
	Personal Microcomputer Support	Void	- - - -
	Distributed Computing	Future	Draft OSF specification (NCS/RPC)
	Telecomms Wiring Standard	Now	FIPS PUB 174
	Telecomms Pathway & Spaces	Now	FIPS PUB 175
	Telecomms (ISDN)	Now	FIPS PUB 182
	Telecomms Inter-operability	Now	MIL-STD-188-700A

Table 3-2. Summary of Standards Availability

Service Areas	Service	Stds Status	Standards (s)
	Security	Now	ISO 7498-2
	Architecture		
	Trusted Netwk Interpretation:	Now	NCSC-TG-005 (TNI)
	Trusted DBase Interpretation:	Now	NCSC-TG-021 (TDI)
	Interoperable LAN security	Now	IEEE 802.10B-1992
	Evaluation Criteria	Now	DoD 5200.28-STD
	Compartmented Mode Wrkstn	Now	DDS-2600-5502-87
	Compartmented Mode Wrkstn Eval criteria	Now	DDS-2600-6243-91
	Compartmented Mode Wrkstn Labeling: encoding format	Now	DDS-2600-56216-91
	Secure Hash Standard	Now	FIPS PUB 180-1
	Automated PW Generator	Now	FIPS PUB 181
	Digital Signature Standard	Now	FIPS PUB 186 (DSS)

Federal Information Technology (IT) standards are divided into three basic types: FIPS, Military Standards (MIL) and Federal Standards (FED-STDS). FED-STDS are applicable only to the following technologies: radar, sonar, radio, television, and telecommunications terminology. All other information technology standards including wiring and cabling, raceways, grounding, bonding, shielding, are FIPS or MIL.

Policy for the use of Federal standards in the acquisition of FIPS resources is specified in paragraph 201-20.303 of the Federal Information Resources Management Regulation (FIRMA), dated 1 October 1990. The policy requires agency personnel to review each standard for applicability to the agency requirement and to ensure that all applicable Federal standards are included in a solicitation. The policy also encourages agencies to use interim Federal standards when acquiring FIPS resources. When Federal standards do not exist, the policy states that agencies should consider the use of voluntary national and international standards. If no voluntary standards exist, the policy states that agencies shall consider the development and use of agency-unique standards, provided that such use is not in violation of the "Competition in Contracting Act," and their use is coordinated with NIST. This is one of the missions of the office of G-SIA which provides this service.

Any standard, besides those contained in the USCG Profile of Standards, should be considered as part of current system development/ migration plans using the "technology insertion" approach. In cases where no prediction can be made regarding the future status of the standard, implementing USCG activities may be taking significant technical risk in adopting any current "de facto standard products" to satisfy long-term user needs. System developers should also use a "technology insertion" clause in acquisitions to ensure contractor compliance with future standards even in these less predictable service areas.

This section of the Information Systems Technology Architecture document will be updated periodically to keep pace with the rapid evolution of standards. Due to the particular interest in operating system standards, Table 3-3 provides additional status on the development of POSIX standards.

Chapter 4. IMPLEMENTATION GUIDANCE

A. **Challenges.** The challenges facing the USCG, DOD, other government agencies, industry, and implementing activities in migrating to open systems can be grouped into three areas:

- o Standards gaps
- o Implementation
- o Conversion

B. **Standards gaps.** Although most of the service areas depicted in the Technical Reference Model are populated with consensus standards, there are many service areas where standards either do not exist or are still under development. For example, many emerging standards identified by NIST are available as "open" specifications, (i.e., they are maintained by a public consensus forum and can be obtained by any interested vendor). Current acquisition regulations do not permit specification of emerging standards in solicitations. NIST is working with GSA to change the appropriate acquisition regulations. New service requirements may arise that will also lead to the need for additional standards. Implementing activities should anticipate these changes and plan for technology insertion in their system development process.

C. **Implementation.** Portability of applications and interoperability of information systems is hindered by the lack of "complete" standards. Many commercial implementations tend to trail the approved standards by several years. Vendors traditionally compensate for the less-than-complete capabilities of standard-conforming products by offering "value-added" features. These features are inconsistently implemented between different vendors and may be used to protect a particular vendor's market niche. For example, FIPS PUB 158-1 only satisfies the requirements of the lower three layers of the User Interface Service Reference Model. Services in the upper four layers must be provided by vendor-unique applications. These vendor products, (e.g., Motif , Open Look , etc) do not permit portability of applications across different window systems.

NIST recommends a strategy of developing a window system interface that makes applications portable across these products. NIST supports development of this window interface standard through the IEEE P1201 committee. For those services not supported by FIPS PUB 158, implementing activities should specify a requirement for application portability and future support of the P1201 standards. Implementing activities must

also minimize the use of vendor-unique features that would prohibit portability of applications to different platforms.

Current USCG Standard software/hardware/communications (services) are provided via the following Selected Technologies:

Technology Services	USCG Selected Technology
Office Applications	CGSW Unisys Cluster/SMP computers
Messaging	CGSW-II operating B-mail (X.400 is the long-term direction for electronic mail)
End User Computing/ Decision Support	CGSW with USCG approved file transfer, spreadsheet, & 4GL/DBMS software.
Teleconferencing	56 to 1,920 Kb/s, (see CCITT Recommendations H.320, H.221, H.242, H.261, H.230, FIPS PUB 178 & MIL-STD-188-331).
Computer Aided Design	PC which will operate AutoCad software.
Online/Batch work (in order of preference)	1st : CGSW-III 2nd : SMP computers 3rd : Mainframe
Embedded systems	Systems using external data communications will comply with the ISTA standards, MIL-STDS, MIL-SPECS, & FIPS.
Tactical Systems	TAG-III/IV, DTC-II, Loran Monitoring, and Vessel Traffic System (VTS).
Ship-to-shore-to-air Telecommunications	Satellite & HF/VHF/UHF communications with cellular phone for close to shore.
Shore-to-shore voice Classified	FTS-2000 and commercial networks. USCG Secure Data Network, Defense Data
Telecommunications	Network, or STU-III.

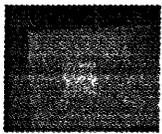
USCG implementation of the standards for future systems will consist of using:

- o The Coast Guard Standard Workstation (CGSW-III) for microcomputers,
- o U.S. Navy TAC III/IV series of computers for workstation applications that exceed the CGSW-III capabilities and,
- o Super Minicomputer Program (SMP) systems.

These are the solutions the Coast Guard is using to move to a Coast Guard open Systems Environment. They are required unless a waiver is obtained from Commandant G-SIA).

- D. **Conversion.** Conversion from the Coast Guard's proprietary CGSWII system to SWIII is addressed in Commandant (G-STC) Migration Management Plan. Solutions for converting other proprietary systems to an open systems environment to meet information systems requirements should be considered on a business case basis. Implementing activities should consider the degree to which the new open system/subsystem must co-exist or be interoperable with legacy systems during transition. A total "grand design" conversion from an existing proprietary system may exceed the operational or technical capabilities of the organization. A transition strategy that plans for the expeditious replacement of inefficient proprietary subsystem/components with products conforming to standards may be the best solution, from both an operational and technical perspective.
- E. **Implementation planning.** Implementing activities should apply the following guidelines for specific information system modernization programs:
- o **Technology refreshment.** Implementing activities should ensure that technology refreshment clauses are included in procurement solicitations. These clauses should specify standards which will mature within 3 to 5 years of the solicitation.
 - o **Avoidance of proprietary environments.** Implementing activities should ensure that information system modernizations are not based upon vendor-proprietary environments. The use of gap-filler standards is preferred over the use of proprietary products.
 - o **Selection of standards.** Table 4-1 presents guidance for the selection of standards.

Table 4-1. Standards Decision Guidance

Can a Reference Model Std Provide Required Service?	Can a non-reference Model Std Provide Required Service?	Are Compliant Products Available?	THEN...
YES		YES	Use of the standard is mandatory
		NO	Use a GAP-filler standard and plan for a transition to a reference model standard.
NO	YES	YES	Use commercial product and plan for technology insertion.
		NO	Custom products or development required. Plan for technology insertion.
	NO		Custom products development required.

Note: The status of the standards is provided in Table 3-2 and can be used to apply this decision table. Table 3-2 will be updated periodically to reflect changing status of emerging standards.

Standards Decision Guidance

Note: The status of the standards is provided in Table 3-2 and can be used to apply this decision table. Table 3-2 will be updated periodically to reflect changing status of emerging standards.

Implementation planning should be based on a high level mission area strategy that identifies opportunities for streamlining business activities or improving business practices. From these higher level requirements, the implementing activity can then develop an application/database architecture. The applications/database architecture can then be examined to identify functions that can be fulfilled with common products and reusable utilities.

After development of the applications/database architecture, the implementing activity assesses this architecture for common applications utilities. For example, a number of different applications may require transaction processing, document processing and electronic publishing. Other applications may share a requirement for electronic mail, decision support and shared-screen teleconferencing. Once the USCG activity defines the support applications entity (i.e., word processing, spreadsheets, etc.), a comparison is made between the support applications service requirements and the application platform services identified in the Technical Reference Model.

The USCG Technical Reference Model has been designed to cover all services commonly needed by USCG information systems.

However, if implementing activities find that additional services are required for the model, changes should be forwarded to the Systems Planning, Architecture and Review Staff (G-SIA).

There should be a complete mapping between support applications service needs and Technical Reference Model application platform services. Not all services may be needed to support a particular mission area. For example, some mission areas may not need product data interchange services. Implementing activities should not "invent" requirements just to "fill in each block" of the reference model.

After identifying each required service, the implementing activity analyzes the relevant standards to determine which standards satisfy the validated services. This review will, for the foreseeable future, indicate several gaps. Network services fall into this category since the Government Open Systems Interconnection Profile (GOSIP) does not yet contain all of the standards needed to support all user network needs. These standards are being addressed by national and international standardization bodies. Acquisition documents should mandate that contractors provide proof of standards compliance through an approved compliance laboratory, such as a NIST/National Voluntary Laboratory Accreditation Program (NVLAP), where such compliance tests exist. Acquisition documents should also indicate that the vendor must provide products that are capable of implementing the emerging standards. In the specific case of GOSIP, NIST has published a User's Guide that supports implementation planning.

USCG activities should not force fit the standards to meet services for which they are not designed. If USCG activities identity service areas where new standards are needed or higher priority placed on the standardization process, recommendations should be forwarded to Commandant (G-SIA).

- F. **Tailoring.** The architecture is intended to be tailored to specific mission area needs by selecting a subset of the standards profile which satisfies the mission area's requirements. Business specific applications and support applications entities can be refined to meet the needs of the mission area.
- G. **Additional implementation guidance.** The Information Systems Technology Architecture, which is a standards-based architecture, represents the technical environment that provides the greatest interoperability, portability, and scalability of information systems for diverse organizations with different missions. Evolving to this standards-based architecture though will require the Coast Guard to:

- o Make decisions about using open system standards and products on a case-by-case basis and justify exceptions to the technical architecture and its guidelines and associated implementation products.
- o Perform an economic analysis with trade-offs for technologies. Ensure the use of the Strategic Information Resource Management Plan (SIRMP), Automated Information System (AIS) proposals, cost-benefit analyses, value added approaches, and other suitable techniques.
- o Perform case studies for representative classes of technology in support software, platform services, hardware, and communications. Conduct targeted economic analysis for selected technologies based on their priority for supporting USCG functions, criticality to the architecture, risk, cost and other pertinent factors.

H. **Waiver/Waiver procedures.** Under certain exceptional circumstances, waivers to standards may be granted as outlined in FIPS PUB 146-1. When USCG system developers require approval for not using an established standard, a written request is to be submitted through the chain of command to Commandant (G-SIA) containing the following:

- o the identification of the standard being waived,
- o a clear indication that the existing standard cannot provide the service required and
- o a concise, quantified, cost-benefit analysis that clearly indicates that it is in the best interest of the USCG to acquire a product that does not conform to the Information Systems Technology Architecture.

The Information Systems Technology Architecture, as an architecture, provides us with the ability to define the communications system components functionally from end-to-end. To assist in this development, completion of a C3 Systems Architecture Planning Guide which will contain imagery, mapping, charting, geodesy, and sensor interoperability planning guidance continues and is near completion. Once we are able to describe the systems in terms of functional blocks and to describe those blocks within a common operating environment, the process can be constructed to move from today's many vertical stovepipe systems and programs to tomorrow's integrated end-to-end and cross-functional systems.

Moving to this standards-based open systems architecture will not be easy. However, use of the Information Systems Technology Architecture and the USCG Technical Reference Model will, in the long-term, allow users to rapidly obtain information services with minimum new developments and at affordable costs.

Appendix A - References

Application Portability Profile (APP), The U.S. Government's Open Systems Environment Profile OSE/1 Version 2.0, NIST Special Publication 500-210, June 1993.

DOD open Systems Environment (OSE) Profile for Imminent Acquisitions, 5 April 1993.

DOD Technical Architecture Framework for Information Management, Vers. 3.0, 30 September 1995 (draft).

IEEE Draft Guide to the POSIX Open System Environment (P1003.0/D15), Institute of Electrical and Electronics Engineers, Inc., May 1992.

ISO 8613, Office Document Architecture (ODA) and Office Document Interchange Format (ODIF).

ISO 8879, 1986, Information Processing: Text and Office Systems--Standard Generalized Markup Language (SGML).

NIST, FIPS 120, Graphical Kernel System (GKS), April 1986.

NIST, FIPS 127-2, Database Language SQL (ANSI X3.135-1989 & X3.168-1989), February 1990.

NIST, FIPS 128, Computer Graphics Metafile (ANSI X3.122-1986), March 1987.

NIST, FIPS 146-2, Profiles for Open Systems Internetworking Technologies (POSIT), Draft, March 1995.

NIST, FIPS 150, Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus, November 1988.

NIST, FIPS 151-1, POSIX: Portable Operating System Interface for Computer Environments (IEEE 1003.1-1988), March 1990.

NIST, FIPS 152, Standard Generalized Markup Language (SGML), September 1988.

NIST, FIPS 153, Programmer's Hierarchical Interactive Graphics System (PHIGS), December 1992.

NIST, FIPS 156, Information Resources Dictionary System (IRDS), November 1988.

NIST, FIPS 158-1, The User Interface Component of the Applications Portability Profile (MIT X Version 11, Release 3), May 1990.

NIST, FIPS 160, C, March 1991.

NIST, FIPS 161, Electronic Data Interchange (EDI), March 1991.

NIST, FIPS 174, Federal Building Telecommunications Wiring Standard, August 1992.

NIST, FIPS 178, Video Teleconferencing Services at 56 to 1,920 Kbps, 21 December 1992.

NIST, FIPS 179, Government Network Management Profile (GNMP), Version 1.0, 14 December 1992.

NIST, FIPS 182, Integrated Services Digital Network (ISDN), 5 October 1993.

NIST Special Publication 500-201, Reference Model for Frameworks of Software Engineering Environments (Technical Report ECMA TR/55, 2nd Edition), December 1991.

Appendix B - Acronyms

AMWG	Architecture Methodology Working Group
ANSI	American National Standards Institute
API	Application Program Interface
APP	Application Portability Profile
ASC	American Standards Committee
ASME	American Society of Mechanical Engineers
ASN	Abstract Syntax Notation
ATM	Asynchronous Transfer Mode
CAD	Computer-Aided Design
CALS	Continuous Acquisition Life cycle Support
CAM	Computer Aided Manufacturing
CASE	Computer-aided Software Engineering (See ISEE)
CCITT	Consultative Committee on International Telegraph and Telephone
CGM	Computer Graphics Metafile
CIM	Corporate Information Management
CIS	CASE Integration Services
CLNP	Connectionless Network Protocol
CMW	Compartmented Mode Workstation
COE	Common Operating Environment
COTS	Commercial-off-the-Shelf
CSL	Computer Systems Laboratory (part of NIST)
CTOS	Convergent Technologies Operating Systems
DBMS	Database Management System
DIA	Defense Intelligence Agency
DIS	Defense Information System

DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DNSIX	DODIIS Network Security for Information Exchange
DOD	Department of Defense
DODIIS	DoD Intelligence Information System
DSS	Digital Signature Standard
DSSSL	Document Style Semantics and Specification Language
DTD	Document Type Definition
DTMP	Data Communications Protocol Standards Technical Language Panel
ECMA	European Computer Manufacturers Association
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange For Administration, Commerce, and Transportation
EEI	External Environment Interface
FIPS	Federal Information Processing Standard
GKS	Graphical Kernel System
GNMP	Government Network Management Profile
GOSIP	Government Open System Interconnection Profile
GSA	General Services Administration
GUI	Graphical User Interface
HCI	Human Computer Interface
HYTIME	Hypermedia/Time-based Structuring Language
I-CASE	Integrated Computer Aided Software Engineering (See ISEE)
ICCCM	Inter-Client Communications Conventions Manual
IEEE	Institute of Electrical and Electronic Engineers
IGES	Initial Graphics Exchange Specification
IGOSS	Industry/Government Open System Specification

INX	Information Exchange
IRAC	International Requirements and Design Criteria
IRDS	Information Resource Dictionary System
ISDN	Integrated Services Digital Network
ISEE	Integrated Software Engineering Environment
LAN	Local Area Network
MHS	Message Handling System
NCSC	National Computer Security Center
NIST	National Institute of Standards and Technology
NISTIR	NIST Interim Report
NLSP	Network Layer Security Protocol
NSD	National Security Directive
NTIS	National Technical Information Service
NVLAP	National Voluntary Laboratory Accreditation Program
ODA	Office Document Architecture
ODIF	Office Document Interchange Format
ODL	Office Document Language
OIW	OSI Implementors' Workshop
OS	Operating System
OSE	Open System Environment
OSF	Open Software Foundation
OSI	Open System Interconnection
PCIS	Portable Common Interface Set
PCTE	Portable Common Tools Environment
PDES	Product Data Exchange using STEP
PEX	PHIGS Extension to X Windows
PHIGS	Programmer's Hierarchical Interactive Graphics System

POSIX	Portable Operating System Interface (for Computer Environments)
RDA	Remote Database Access
SDNS	Secure Data Network System
SGML	Standard Generalized Markup Language
SMDS	Switched Multimegabit Data Service
SMF	System Management Function
SQL	Structured Query Language
STEP	Standard for the Exchange of Product Module Data
STM	Synchronous Transfer Mode
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TDI	Trusted Database Interpretation
TFA	Transparent File Access
TLSP	Transport Layer Security Protocol
TNI	Trusted Network Interpretation
TRI-TAC	Tri-Service Tactical Communications Systems
TRM	Technical Reference Model
TTS	Telecommunications Standardization Sector (Formerly CCITT)
UIDL	User interface Definition Language
UISRM	User Interface System Reference Model
XVT	Extensible Virtual Toolkit