



SFA Modernization Partner
US Department of Education

**SFA Common Operating Environment
(COE)**

Task Order #4
Deliverable # 4.1.3

February 16th, 2000

Department of Education
Student Financial Assistance
Common Operating Environment Document

Table of Contents

1.	INTRODUCTION	1-1
1.1.	Current Title IV System Environment	1-1
1.2.	COE Document Purpose and Scope	1-4
1.3.	Document Organization and Content	1-4
2.	TECHNICAL APPROACH	2-1
2.1.	Assumptions and Constraints	2-1
2.1.1.	Assumptions	2-1
2.1.2.	Constraints	2-1
2.2.	Architecture Principles	2-2
2.2.1.	SFA Architecture Principles	2-2
2.2.2.	Process and Data Distribution Principles	2-5
2.3.	Standards Selection Process and Factors	2-7
3.	ARCHITECTURE SERVICES, STANDARDS, AND PRODUCTS	3-1
3.1.	Data Interchange Services	3-2
3.1.1.	Strategic Findings	3-2
3.1.2.	Document Interchange	3-2
3.2.	Data Management Services	3-4
3.2.1.	Strategic Findings	3-4
3.2.2.	Data Warehousing	3-4
3.3.	Distributed Computing Services	3-7
3.3.1.	Strategic Findings	3-7
3.3.2.	Directory Services	3-7
3.3.3.	Distributed Time	3-8
3.4.	Middleware Services	3-10
3.4.1.	Strategic Findings	3-10
3.4.2.	Object Services	3-10
3.5.	Network Services	3-12
3.5.1.	Strategic Findings	3-12
3.5.2.	Internet	3-12
3.6.	Security Services	3-15
3.6.1.	Strategic Findings	3-15
3.6.2.	Confidentiality	3-15
3.6.3.	Integrity	3-18
3.6.4.	Availability	3-20
4.	SUMMARY	4-22

Appendix A - ACRONYMS AND DEFINITIONS

Appendix B - GLOSSARY

Appendix C - REFERENCES

Appendix E - NON-SELECTED STANDARDS

Department of Education
Student Financial Assistance
Common Operating Environment Document

Table of Tables

		<i>Page</i>
Table 1-1.	Current Title IV System Operating Environment	1-3
Table 3-1.	Document Interchange Standards	3-3
Table 3-2.	Document Interchange Products	3-3
Table 3-3.	Data Warehousing Standards	3-5
Table 3-4.	Data Warehousing Products	3-6
Table 3-5.	Directory Standards	3-8
Table 3-6.	Directory Products	3-8
Table 3-7.	Distributed Time Standards	3-9
Table 3-8.	Distributed Time Product	3-9
Table 3-9.	Object Standards	3-11
Table 3-10.	Object Products	3-11
Table 3-11.	Internet Standards	3-14
Table 3-12.	Internet Products	3-14
Table 3-13.	Confidentiality Standards	3-17
Table 3-14.	Confidentiality Products	3-18
Table 3-15.	Integrity Standards	3-19
Table 3-16.	Integrity Products	3-20
Table 3-17.	Availability Standards	3-21
Table 3-18.	Availability Products	3-21

1. INTRODUCTION

The Office of Student Financial Assistance (SFA) Common Operating Environment (COE) document is one of a series of products developed in conjunction with Department of Education managers and community representatives to define information system requirements and architecture.

This section introduces the COE Document. Subsection 1.1 presents an overview of the current Title IV system environment. Subsection 1.2 more fully explains the documents purpose and scope. Subsection 1.3 explains how the remainder of the document is organized, and briefly describes the contents of each major element.

1.1. *Current Title IV System Environment*

The Office Student Financial Assistance (SFA), is responsible for administering and managing postsecondary student financial aid programs authorized under Title IV of the Higher Education Act of 1965, as amended. Currently, ED/SFA uses 12 major information systems to fulfill this responsibility.

- Campus-Based Programs System
- Central Processing System (CPS)/Electronic Data Entry (EDE) Express/Free Application for Federal Student Aid (FAFSA) on the Web
- Direct Loan Central Database System
- Direct Loan Consolidation System
- Direct Loan Origination System
- Direct Loan Servicing System
- Federal Family Education Loan Program (FFELP) System
- Multiple Data Entry (MDE) Contractor
- National Student Loan Data System (NSLDS)
- Postsecondary Education Participants System (PEPS)
- Recipient Financial Management System (RFMS)
- Title IV Wide Area Network (TIV WAN)

In general, these systems were built to support specific Title IV aid programs or functions (e.g., application processing). Although most of the systems are less than 10 years old, they were developed without the requirement to adhere to an overall technical architecture or set of technology standards. As a result, the systems operate on diverse hardware platforms, using a wide range of system and application software to deliver required functionality. Because the systems were not required to adhere to data standards, a single data attribute may be defined and stored in multiple ways across the systems.

Table 1-1 summarizes the operating environment represented by the current Title IV systems.

Title IV System	Integrated COTS Software	Custom Application Software	Data Management Software	Operating System	System Management Software
Campus-Based Programs System	Not Applicable	COBOL II Clipper 5.3	VSAM	MVS/ESA	MVS/ESA
CDS	FARS	IEF COBOL COBOL II C++	DB2	MVS/ESA	TMON Composer
CPS and EDEExpress	Enfin Crystal Reports	COBOL II Visual C++	DB2	MVS DOS Windows 95	Hear DB2 Custom Software for System Performance Monitoring
LOS	SNAP RJE MS Access CA Unicenter	Microfocus COBOL Powerbuilder C	Informix MS Access	HP-UX Netware OS2	Harvest CA Unicenter McAfee Novaback
LCS	UX-SNA-PLUS RJE CA Unicenter	Powerbuilder 4.0 COBOL C	ESQL/ Runtime Online DS	HP-UX	CA Unicenter Mirror Disk/UX OpenView OMNI BACK II Novaback
LSS	PowerBuilder Cognos Easytrieve Filenet	COBOL II	RDB for Open VMS	Open VMS MVS/XA	DEC PS
FFELP	DYL-Audit Informix ViewPoint	COBOL II Assembler JCL	IDMS Informix	MVS/ESA	CA-11 LandMark
MDE	PowerScan KIPP Image Key RexxLib PVFS	SAS C Rexx DELB	DB2 MS Access RRI DMS	SunOS Windows NT	SAT Inventory Manager
NSLDS	Not Provided	COBOL II Rexx COBOL	DB2 CICS	MVS/ESA	InfoMan Netview OmegaMon TMON
PGR/FMS	Easytrieve SAS	COBOL COBOL II Dbase Rexx	Oracle	MVS/ESA SunOS	Not Applicable

Title IV System	Integrated COTS Software	Custom Application Software	Data Management Software	Operating System	System Management Software
PEPS	HP-UX CA Unicenter	Developer 2000 PL/SQL and Oracle Pro C	Oracle	HP-UX	HP-UX CA Unicenter
TIVWAN	Focus DataAnalyzer Easytrieve	COBOL II	Not Applicable	MVS/ESA	Heat WAN System

Table 1-1. Current Title IV System Operating Environment

SFA is able to manage the Title IV programs and deliver aid using these systems. However, the current technical architecture has several drawbacks.

- Contributes to system interoperability issues
- Adversely affects the systems' flexibility to change to meet new user and programmatic requirements
- Adversely affects the systems' ability to benefit from advances in technology
- Contributes to higher program costs for ED and for the community
- Requires services of staff with a great range of technical skills and knowledge to maintain and enhance the systems
- Makes it more difficult for ED and the community to interact easily, cost effectively, and efficiently

1.2. COE Document Purpose and Scope

The COE Document is the primary tool for ensuring implementation using a standards-based, open architecture. The COE defines the architecture services expected to comprise SFA systems, and identifies the standards and products with which any SFA system implementation must comply. By establishing these standards, SFA can ensure that systems are incrementally developed by various providers, each increment will work with other increments already implemented or planned. In the case of outsourced functionality, the COE provides specifications that providers will need to adhere to in order to communicate with SFA systems and to exchange data.

The COE defines the target architecture standards for SFA. As long as the current Title IV systems are still in use, it is not expected that they will comply with this architecture. However, the COE does dictate that no new development will be undertaken in technologies non-compliant with the specified standards unless this development is explicitly evaluated and approved by appropriate ED managers prior to its initiation.

Beyond its immediate value to SFA, the COE is an important part of ED's overall response to the Clinger-Cohen legislation that dictates that ED have an overarching architecture. While the COE addresses only one component of this architecture requirement -- i.e., technical architecture standards -- it provides ED a viable sub-architecture that can be used to support the Department's overall effort in response to Clinger-Cohen.

The COE does specify a system solution using particular software. As ED awards contracts for various components to be implemented, each provider will implement based on the COE and other definition documentation.

1.3. Document Organization and Content

The remainder of the COE Document is organized as described below.

Section 2 - Technical Approach. This section describes the assumptions and constraints that affected definition of the COE. It also presents all architecture principles identified to date for SFA. Finally, it briefly explains the process and filters used to determine which standards should be used when implemented selected architecture services.

Section 3 - Architecture Services, Standards, and Products. This section presents the heart of the COE definition. For each service component within the application support layer, this section presents:

- Brief definition

- Sample correlation to business functions
- Standards to be followed when implementing the service component
- Products to be used in implementing the service component and standards, as applicable

Section 4 - Summary. This section concludes the COE.

The following appendices provide supplementary information for the COE.

Appendix A - Acronyms and Definitions. This appendix lists each acronym used in the COE Document, along with the acronym's definition.

Appendix B - Glossary. This appendix lists and defines many of the technical terms used in the COE Document.

Appendix C - References. This appendix lists the references used to develop the COE Document.

Appendix D - Excluded TOGAF TRM Components. This appendix identifies those service components that were included in The Open Group Architecture Framework (TOGAF), but which were excluded from this document. It also provides a brief explanation why each service listed was excluded.

Appendix E - Non-Selected Standards. This appendix lists those standards that were considered for inclusion in the COE, but were rejected. The reasons for not selecting these standards are also provided.

2. TECHNICAL APPROACH

This section identifies the assumptions and constraints that affected definition of the COE Document (subsection 2.1). In addition, it lists the architectural principles that influenced the selection of services and standards for inclusion in the COE. Finally, the decision process and factors used to identify the standards specified are summarized (subsection 2.3).

2.1. Assumptions and Constraints

Several assumptions and constraints affected decisions regarding COE scope and content. Subsection 2.1.1 lists assumptions. Subsection 2.1.2 identifies constraints.

2.1.1. Assumptions

1. Services and standards are based upon business requirements identified in the *Project EASI/ED BARD*.
2. SFA systems will contain or use data that is sensitive, but unclassified (e.g., proprietary business information, Privacy Act protected), but will not contain national security classified data.
3. SFA systems users will access the system using disparate technology (e.g., telephone, facsimile, postal mail, computer access via public networks).
4. SFA systems users will require access to the system without restriction by location, system access time, or specialized technical requirements.
5. SFA has no existing standards with which the COE Document is in conflict.
6. SFA systems must leverage public network resources (e.g., the Internet) wherever possible, practical, and appropriate so that accessibility and interoperability are maximized.

2.1.2. Constraints

- SFA architecture principles are not yet finalized, and changes to the draft principles (presented in subsection 2.2) may affect decisions reflected in the COE.
- The COE is required to rely upon Federal Information Processing System (FIPS) guidelines to the fullest extent possible.

2.2. **Architecture Principles**

Architecture principles are statements of preferred architectural direction or practice. They establish a context for architecture across an organization, and help bridge the gap between business and technical criteria. Architecture principles build upon the organization's strategic drivers and upon its stated objectives and goals.

In parallel with COE Document development, representatives of ED/SFA, worked to define architectural principles. These principles appear in subsection 2.2.1. In addition, based upon work performed for the *Project EASI/ED LDM* and for the *Project EASI/ED ASDD: SID*, principles for data and process distribution were defined. These principles are presented in subsection 2.2.2.

2.2.1. SFA Architecture Principles

SFA architecture principles are organized into framework and component principles. The framework principles are the umbrella guidelines for all IT decision-making. The component principles are more specific guidelines and are organized into four categories: data architecture, application architecture, technical infrastructure architecture, and IT management architecture.

Architecture Framework Principles

1. **The Architecture Must Support the Business:** The enterprise architecture and standards will be designed to (1) support and optimize the mission of SFA, (2) be highly flexible to accommodate future business changes and (3) help ensure the overall success of the SFA business.
2. **Periodic Architecture Review, Alignment, & Refreshment:** The IT architecture will be periodically reviewed (at least annually) and updated according to a disciplined, structured maintenance and technology refreshment process. This structure will include a configuration management process and supporting tools.
3. **Reengineer Business Processes and Supporting IT Together.** New information systems will be implemented after work processes have been analyzed, simplified or otherwise redesigned as appropriate, in compliance with the Clinger-Cohen legislation and Raines rules.
4. **Architecture Enforcement:** The information systems and technology infrastructure implemented by SFA will be compliant with the SFA Enterprise Architecture and COE described within.
5. **Use Industry Proven Technology:** Information technology applications and technical infrastructure decisions must be based on industry proven and supported components, methods, standards, and tools consistent with industry technological and market direction and as defined by this architecture.

6. **No vendor bias:** Standards and technology choices will be based on vendor-neutral standards where they are available and realistically can be implemented. Products will be chosen from any vendor with strong business stability, who provides the best technology and service for a business need and whose products are compliant with its architecture standards.
7. **Solutions Preference:** Where most cost effective and beneficial, SFA solutions preference will be (1) outsourcing; (2) commercial-off-the-shelf (COTS) products; (3) reuse of existing applications; and (4) custom applications.
8. **Access to Information:** Timely access to information and the tools and applications required to access and manipulate that information will be available to all individuals unless there is a specific, compelling reason to restrict access.
9. **Reduce Integration Complexity:** Products, tools, designs, applications, and methods will be selected to reduce integration and infrastructure complexity

Architecture Component Principles

- Data Architecture Principles

10. **Data Stewardship:** Data is an SFA asset and does not belong to a particular business, program or individual.
11. **Data Capture and Replication:** Data will be captured only once at the source. All data will be stored in a single master “authoritative source”. Replicated/aggregated copies (datamarts) will be created where required for performance or other reasons. Replicated copies will be updated from the master source as often as required by the applications.
12. **Manage data in its most appropriate form:** SFA architecture and systems will address the storage and management of all forms of data (text, voice, video, etc.) needed to support the functional requirements of the business.
13. **Operational Data Storage:** Operational data (used for OLTP) shall be separated from analysis or decision support data by creating data warehouses from the operational databases as required.
14. **Database Design:** All databases will use the standard SFA entity relationship tool for database design and documentation of the data structures. The data models will be kept in a central repository and databases will share common data models and data definitions. A metadata dictionary (repository warehouse) defining fields and attributes will be maintained in a shared accessible area and used as the basis for the creation of data structures.
15. **Business Logic:** Where appropriate and cost effective, business logic will be separate from data structures in SFA future information systems.

- **Application Architecture Principles**

16. **Structure of Business Applications** : Application design shall be based on an n-tier partitioned logical model (presentation, application logic, database) with firm logical boundaries established between the partitions.
17. **Reuse and Components** : Opportunities will be identified for cross-functional, integrated systems and these systems will be implemented to take advantage of standard components that can be shared and reused throughout SFA for similar business functions.
18. **Modular implementation for upgrade** : Technology components will be implemented in as modular a fashion as possible to allow the upgrade and exchange of vendor products with minimal disruption to the overall environment.
19. **Presentation Consistency**: All presentation user interfaces will adhere to SFA's standard graphical user interface to have a consistent look and feel. Presentation layer interfaces will be consistent across local and remote access. The preferred presentation interface will be based on Web browser technology capabilities.
20. **Object-oriented Design and Structure**: Where practical, applications shall be designed using objects, which encapsulate data structures and present a functional interface to application logic.
21. **Event Driven Processing**: Where practical, application design shall be event driven, employing a real-time processing methodology versus batch processing.
22. **Use of Automated Development and Testing Tools**: Standardized information systems tools will be used across SFA for systems design, development, and configuration management. Application development and testing will maximize their reliance on automated tools.

- **Technical Infrastructure Architecture Principles**

23. **Common Security Access**: The infrastructure will present a consistent, uniform, and adequate security mechanism across all applications, data access, and related components independent of physical location. Technologies such as a single logon with a database for profile definition and token-based authentication will be incorporated when applicable.
24. **Network Design**: All network components will adhere to the SFAP network standards for protocols, addressing, and firewall security. Any SFA desktop will be logically able to access any application and database within the SFA computing environment, within security and operational considerations

- **IT Management Architecture Principles**

26. **Common IT Infrastructure:** SFA will implement a common IT infrastructure for its systems. Applications will operate on this infrastructure.
27. **Migration Planning:** Movement toward the target architecture implementation and replacement efforts will be planned and implemented in functional or technical infrastructure sub-elements (e.g., chunks, releases, plateaus) to minimize SFA risk.
28. **Security Policy:** Security policies and practices will be consistently implemented to ensure the confidentiality, integrity, and availability of SFA data and systems. Policy monitoring and coordination of system-wide security measures and contingency plans will be the responsibility of SFA -level management.
29. **IT Project Evaluation and Review:** A structured IT investment process consistent with the Clinger-Cohen legislation and OMB / GAO capital planning requirements will be used by SFA to manage its IT investments. This process should be implemented in a pragmatic way without sacrificing the key discipline elements.
30. **Security Conformance:** All users of IT will conform to group and corporate security policies, protecting the integrity, reliability, and privacy of all SFA information assets. All users will conform to purchased product-licensing policies.
31. **Systems Development Methodology:** SFA will adopt and utilize a standard methodology for the implementation of IT solutions. The methodology will, at a minimum, address systems development -- design, development, and testing of IT solutions. Consistent with SFA priorities, the methodology should be a COTS product.
32. **Acquisition Methodology:** Software implementing the target architecture will be acquired by SFA using a structured process consistent with the Software Engineering Institute's Software Acquisition Capability Maturity Model, to mitigate risk. SFA will work to continuously improve this process over time.
33. **Project Tracking:** IT projects will use the standard SFA project management methodology and tool to track projects.
34. **Metrics Tracking:** Applications and technical infrastructure will be implemented in a way that facilitates the capture of measurement data and metrics for analysis and for management of the information technology and business environments.

2.2.2. Process and Data Distribution Principles

The principles presented in this subsection are intended to reflect expectations of process (software) and data distribution.

- SFA systems software and data distribution strategies will:
 1. Mitigate risk associated with untried technologies.
 2. Provide independence from specific proprietary hardware-based operating environments.
 3. Facilitate integration of information systems with other resources.
 4. Scale to meet necessary data volume, transaction volume, and performance requirements.
 5. Provide flexibility to cope with inevitable change in technology and requirements.
- SFA systems software and data will be physically distributed in a way that allows transition to platforms that accommodate future functional and technology changes.
- SFA systems software and data will be physically distributed in a manner to permit ease of administration (i.e., to leverage system administrator availability).
- SFA systems software and data will be distributed in a manner that permits fail-safe recovery or effective disaster recovery and control in the event of failure of part or all of the system.
- SFA systems software and data will be physically distributed in a manner that permits access to data sources outside the local data source, such as real-time data feeds, flat files, and/or multiple heterogeneous databases.
- SFA systems software will be physically distributed in a manner that permits ease of implementation of production software.
- SFA systems software will be physically distributed in a manner to permit ease of interaction with and synchronization with other peer applications.
- SFA systems software physical distribution will accommodate dependence upon the existing infrastructure (e.g., dependencies that may bind a process to a specific location), upon organization issues and requirements, and upon current system requirements (e.g., operating systems, security, database management system interface, data).
- SFA systems software will be physically distributed in a manner that facilitates ease of testing.
- SFA systems software will be physically distributed in a manner to allow ease of maintenance (e.g., facilitates changes to application or presentation logic).
- SFA systems software will be physically distributed in a manner that server-based application logic can be invoked by one or many front-end sources, including web browsers, inter- and intra-enterprise messages, microcomputer-based or network clients, and batch applications.
- SFA systems software will be physically distributed modularly to increase server scalability.

- SFA systems data will be distributed to allow the identification of a single, authoritative source of data for each data element in the Project EASI/ED LDM.
- SFA systems data will be distributed to ensure the integrity of data.
- SFA systems data will be distributed to ensure synchronization and consistency of data across all physical data stores within SFA systems.
- SFA systems data will be distributed to ensure availability of data on a 24 hours per day, seven days a week basis for those users who require it.
- SFA systems data will be distributed to provide access to up-to-date information, given the data currency requirements of different groups of users.
- SFA systems data will be distributed in such a way as to ensure the security of sensitive data.
- SFA systems data will be distributed in such a way as to allow ownership of data and access rights to data to be clearly identified and implemented.
- SFA systems data will be distributed to allow optimization of individual databases to support particular types of processing (e.g., transaction processing, decision support).

2.3. Standards Selection Process and Factors

The standards identification and selection process followed the approach described below.

- **Step 1 - Identify candidate pool of standards** available from government and private standards-making organizations, and also considering de facto standards.
- **Step 2 - Initially screen available standards for applicability.** Appendix E identifies all standards considered for the COE, but rejected during this or subsequent steps in the selection process.
- **Step 3 - Assess remaining standards against evaluation filters .** The five filters used for this step are listed below.
 1. **Functional fit** - assesses whether key features of a standard are necessary to support a specific business need.
 2. **Federal fit** - assesses whether a standard is consistent with federal guidelines for information systems technology implementation and architecture.
 3. **Openness and maturity** - assesses the degree to which a standard is open (i.e., A system whose interfaces (e.g., application programming interfaces or protocols) conform to formal, multilateral, generally available industry standards.) and the degree to which its features promote definition of a robust and interoperable architecture.

4. **Transition complexity** - assesses the degree to which a standard is still emerging or unproved, and flags or eliminates these from the COE at this time to help minimize ED risk.
5. **Interoperability** - assesses the extent to which a standard is able to interact or operate with other standards considered for the COE, so that services implementing the standards can function without interfering with one another.

Through the application of these filters, a candidate set of standards to implement each service was identified. The candidate standards were reviewed using the following qualitative factors that ED managers had previously identified as being of high importance for SFA and any other information systems.

- **Implementability.** To successfully meet stated objectives, the architecture needs to provide a comprehensive, flexible, and integrated approach to implement the system and to interact with external users and organizations. Implementability is assessed in terms of the degree to which the services and standards selected are mature, understandable, facilitate COTS-based solutions, and, to an extent, are supportable by available skilled personnel.
- **Flexibility.** This criterion is assessed in terms of the degree to which selected services and standards are open to product or vendor heterogeneity, are based on widely accepted standards, and are scalable. The architecture needs to allow processing components to be partitioned and distributed among homogenous or heterogeneous operating environments. This provides supplier independence; allows ED to better leverage processing capabilities at various levels throughout the architecture; and improves the ability of the system to readily respond to changing capacity requirements.
- **Manageability.** A key concern of ED managers is the degree to which they can readily manage system resources. This characteristic is assessed in terms of the degree to which selected services and standards promote selection of technologies that are reliable, available, serviceable, and controllable. Reliability and availability address the ability of architecture services to perform without failure and to be continuously available, in accordance with business needs. Serviceability relates to the degree to which standards and services support efficient software distribution, trouble shooting, fault detection, etc. Controllability assesses the degree to which the architecture enables ED to manage the systems availability, operations, and maintenance.
- **Usability.** SFA faces the challenge of enabling multiple organizations and a multitude of individual users to generate, use, and effectively manage large amounts of data using widely disparate technologies. Usability is assessed in terms of two principal factors: (1) the degree to which selected services and standards support realization of improved system and data usability, while masking system complexities from users; and (2) the degree to which the architecture is capable of providing appropriate access to information and functions from anywhere within a system.

Consideration of these factors pervades the COE, from identification of services and components through selection of standards and definition of the envisioned architecture topology.

3. ARCHITECTURE SERVICES, STANDARDS, AND PRODUCTS

This section presents the core of the COE Document. It describes each service and its associated components; correlates the components to business functionality; specifies standards and products to be used when each service component is implemented.

The remainder of this section is organized into the major subsections identified below. Strategic findings for the service are discussed at the beginning of each major subsection. These findings provide an integrated summary of architecturally significant standards for that service's components and discuss such factors as how the standards align with current industry and technology trends, how the standards in different services inter-relate to support an integrated architectural framework, and how the standards fit with high-level architecture objectives.

- Subsection 3.1 - Data Interchange Services
- Subsection 3.2 - Data Management Services
- Subsection 3.3 - Distributed Computing Services
- Subsection 3.4 - Middleware Services
- Subsection 3.5 - Network Services
- Subsection 3.6 - Security Services

Each service component is briefly defined and correlated to business requirements to illustrate how it might be used to implement desired functionality. Following each business requirement, a number in parentheses refers to the functional requirement number in the *BARD*. Each subsection also contains tables documenting the standards and products to be used when the service component is implemented.

- **Standards Table**. Each standards table presents the title(s) of applicable standard(s), the abbreviated name and sponsoring organization, a brief description of the standard's scope or purpose, and comments.
- **Products Table**. Each products table identifies the name(s) of mandated product(s), the product vendor, the product functionality type (e.g., DBMS), and the standards that the product implements.

3.1. Data Interchange Services

Data interchange services provide specialized support for the exchange of information between application software on the same or different platforms.

Subsection 3.1.1 presents the strategic findings for data interchange services. Subsection 3.1.2 describes the document interchange service component

3.1.1. Strategic Findings

Within SFA systems, one of the fundamental purposes of data interchange is to support information transfer into and out of the system. In all other service areas, the *COE* strategy is to limit standards to a small, manageable number of selections with minimal overlap between functional areas covered by the selected standards. In the data interchange area, however, this strategy is relaxed to provide the ability to exchange a wide variety of information with a wide variety of external systems. By supporting many mainstream data format standards, this interchange will be possible with a wide variety of external systems and organizations without overburdening these systems or organizations with requirements to translate data to a specific format.

Two Internet-derived standards for documents are selected: Hypertext Markup Language (HTML) and eXtensible Markup Language (XML). HTML is a very widely used Web document presentation standard, but does not include page-formatting features. XML extends HTML to provide page formatting, but is a fairly new standard with much less industry support.

3.1.2. Document Interchange

Description. Document interchange services support the exchange of formatted messages and of electronic forms between homogenous and heterogeneous computer systems. They are also used for publishing and managing mixed mode documents. Through document interchange services, formatted documents can be transferred across a network and be exactly reproduced at any location.

Correlation to SFA. Within SFA systems, document interchange services might be used to support the following example business requirements.

- Provide information contained in the ED Student Aid Handbook and in the Student Guide, and information about school participation in the Title IV programs. (1050)
- Send all Perkins Loan schools a copy of the low-income-school directory annually. (1258)

Applicable Standards. Given the wide variety of users SFA systems must support, two industry-standard document interchange formats will be supported.

Table 3-1 presents the standards that are to be followed when implementing document interchange services for SFA systems.

Standard Title	Organization and Standard Name	Description	Comments
eXtensible Markup Language (XML)	W3C PR-xml-971208	XML is a simple dialect of SGML. The goal is to enable generic SGML to be served, received, and processed on the Web in the way that is now possible with HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML.	Architecturally Significant
Hypertext Markup Language (HTML)	The Open Group HTML 3.2:1997	HTML is a markup language used to construct documents for viewing by World Wide Web browsers. HTML 3.2 is a specification of HTML issued by the World Wide Web Consortium (W3C) as a W3C Recommendation.	Architecturally Significant

Table 3-1. Document Interchange Standards

Mandated Products. Table 3-2 lists products that will be used to support document interchange services.

Product Name	Vendor	Product Type	Applicable Standards
iPlanet Enterprise Server 4.0	Netscape	Web Server	Hypertext Markup Language (HTML) HTML 3.2:1997
Financial Server	Innovision	XML Server	Extensible Mark-up Language (XML)/XSL
e*Gate	Software Technologies Corporation	Middleware	Extensible Mark-up Language (XML)

Table 3-2. Document Interchange Products

3.2. Data Management Services

Data management services provide access to data, store data, monitor data storage, and control data I/O operations. Through the use of features such as data locking and replication these services also ensure that data is consistent and available throughout distributed system environments. Within SFA systems, data management services are central to one of the core objectives for the vision -- to allow users ready, flexible, understandable access to data (within security constraints).

Subsection 3.2.1 presents strategic findings for data management services. Subsection 3.2.2 describes the Data Warehousing service component.

3.2.1. Strategic Findings

Data management service standards are driven by major relational DBMS vendors – Oracle, Sybase, and Informix. There is little standardization and interoperability between vendor product lines, with the exception of the Structured Query Language (SQL) standard. Recently, industry trends and developments have begun to change this situation. An example is the emergence of data warehousing technology, which offers the capability to extract information from multiple DBMS sources.

3.2.2. Data Warehousing

Description. Data warehouses are special-purpose DBMSs in which extracts of operational data are specially pre-processed (i.e., indexed, partitioned, and aggregated) to provide a unified repository of known facts. Information in data warehouses is subject-oriented, integrated, time-variant, and non-volatile. It is an effective way to transform data into information, providing critical repositories of timely, accurate information for decision-making and management. Several technology components are required for data warehousing. These are categorized as warehouse generation (getting data in), data management (storing data), and information access (getting data out).

Correlation to SFA. Within SFA systems, data warehousing services might be used to support the following example business requirements.

- Provide authorized parties visibility to Title IV participant information at varying levels of detail, and associate Title IV participant information across functional areas (e.g., application, disbursement, repayment). (2900)
- Provide statistical sampling and modeling capabilities to support Title IV program oversight functions. (2930)

- Monitor key performance indicators and flag those indicators whose values are outside predetermined parameters. (2950)
- Maintain performance measurements for each aid organization, school, and the EASI/ED system itself. Provide relevant information on these performance measurements to authorized external organizations and individuals. (2952)
- Provide what-if analysis capability to support formulation of program legislation and policy. (2960)
- Receive financial aid simulation modeling information (e.g., average salaries for various professions) from state departments of labor. (1960)

Applicable Standards. Various groups within the data warehousing vendor and user community advocate a broad range of emerging standards; however, no widely accepted data warehousing standard exists yet. The Metadata Coalition, a group of more than 50 data warehousing vendors and users, is a leader in metadata standards development. Relational database vendors are also trying to establish de facto standards for metadata.

Table 3-3 presents the standards that are to be followed when implementing data warehousing services.

Standard Title	Organization and Standard Name	Description	Comments
Database Language - SQL2	ANSI X3.135:1992	Defines the syntactic and semantic rules for database definition and data manipulation in a relational database management system. One of the database management system standards provided for use by all Federal departments and agencies, in accordance with FIPS Pub 127. FIPS SQL is suited for use by applications that employ the relational data model. SQL3 is an emerging standard that should be considered when mature.	
Relational On-Line Analytical Processing (ROLAP)	Relational On-Line Analytical Processing (ROLAP)	The end-user tool directly queries the central data warehouse. Advantages of this strategy include scalability and simpler, centralized management of the warehouse.	
Oracle	Oracle	SFA has chosen Oracle as their RDBMS	
Open Database Connectivity (ODBC)	Open Database Connectivity (ODBC)	Microsoft's Open Database Connectivity has become a defacto standard for database connectivity.	
Metadata Exchange (MX) Architecture	Informatica MX	MX lets vendors create links between their data access and query and reporting tools. MX also offers access to metadata via a visual Web browser.	

Table 3-3. Data Warehousing Standards

Mandated Products. Table 3-4 lists products that support data warehousing services.

Product Name	Vendor	Product Type	Applicable Standards
MicroStrategy6	MicroStrategy	Data Warehouse	ROLAP, MX, ODBC, Oracle, SQL2

Table 3-4. Data Warehousing Products

3.3. *Distributed Computing Services*

Distributed computing services enable various tasks, operations, and/or information transfers to occur on multiple, physically or logically dispersed computer platforms while maintaining a cooperative processing environment. These services allow users and application developers to maximize network-computing power by transparently assigning tasks to the most appropriate processors.

Subsection 3.3.1 presents strategic findings for distributed computing services. Subsection 3.3.2 describes the Directory services component and Subsection 3.3.3 describes the Time services component.

3.3.1. Strategic Findings

Subsection 3.3 focuses on distributed computing services only, i.e., LDAP. The closely related distributed object standard (CORBA) is addressed in subsection 4.5, Middleware Services.

Directory services are a key component of distributed computing. Directory services are strongly related to many other areas. For example, security depends upon a well-defined and well-maintained directory of users and resources. The main standard is:

- Lightweight Directory Access Protocol (LDAP)

LDAP is simple, addresses a wide range of applications, and is well supported by products.

3.3.2. Directory Services

Description. Directory services maintain dynamic lists of all application services available throughout a system. This directory is akin to an electronic telephone book that helps network clients find objects and services. When a client machine makes a request, the directory service locates the application service that can handle the request and tells the client how to communicate with the application service.

Correlation to SFA. Within SFA systems, directory services may be used to support the following business functions.

- The system shall allow participants to request simulations of possible financial aid packages and financing options, including:
 - Simulating the participant's likely eligibility for Federal financial aid
 - Simulating costs that would be incurred in attending a particular program at a given school

- Simulating the financial aid package options that may be available to the participant

Simulating the financing options that may be available to the participant. (1060)

- The system shall apply disbursements, adjustments, and cancellations to achieve an accurate daily net settlement. (1220)

Applicable Standards. Table 3-5 presents the standards that are to be followed when implementing directory services.

Standard Title	Organization and Standard Name	Description	Comments
Lightweight Directory Access Protocol (LDAP)	IETF RFC 1777:1995	Provides access to the X.500 Directory while not incurring the resource requirements of the Directory Access Protocol (DAP).	Architecturally Significant

Table 3-5. Directory Standards

Mandated Products. Table 3-6 lists products that support directory services.

Product Name	Vendor	Product Type	Applicable Standards
Directory Server V4.0	Netscape	Directory Server	Lightweight Directory Access Protocol (LDAP)v3

Table 3-6. Directory Products

3.3.3. Distributed Time

Description. With a distributed environment, keeping clocks on various system components synchronized presents a major challenge. Even if all clocks could be set to precisely the same time at some point, they would gradually drift apart in time at different rates from one another. As a result, each component would "believe" the time to be different, which causes problems when distributed programs have dependencies upon event ordering. For example, it would be difficult to determine whether Event A on System Component 1 occurred before Event B on System Component 2 because 1 and 2 may have different notions of the current time.

Distributed time services enable system resources to access a host that provides the "correct" time for all resources on a network. In addition, these services synchronize the host clocks, using either one machine or a "committee" of machines to provide the "correct" time for all other resources. These services are also essential to support time-dependent distributed processing activity, such as the maintenance of session keys for security purposes.

Correlation to EASI/ED. With EASI/ED, distributed time services may be used to support the following business functions.

- The system shall prompt the participant to authorize the disbursement of funds to a school for the participant's loan. The prompt shall occur when the participant has not authorized the disbursement to the school within 30 days of the effective date of the disbursement request made by the school. (1390)
- The system shall send the participant a disclosure statement 60 days prior to the end of the grace period. (2004)
- The system shall notify schools of participants' delinquency within 90 days of a missed loan repayment due date. (2550)

Applicable Standard. Table 3-7 presents the standard that is to be followed when implementing distributed time services for EASI/ED.

Standard Title	Organization and Standard Name	Description	Comments
DCE 1.1: Time Services Specification	The Open Group CAE Specification C310	CAE C310 specifies the Distributed Time Service (DTS) time representations, RPC interfaces to the DTS, and application programming interfaces to the DTS. It provides a portability guide for DTS application programs and a conformance specification for DTS implementations.	Architecturally Significant

Table 3-7. Distributed Time Standard

Mandated Products. Table 3-8 lists the mandated product that support distributed time services.

Product Name	Vendor	Product Type	Applicable Standards
Oracle 8i	Oracle	RDBMS	The Open Group CAE Specification C310

Table 4-8. Mandated Distributed Time Product

3.4. Middleware Services

Middleware services are network-aware services that layer between an application, the operating system, and the network transport layers. Middleware services also provide the network connectivity required for multi-tiered distributed computing. For SFA systems, middleware services include Object Services.

Subsection 3.4.1 presents strategic findings for middleware services. Subsections 3.4.2 briefly describes the service component.

3.4.1. Strategic Findings

The Object Management Group's CORBA's stronghold is the network; the Internet Inter-ORB Protocol (IIOP) is very powerful and is a widely accepted mechanism to allow software objects to interoperate over the Internet. CORBA has strong backing from vendors such as Netscape, Oracle, IBM, and Sun Microsystems.

This technology is very important to the design and implementation of new distributed systems. As a result, CORBA is specified as the preferred standard because of its vendor independence.

3.4.2. Object Services

Description. An object is an identifiable, encapsulated entity that provides one or more services that a client may request. Clients request an object service by invoking the appropriate method associated with the object; the object then carries out the service on the client's behalf. Object services are used to create, locate, and name objects, and to allow them to communicate in a distributed environment. Object services include common object services and Object Request Brokers (ORB). Common object services provide basic functions for object use and implementation, and are necessary to construct any distributed application. ORBs enable objects to transparently make and receive requests and responses in a distributed environment.

Correlation to SFA. Within SFA systems, object services might be used to support the following example business requirements.

- Calculate income contingent repayment terms for Direct Loans and for those loans assigned to ED for debt collection. (2360)
- Notify schools of participants' delinquency within 90 days of a missed loan repayment due date. (2550)

Applicable Standards. Table 3-9 presents the standards that are to be followed when implementing object services.

Standard Title	Organization and Standard Name	Description	Comments
Internet Inter-ORB Protocol	OMG IIOP	Like HTTP, CORBA's IIOP uses the Internet as backbone, which means that both IIOP and HTTP can run on the same networks. Browsers that are extended with an ORB and IIOP can thus call objects located on remote servers on the Internet.	
CORBA Architecture and Specification	OMG CORBA 2.3:1999	Describes the CORBA. Defines the Persistent Object, Concurrency Control, Externalization, Relationship and Transaction Services.	Architecturally Significant

Table 3-9. Object Standards

Mandated Products. Table 3-10 lists products that support object services.

Product Name	Vendor	Product Type	Applicable Standards
e*Gate	Software Technologies Corporation	Middleware	OMG CORBA 2.3:1999, OMG IIOP

Table 3-10. Object Products

3.5. Network Services

Network services provide connectivity and basic services to facilitate communications across workgroups and among sites. Network services comprise the network infrastructure required to support distributed data access and interoperability in a heterogeneous environment. For SFA systems, network services includes the Internet component.

Subsection 3.5.1 presents strategic findings for network services. Subsection 3.5.2 briefly describes the Internet service component.

3.5.1. Strategic Findings

In most cases, network services rely on the Internet to provide standard protocols for functions such as multimedia document transfer (HTTP). Most of the fundamental protocols to support network services have been stabilized by the Internet's influence. Basic file transfer and other high-level network functions are well supported by mature standards and widespread interoperability can be achieved.

3.5.2. Internet

Description. Internet services enable users to access the World Wide Web (WWW), and to use Internet protocols to access Internet resources. Internet-based architectures are facilitated by a technology infrastructure that permits globally distributed clients to access and use services provided by a variety of back-end services and resources -- such as DBMSs, transaction processing monitors, middleware, workflow products, file systems, and data warehouses.

Two additional network types based on Internet technology are described below.

- **Intranet.** A private network that uses Internet software and standards. An intranet may be a private Internet or group of private segments of the public Internet that is reserved for use by people given authority and access to that network. Intranets are increasingly being used to provide individuals within an organization easy access to corporate information.
- **Extranet.** An expansion of an organization's intranet to serve key customers, suppliers, or employees.

Correlation to SFA. Within SFA systems, Internet, intranet, and/or extranet services might be used to support the following example business requirements.

- Provide a single point of interface for receiving student aid data and payment history for federal loans. (1280)

- Allow participants to provide feedback on services offered by organizations associated with the Title IV programs. Feedback shall contain comments on: performance rating of schools, lenders, guaranty agencies, and ED; and EASI/ED system software service and performance. (1170)
- Publish results on the feedback received from schools, other organizations, and participants. (1190)
- Enable participants to apply for federal financial aid with application mechanisms available 24 hours a day, 7 days a week. (1690)
- Provide participants with information on long-term debt management, including: projected potential earnings after graduate by school program, and projected monthly payments after graduation based on different types of aid packages available. (1080)

Applicable Standards. Table 3-11 presents the standards that are to be followed when implementing Internet services.

Standard Title	Organization and Standard Name	Description	Comments
Requirements for Internet Hosts	InterNIC Internet Standard 0003:1989	Umbrella standard for Internet host software.	
Hypertext Transfer Protocol (HTTP)	IETF RFC 2616:1999	According to the Gartner Group, Internet Standards will be forced to evolve considerably to support an acceptable level of commercial functionality.	
Java 2 Platform Enterprise Edition (J2EE)	Java 2 Platform Enterprise Edition (J2EE)	Transaction Processing, State Management, Resource Pooling, and Messaging	
Java Server Pages (JSP) 1; Java Servlets 2.2	Java Server Pages (JSP) 1; Java Servlets 2.2	Dynamic Information Display; Display Logic	
Enterprise Java Beans (EJB) 1.1	Enterprise Java Beans (EJB) 1.1	Authorization and Authentication Security	

Table 3-11. Internet Standards

Mandated Products. Table 3-12 lists products that support Internet services.

Product Name	Vendor	Product Type	Applicable Standards
iPlanet Enterprise Server 4.0	Netscape	Web Server	Hypertext Transfer Protocol (HTTP) HTTP 1.0, Java Server Pages (JSP) 1; Java Servlets 2.2
WebSphere Enterprise Edition V3.0	IBM	Application Server	Java 2 Platform Enterprise Edition (J2EE), Enterprise Java Beans (EJB) 1.1
MicroStrategy6	MicroStrategy	Data Warehouse	Hypertext Transfer Protocol (HTTP) HTTP 1.0
e*Gate	Software Technologies Corporation	Middleware	Hypertext Transfer Protocol (HTTP) HTTP 1.0

Table 3-12. Internet Products

3.6. Security Services

Security services provide cross-platform management control over who can do what within a computer system and network. Security services support secure distribution and integrity of information, and protect the computing infrastructure from unauthorized access. Application-coupled security is usually provided by applications with specific security requirements, and is typically implemented as a transport layer technology, such as Netscape Secure Socket Layer (SSL). For SFA systems, security services include the following components.

- Confidentiality
- Integrity
- Availability

Subsection 3.61 presents strategic findings for security services. Subsections 3.6.2 through 3.6.4 briefly describe these service components.

3.6.1. Strategic Findings

A fundamental SFA system objective is to make information more readily accessible to a wide range of users. This objective increases the importance of information security and of the need to ensure data confidentiality, integrity, and availability. SFA systems are not expected to contain national security information (i.e., Top Secret, Secret, or Classified); rather, most data is considered Sensitive, But Unclassified (SBU). Despite this, the task of securing system resources and information is not necessarily easier, even though formal national security information clearance and handling procedures don't apply to the system. Security procedures and protocols for SFA systems must provide adequate protection for SBU information.

Security standards for SFA systems originated primarily from two sources: (1) the Internet, and (2) a long-time leader in information security—RSA Secure Data, Inc. The Internet has spawned numerous useful security standards, including Secure Hypertext Transfer Protocol (S-HTTP) and SSL.

3.6.2. Confidentiality

Description. Confidentiality services prevent the unauthorized disclosure of information. They are provided via mechanisms such as those listed below.

- **Identification and authentication** - is the verification of a user's claimed identity. This service ensures system entities (e.g., processes, hardware, personnel) are uniquely identified and authenticated. Authentication is employed when users initially identify

themselves (i.e., log in) to the system and when a process is transferred to, or initiated on, someone's behalf on another system in a network.

- **Authorization** - is the process of determining how an authenticated user is permitted to use specific system resources (e.g., data files, operator commands, I/O devices). An authorization mechanism automatically enforces management policies governing resource use.
- **Encryption** - provides a means to encode data so that it only can be decoded by a party who possesses the appropriate key.

Correlation SFA. Within SFA systems, confidentiality services might be used to support the following example business requirement.

- Receive a signature or authentication from participants to endorse an aid application, multi-year promissory note, or waiver to release information to or from external databases. (1742)

Applicable Standards. Table 3-13 presents the standards that are to be followed when implementing confidentiality services.

Standard Title	Organization and Standard Name	Description	Comments
Secure Sockets Layer (SSL) V3.0 Protocol	The Open Group CAE Specification SSL_3:1996	Secure Sockets Layer (SSL) is an open protocol for securing data communications across computer networks. Incorporating RSA data security technology, SSL provides a straightforward method for adding strong security to existing applications and network infrastructures.	Architecturally Significant
Enterprise Java Beans	Enterprise Java Beans (EJB) 1.1	Enterprise Java Beans architecture is inherently transactional, distributed, portable, multi-tier, scalable and secure	
RSA Public Key Cryptography	RSA Data Security, Inc. RSA	RSA provides a public-key crypto system for both encryption and authentication. Encryption and authentication take place without any sharing of private keys.	
Public Key Infrastructure	ITU X.509	Specifies the format for the certificate containing public key information.	
Security Architecture for Internet Protocol	IETC RFC 1825	Describes the security mechanism for IP Version 4 (IPv4) and IP Version 6 (IPv6) and the IP layer security service they provide.	

Table 3-13. Confidentiality Standards

Mandated Products. Table 3-14 lists products that support confidentiality services.

Product Name	Vendor	Product Type	Applicable Standards
iPlanet Enterprise Server 4.0	Netscape	Web Server	Secure Sockets Layer (SSL) 3.0, Federal Information Processing Standard (FIPS)-140-1
WebSphere Enterprise Edition V3.0	IBM	Application Server	Enterprise Java Beans (EJB) 1.1
Financial Server	Innovision	XML Server	Public Key Infrastructure X.509, Secure Sockets Layer (SSL) 3.0
Certificate Management System V4.0	Netscape	Certificate Server	Public Key Infrastructure X.509, RSA/Digital Signature Algorithm

Product Name	Vendor	Product Type	Applicable Standards
			(DSA), Certificate Revocation List (CRL)
Directory Server V4.0	Netscape	Directory Server	Public Key Infrastructure X.509, Secure Sockets Layer (SSL) 3.0

Table 3-14. Confidentiality Products

3.6.3. Integrity

Description. Integrity services prevent unauthorized modification of data within a system. Integrity services commonly are provided via digital signatures, which allow the recipient of a digitally signed electronic message to authenticate who the message sender is and to verify the message's integrity.

Correlation to SFA systems. Within SFA systems, integrity services might be used to support the following example business requirement.

- Receive a signature or authentication from participants to endorse an aid application, multi-year promissory note, or waiver to release information to or from external databases. (1742)

Applicable Standards. Table 3-15 presents the standards that are to be followed when implementing integrity services.

Standard Title	Organization and Standard Name	Description	Comments
Digital Signature Standard	NIST FIPS Pub 186:1994	The DSS defines a cryptographic system for generating and verifying digital signatures. The private key is randomly generated.	
The Digital Signature Algorithm (DSA)	ANSI X9.30.1	This standard shall be used in designing and implementing public-key based signature systems that federal departments and agencies operate or that are operated for them under contract.	
Computer Data Authentication	NIST FIPS Pub 113:1985	Specifies a Data Authentication Algorithm (DAA) that, when applied to computer data, automatically and accurately detects unauthorized modification, both intentional and accidental.	
Public Key Infrastructure	ITU X.509	Specifies the format for the certificate containing public key information.	

Table 3-15. Integrity Standards

Mandated Products. Table 3-16 lists products that support integrity services.

Product Name	Vendor	Product Type	Applicable Standards
Financial Server	Innovision	XML Server	Public Key Infrastructure X.509
Certificate Management System V4.0	Netscape	Certificate Management Server	Public Key Infrastructure X.509, RSA/Digital Signature Algorithm (DSA)
Directory Server V4.0	Netscape	Directory Server	Public Key Infrastructure X.509

Table 3-16. Integrity Products

3.6.4. Availability

Description. Availability services prevent unauthorized withholding of data or resources. Availability services commonly are implemented via firewalls, which are dedicated hardware and software systems that screen network traffic and validate the flow of information among networks. A firewall provides both a perimeter defense and a control point for monitoring access to services, both from inside and outside a private network. The use of a firewall is essential when connecting a network to a non-trusted or public network, especially the Internet.

Correlation to SFA. Within SFA systems, availability services will be used to control access to data and resources and thus ensure the data and resources are available for authorized users.

Applicable Standards. Table 3-17 presents the standards that are to be followed when implementing availability services.

Standard Title	Organization and Standard Name	Description	Comments
Security Architecture for the Internet Protocol	IETF RFC 1825:1995	Guidelines for the security using IP.	
Firewall Technology	Check Point Software Technologies, Inc.	Firewall standards implemented for state of the art firewall products.	De Facto Standard

Table 3-17. Availability Standards

Mandated Products. Table 3-18 lists products that support availability services.

Product Name	Vendor	Product Type	Applicable Standards
Check Point FireWall-1	Check Point Software Technologies, Inc.	Firewall	IETF RFC 1825, Check Point

Table 3-18. Availability Products

4. SUMMARY

The COE Document identifies the services appropriate to ED business requirements, and selects the best set of open, and technologically sound standards and products to implement those services. Services and their components are defined, and a set of standards is selected for each of those components. A mandated list of products is presented that must be used to implement the services, and which adhere to the standards within those services.

APPENDIX A

ACRONYMS AND DEFINITIONS

APPENDIX A ACRONYMS AND DEFINITIONS

This appendix lists and defines the acronyms used in the COE Document. Additional information on selected acronyms and terms is available in the glossary in Appendix B.

A

API Application Program Interface

B

BARD Business Applications Requirements Document

C

CAE Common Applications Environment
CGI Common Gateway Interface
CGI Computer Graphics Interface
CICS Customer Information Control System
CM Configuration Management
COBOL Common Business Oriented Language
COE Common Operating Environment
COM Component Object Model
CORBA Common Object Request Broker Architecture
COTS Commercial Off-the-Shelf

D

DAP Directory Access Protocol
DBMS Database Management System
DCE Distributed Computing Environment
DFS Distributed File System
DSA Digital Signature Algorithm
DTS Distributed Time Service

E

EASI Easy Access for Students and Institutions
ED US Department of Education

F

FAFSA	Free Application for Federal Student Aid
FFELP	Federal Family Education Loan Program
FIP	Federal Information Processing
FIPS	Federal Information Processing Standards
FIRMR	Federal Information Resource Management Regulation
FISAP	Fiscal operations report and Application to Participate

G

GAO	Government Accounting Office
GB	Gigabyte
GOTS	Government Off-the-Shelf
GSA	General Services Administration
GUI	Graphical User Interface

H

HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol

I

IEEE	Institute of Electrical and Electronic Engineers
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IIOF	Internet Inter-ORB Protocol
InterNIC	Internet Network Information Center
IP	Internet Protocol
IPSEC	Internet Protocol Security
IS	Information System
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunications Union

J

JTC	Joint Telecommunications Committee
-----	------------------------------------

K

Kbps	Kilobits Per Second
------	---------------------

L

LAN	Local Area Network
LCS	Loan Consolidation System
LDAP	Lightweight Directory Access Protocol
LDM	Logical data Model

LDMD Logical Data Model Document
LEAF Law Enforcement Access Field
LOS Loan Origination System
LSS Loan Servicing Systems

M

MAN Metropolitan Area Networks
MB Megabyte
Mbps Megabits Per Second
MDE Multiple Data Entry (System)
MIPS Million Instructions Per Second
MX Metadata Exchange

N

NFS Network File System
NIST National Institute of Standards and Technology
NSLDS National Student Loan Data System
NTP Network Time Protocol

O

ODBC Open Database Connectivity
OIM Open Information Model
OLAP Online Analytical Processing
OLE Object Linking and Embedding
OLTP On-Line Transaction Processing
OMB Office of Management and Budget
OPE Office of Postsecondary Education
ORB Object Request Broker
OS Operating System
OSI Open Systems Interconnect

P

PC Personal Computer
PEPS Postsecondary Education Participants System
PKCS Public Key Cryptography Standard
POSIT Profiles for Open Systems Internet Working Technologies
POSIX Portable Operating Systems Interface
PTO Patent and Trademark Office

R

RDBMS Relational Database Management System
RFC Request For Comments
RFMS Recipient Financial Management System
ROLAP Relational Online Analytical Processing
ROM Read Only Memory

RPC Remote Procedure Call
RTCP Real Time Transport Control Protocol
RTP Real Time Protocol

S

SBU	Sensitive, but Unclassified
SCO	Santa Cruz Operation
SFA	Student Financial Assistance
SFAP	Student Financial Assistance Program
SGML	Standard Graphical Markup Language
SHS	Secure Hash Standard
S-HTTP	Secure Hypertext Transfer Protocol
SQL	Standard Query Language
SSL	Secure Sockets Layer

T

TAFIM	Technical Architecture Framework For Information Management
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TIA	Telecommunications Industries Association
TIVWAN	Title IV Wide Area Network
TOGAF	The Open Group Architecture Framework
TP	Transaction Processing

U

UA	User Agent
UDP	User Datagram Protocol
UML	Universal Modeling Language
Unicode	Not an acronym, shorthand for Universal Multiple Octet Coding Scheme, see UCS
URL	Universal Resource Locator
US	United States

V

VAN	Value Added Network
VPN	Virtual Private Network
VRML	Virtual Reality Modeling Language

W

W3C	World Wide Web Consortium
WAI	Web Accessibility Initiative
WAN	Wide Area Network
WWW	World Wide Web

X

XML	Extensible Markup Language
-----	----------------------------

APPENDIX B

GLOSSARY

APPENDIX B

GLOSSARY

This appendix lists and defines selected terms and provides additional information on selected acronyms used in the *Project EASI/ED COE Document*.

<u>Term or Acronym</u>	<u>Definition</u>
Architecture Services/ Components	The major classes (and sub-classes) of functionality provided by a computer system.
ATM	Short for asynchronous transfer mode, it's a way of designing data packets that's particularly suited to sending video and audio information as well as text. Besides offering very high speed, ATM is attracting attention because it is favored by phone companies, cable operators and corporate computer users alike, which may make for easier networking between offices and homes.
Bandwidth	A measure of how fast a network can move information, usually measured in thousands or millions of bits, or units of data, per second.
Business Application	An operation that fulfills some specific business function.
CCITT	The initials for the French International Telegraph and Telephone Consultative Committee. The CCITT has been renamed the International Telecommunications Union or ITU. This organization defines standards or recommendations (e.g., X.25) for international networking.
Client	A client is usually a PC that communicates over a network both with its peers, other clients, and with a larger computer, called a server, which typically stores data that many workers need to use. The client has just one user, the server many.
Client-Server	The use of combinations of large and small computers to satisfy large system requirements using smaller components.
Communications Server	A hardware and software device that allows devices such as terminals, host computers, or printers to access a network without having to implement the communications protocol in the device itself. The communications server communicates with the device using standard protocols built into the device.
Connection	A communications path between two devices that allows the exchange of information. Other terms used to refer to a connection are session or circuit.
Distributed Computing	Another name for the type of computing that networks allow. With combinations of PCs and servers, an organization's data and applications software may be scattered among different machines.

<u>Term or Acronym</u>	<u>Definition</u>
Enterprise Architecture	A high-level description and drawing representing an information system design for an organization or enterprise
Ethernet	A local area network that utilizes baseband signaling at 10 Mbps. The development of the Ethernet specification was a joint effort by Xerox, DEC and Intel and is the predominant local area network standard. The most common sort of network used in corporations. Its top speed is 10 million bits a second.
Fast-Ethernet	A revision of Ethernet which allows data to be transmitted at 10 times the speed of Ethernet – 100Mbps.
Firewall	One way to keep unauthorized persons out of a network. Some networking devices can limit access to sensitive parts of a network. For example, a company might authorize access to its salary records only to a computer in a particular location that gives a secret password. But any PC user might be able to send e-mail to the personnel department requesting information.
Gateway	How a user or another system can get access to a network. One of the most common usage's for the term is an on-line service company that gives customers access to the Internet. Inside a company, the term usually refers to specialized hardware that connects two different types of systems, such as a mainframe to a local-area network.
Gigabit Network	A network that operates at a billion bits a second -- 100 times Ethernet's speed.
Internet	The interconnection of thousands of separate networks using a common terminology. Developed by the Pentagon, the Internet first linked government agencies and colleges. Now the Internet also connects thousands of companies and millions of individuals who subscribe to on-line services; they can use it to exchange messages or data files.
ISDN	An interim step to take phone companies into the digital age. Integrated Services Digital Network is a technology that lets both voice and data flow over a standard phone line to a home or office. It runs six times faster than most PCs can communicate over a modem, though less than 1/100th the speed of Ethernet.
ISO Model	International Standards Organization (ISO) developed Reference Model for Open Systems Interconnection, which divides a complex set of communications functions into self-contained modules.
LAN	A Local Area Network (LAN) is a communications network that provides high-speed data transmission over a small geographic area. LAN also refers to a group of computers that are connected by cable and share data, software and storage devices. LANs are needed to practice client-server computing.
Network Management	The overseeing and maintaining of a network. The duties performed by a system or network manager using a network management system include

<u>Term or Acronym</u>	<u>Definition</u>
	installing and configuring the network, maintaining an operation log, monitoring network performance, and statistics.
Network	A system of computers and other hardware and software that is connected and allows users to transmit data and messages.
Network Topology	The geography of a network.
Notional Topology	A technical diagram describing a network and its resources. A notional topology will show all aspects of the network from a consistent level of abstraction.
Organization	An organization may be a school, government agency, funding source, outsource, institution, standards committee, or ED itself.
Protocol	A strictly defined procedure and message format that allows two or more systems to communicate over a physical transmission medium. Due to the complexity of communications between systems and the need for different communications requirements, protocols are divided into layers. Each layer of a protocol performs a specific function, such as routing, end-to-end reliability, and connection.
Service	A method for making systems resources available to users, electronic or human, in a consistent manner.
Standards	A standard is a well-defined, and typically published, definition for the method of satisfying some aspect of a computer system. Standards may be endorsed and/or published by one or more accredited standards committees, or they may be so widely used that they have become de facto industry standards.
Strategic Finding	Strategic finding sections summarize the state of the industry for each service. Strategic findings describe the service in terms of where the service (and sub-services) have been, where it is currently, and, most importantly, where the service is headed.
T-1 Carrier	A digital transmission system developed by AT&T that sends information at 1.544 megabits per second. T-1 links can transmit voice or data.
TCP/IP	Transmission Control Protocol/Internet Protocol. A set of de facto networking standards commonly used over Ethernet or X.25 networks. It was originally developed by the U.S. Government and is now supported by many equipment manufacturers. It defines high-level protocols such as Telnet (terminal connection), FTP (file transfer), and SMTP (electronic mail).
Technical Reference Model	A TRM describes platform functions that support business applications. The purpose is to aid understanding of the taxonomy of information systems and of platform services in particular.

<u>Term or Acronym</u>	<u>Definition</u>
Virtual Circuit	A facility in a packet switching network in which packets passing between a pair of devices are kept in sequence. This is a virtual circuit because it appears there is an actual point-to-point connection.
WAN	A Wide Area Network is data communications network designed to serve an area of hundreds or thousands of miles. A WAN can be public or private.
X.25	An ITU (formerly CCITT) standard that defines the standard communications protocol by which mainframes access a public or private packet switching network. These networks are often referred to as X.25 networks.

APPENDIX C

REFERENCES

APPENDIX C

REFERENCES

This Appendix cites the references used for the COE Document.

Project EASI/ED References

- US Department of Education, Project EASI/ED Common Operating Environment (COE) Document, 1998.
- ----, Project EASI/ED Application Services Definition Document: Subsystem and Interface Definition (ASDD: SID), 1998.
- ----, Project EASI/ED ASDD: Implementation Options Analysis (ASDD: IOA), 1998
- ----, Project EASI/ED Business Area Requirements Document (BARD), Volumes 1 and 2, 1997.
- ----, Project EASI Concept Document, 1997.
- ----, Project EASI/ED Logical Data Model Document (LDMD), 1998.
- ----, Project EASI/ED Technical Vision and Target Architecture (TVTA) Report, 1997.

Internet References

- <http://www.ansi.com/>, American National Standards Institute, 1998.
- <http://www.aiim.org/>, Association for Information and Image Management, 1998.
- <http://spider.osfl.disa.mil/dii/>, Defense Information Systems Agency, Defense Information Infrastructure Common Operating Environment, 5/1/98.
- <http://www.camb.opengroup.org/dce/>, Distributed Computing Environment, undated.
- <http://www.aiim.org/dma/>, Document Management Alliance, 5/27/98.
- <http://www.eia.org/>, Electronic Industries Association, 5/21/98.
- <http://www.ectf.org/>, Enterprise Computer Telephony Forum, undated.
- <http://www.software.ibm.com/openblue/opencomp.htm>, IBM Corporation, Open Blueprint Component Description Papers, 10/22/97.
- <http://www.ieee.org/>, Institute of Electrical and Electronics Engineers, 1998.
- <http://www.iec.ch/>, International Electrotechnical Commission, 1997.

- <http://www.iso.ch/>, International Organization for Standardization, 1998.
- <http://www.itu.ch/>, International Telecommunications Union, 1998.
- <http://www.isi.edu/iab/>, Internet Architecture Board, 9/10/96.
- <http://www.ietf.org/>, Internet Engineering Task Force, 1998.
- <http://www.internic.net/>, InterNIC, 5/22/98.
- <http://web.mit.edu/kerberos/www/>, Massachusetts Institute of Technology, 1998.
- <http://www.microsoft.com/>, Microsoft Corporation, 1998.
- <http://www.nist.gov/>, National Institute of Standards and Technology, undated.
- <http://www.nmf.org/>, Network Management Forum, 1998.
- <http://www.omg.org/>, Object Management Group, 1998.
- <http://www.opengroup.org/>, The Open Group, 1998.
- <http://www.rsa.com/rsalabs/>, RSA Data Security, Inc., RSA Laboratories, 1998.
- <http://www.uspto.gov/web/offices/cio/>, US Patent and Trademark Office, 4/18/97.
- <http://www-it.hr.doe.gov/standards/>, US Department of Energy, 11/19/97.
- <http://www.w3.org/>, World Wide Web Consortium, 1997.

Other References

- American National Standards Institute, ANSI-ISO-IEC Catalog: Searching the ANSI, ISO, and IEC Standards, 2/11/98.
- Faulkner Information Services, Faulkner Advisory on Computer and Communications Technologies, 1998.
- Gartner Group, Inc., Gartner Group Research, 1998.
- National Institute of Standards and Technology, The Federal Information Processing Standards Publication: Index List By FIPS Number, 1997.
- Office of Management and Budget, Memorandum, Subject: Information Technology Architectures, 1997.
- The Open Group, The Open Group Architecture Framework, undated.

- Price Waterhouse LLP, Technology Forecast: 1995. Price Waterhouse World Technology Center, Menlo Park, CA, 1994.
- ----, Technology Forecast: 1996. Price Waterhouse World Technology Center, Menlo Park, CA, 1995.
- ----, Technology Forecast: 1997. Price Waterhouse World Technology Center, Menlo Park, CA, 1997.
- ----, Technology Forecast: 1998. Price Waterhouse World Technology Center, Menlo Park, CA, 1998.
- US Department of Defense, Technical Architecture Framework for Information Management Version 3.0, 1998.
- US Department of the Navy, Center for Architecture and Standards, List of Standards, undated.

APPENDIX D

EXCLUDED TOGAF TRM COMPONENTS

APPENDIX D

EXCLUDED TOGAF TRM COMPONENTS

This Appendix provides a list of the TOGAF components that were excluded from the EASI/ED TRM.

<u>TOGAF COMPONENT</u>	<u>REASON FOR EXCLUSION</u>
Data Interchange Service Components:	
Specialized Data Interchange	Applies to vertical markets, which are covered in data interchange services for EASI/ED.
Data Management Service Components:	
Object Oriented Database	Covered in DBMS for EASI/ED.
Distributed Computing Service Components:	
Remote Print Spooling and Output Distribution	Covered in distributed file services in EASI/ED.
Graphical Object Management Services	Since graphical object management is not a primary component of EASI/ED, this was merged into other areas. Imaging is covered under document management services in EASI/ED. Graphics is covered under data interchange services in EASI/ED.
Drawing	Not an EASI/ED function.
Operating System Service Components:	
File and Directory Synchronization Services	These services are affected by design considerations. Consider adding later in development life cycle as design and implementation decisions are made.
Software Engineering Service Components:	
Graphical User Interface Building	Software engineering is dependent upon life cycle development methodology and CASE tools selected for EASI/ED, which are decisions ED is currently making. Consider adding later in development life cycle as design and implementation decisions are made.

TOGAF COMPONENT

REASON FOR EXCLUSION

Software Engineering Service Components (cont'd):

Scripting Languages Software engineering is dependent upon life cycle development methodology and CASE tools selected for EASI/ED, which are decisions ED is currently making. Consider adding later in development life cycle as design and implementation decisions are made.

Object Code Linking Software engineering is dependent upon life cycle development methodology and CASE tools selected for EASI/ED, which are decisions ED is currently making. Consider adding later in development life cycle as design and implementation decisions are made.

Language Building Software engineering is dependent upon life cycle development methodology and CASE tools selected for EASI/ED, which are decisions ED is currently making. Consider adding later in development life cycle as design and implementation decisions are made.

Run Time Environment Software engineering is dependent upon life cycle development methodology and CASE tools selected for EASI/ED, which are decisions ED is currently making. Consider adding later in development life cycle as design and implementation decisions are made.

Application Binary Interface Software engineering is dependent upon life cycle development methodology and CASE tools selected for EASI/ED, which are decisions ED is currently making. Consider adding later in development life cycle as design and implementation decisions are made.

User Interface Service Components:

Computer-Based Training and On-line Help Based on COTS products chosen during implementation phase. Standards available were just guidelines for on-line help development. Consider adding later in development life cycle as design and implementation decisions are made.

TOGAF COMPONENT

REASON FOR EXCLUSION

Security Service Components:

System Entry Control Services	Covered in EASI/ED through confidentiality, integrity, and availability service components, which are more representative of industry-accepted approach.
Audit	Covered in EASI/ED through confidentiality, integrity, and availability service components, which are more representative of industry-accepted approach.
Access Control	Covered in EASI/ED through confidentiality, integrity, and availability service components, which are more representative of industry-accepted approach.
Security Management	Covered in EASI/ED through confidentiality, integrity, and availability service components, which are more representative of industry-accepted approach.
Trusted Recovery	Covered in EASI/ED through confidentiality, integrity, and availability service components, which are more representative of industry-accepted approach.
Trusted Communication	Covered in EASI/ED through confidentiality, integrity, and availability service components, which are more representative of industry-accepted approach.
Non-Repudiation	Covered in EASI/ED through confidentiality, integrity, and availability service components, which are more representative of industry-accepted approach.

System and Network Management Service Components:

Network Management	Covered through fault management and usage management in EASI/ED.
On-line Disk Management	Eliminated; too detailed for EASI/ED (at this stage).

TOGAF COMPONENT

REASON FOR EXCLUSION

System and Network Management Service Components:

Capacity Management

Covered through usage management in
EASI/ED.

APPENDIX E

NON-SELECTED STANDARDS

APPENDIX E

NON-SELECTED STANDARDS

This appendix lists those standards that were considered for inclusion in the *EAS/ED COE*, but were rejected. The reasons for rejecting these standards are also provided.

Standard Name	Standard Title	Standard Date	Rationale
1,200 baud Modems	1,200 Bits Per Second Two-Wire Duplex Modems for Data Communications Use on Telephone-Type Circuits	1992	Obsolete
Alpha-Windows	AlphaWindows		Obsolete
ANSI - P - T1.101	Synchronization Interface Standards for Digital Networks	1994	Similar to CAE Specification C310
ANSI T1.617	DSS1 Signaling Specification for Frame Relay Bearer Service		Not Applicable
ANSI T1.618	Core Aspects of Frame Protocol for Use with Frame Relay Bearer Service		Not Applicable
ANSI T1.635	ATM Adaptation Layer Type 5 Common Part Functions and Specifications, 1994, which adopts ITU-T I.363, section 6	1994	Too low-level
ANSI X3.100	Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Operation with Packet-Switched Data Communications Networks (PSDN), or between Two DTEs, by Dedicated Circuit	1989	FIPS Pub 100-1
ANSI X3.106	Data Encryption Algorithm, Modes of Operation	1983	Included in FIPS Pub
ANSI X3.124	Graphical Kernel System (GKS)	1991	Only applicable to graphics intensive applications
ANSI X3.131	Small Computer Systems Interface-2 (SCSI-II)	1990	Hardware interface outside of <i>COE</i> scope
ANSI X3.229	FDDI Station Management		Low level standard, component of FDDI standard
ANSI X3.30	Representation for Calendar Date and Ordinal Date for Information Interchange	1998	Functionality provided by preferred standard FIPS Pub 4-1
ANSI X3.51	Representations of Universal Time, Local Time Differentials, and United States Time Zone References for Information Interchange	1994	Functionality provided by preferred standard CAE Specification C310
ANSI X9.17	Financial Institution Key Management (Wholesale)	1985	Not applicable
ANSI X9.30.2	Secure Hash Algorithm	1997	Covered by NIST FIPS Pub 180-1
ANSI Z39.2	Bibliographic Information Interchange	1985	No functional fit
ANSI Z39.59	Electronic Manuscript Preparation and Markup (EMPM)	1988	Not applicable

Standard Name	Standard Title	Standard Date	Rationale
ANSI/AIIM MS44-1988	Recommended Practice for Quality Control of Image Scanners		Guideline – not a standard
ANSI/AIIM MS52	Recommended Practice for the Requirements and Characteristics of Original Documents Intended for Optical Scanning	1991	Guideline – not a standard
ANSI/AIIM MS53	Recommended Practice; File Format for Storage and Exchange of Image; Bi-Level Image File Format: Part 1	1993	Guideline – not a standard
ANSI/AIIM MS58	Standard Recommended Practice for Implementation of Small Computer Systems Interface (SCSI-2), (X3.131-1994) Standard Recommended Practice for Implementation of Small Computer Systems Interface (SCSI-2), (X3.131-1994)	1996	Out of scope – hardware interface
ANSI/ISO 9593-1	PHIGS Language Bindings - FORTRAN	1991	Programming language not recommended for EASI/ED
ANSI/ISO 9593-3	PHIGS Language Bindings - ADA	1991	Programming language not recommended for EASI/ED
ANSI/ISO Z39.50	Information Retrieval Service Definition and Protocol Specification for Library Applications	1995	FIPS Pub 192
ANSI/ISO/IE C 8211	Specification for a Data Descriptive File for Information Interchange (DDF)	1985	Too low-level
ANSI/ISO/IE C 8652	Programming Languages - Ada	1995	Programming language not recommended for EASI/ED
ANSI/MDC X11.1	Programming Languages - MUMPS	1990	Programming language not recommended for EASI/ED
ASC X12 3040	ASC X12 3040 Federal Implementation Conventions	n/a	Guideline – not a standard
ASC X12 3050	ASC X12 3050 Federal Implementation Conventions	n/a	Guideline – not a standard
ASC X12 3060	ASC X12 3060 Federal Implementation Conventions	n/a	Guideline – not a standard
ASC X12 3070	ASC X12 3070 Federal Implementation Conventions	n/a	Guideline – not a standard
CGI/1.1	The WWW Common Gateway Interface Version 1.1	1996	Functionality provided through more recent interfaces (e.g. ODBC)
CORBA IDL/Java Mapping	CORBA IDL/Java Language Mapping	1997	Not a standard
Document Printing Application	Document Printing Application (DPA), Part 1: Abstract service definition and procedures		Too low-level
EIA 641	Software Life Cycle Processes	n/a	Not within the scope of this COE
FIPS Pub 112	Password Usage	1985	Mature guidelines for ensuring password security.

Standard Name	Standard Title	Standard Date	Rationale
FIPS Pub 141	Interoperability and Security Requirements for Use of the Data Encryption Standard with CCITT Group 3 Facsimile Equipment	1985	Obsolete
FIPS Pub 144	Data Communication Systems and Services User- Oriented Performance Parameters	1985	Too low-level
FIPS Pub 154	High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment	1988	Too low-level
FIPS Pub 155	Data Communication Systems and Services User- Oriented Performance Measurement	1988	Functionality provided through preferred standard C427 (UMA)
FIPS Pub 156	Information Resource Dictionary System (IRDS)		MIB-II is more widely used
FIPS Pub 163	2,400 Bits Per Second Two-Wire Duplex Modems for Data Communications Use on Telephone-Type Circuits	1992	Rolled into FIPS Pub 168 obsolete
FIPS Pub 164	2,400 Bits Per Second Four-Wire Duplex and Two-Wire Half-Duplex Modems for Data Communications Use on Telephone-Type Circuits	1992	Rolled into FIPS Pub 168 obsolete
FIPS Pub 165	4,800 Bits Per Second Four-Wire Duplex and Two-Wire Half-Duplex Modems for Data Communications Use on Telephone-Type Circuits	1992	Rolled into FIPS Pub 168 obsolete
FIPS Pub 166	4,800 and 9,600 Bits Per Second Two-Wire Duplex Modems for Data Communications Use on Telephone-Type Circuits	1992	Rolled into FIPS Pub 168 obsolete
FIPS Pub 167	9,600 Bits Per Second Four-Wire Duplex Modems for Data Communications Use on Telephone-Type Circuits	1992	Rolled into FIPS Pub 168 obsolete
FIPS Pub 172	VHSIC HARDWARE DESCRIPTION LANGUAGE (VHDL)	1995	Hardware interface outside of <i>COE</i> scope
FIPS Pub 173	Spatial Data Transfer Standard (SDTS)	1994	No application for spatial data
FIPS Pub 178	Video Teleconferencing Services at 56 to 1,920 KB/S	1992	Selected H.300 as the VTC standards group because of wide industry support
FIPS Pub 179-1	Government Network Management Profile (GNMP)	1995	Selected MIB-II as network management standard because of wide industry support
FIPS Pub 181	Automated Password Generator (APG)	1993	FIPS Pub 46-2.
FIPS Pub 183	Integration Definition for Function Modeling (IDEFO)	1993	Function Modeling is outside scope
FIPS Pub 184	Integration Definition for Information Modeling (IDEFIX)	1993	Information Modeling is outside scope
FIPS Pub 194	Open Document Architecture (ODA) Raster Document Application Profile (DAP)	1995	Using PDF and XML standards instead of the more complex ODA

Standard Name	Standard Title	Standard Date	Rationale
Futurebus Spcification	Standard for Futurebus Physical Layer and Profile Specification	n/a	Hardware standard outside scope
HDF	Hierarchical Data Format (HDF)	n/a	Legacy
HTML	Hypertext Markup Language (HTML)	n/a	Succeeded by HTML 3.2
IDEA	International Data Encryption Algorithm (IDEA)	1992	Using Federally approved DES instead
IEC 60050-722 Ed. 1.0 b	International Electrotechnical Vocabulary - Chapter 722: Telephony	1993	Outside scope
IEEE 10038	Local area networks - Media access control (MAC) bridges	1993	Low-level standard – below level of current <i>COE</i> detail
IEEE 1008	Software Unit Testing	1987	Software development standard outside of scope
IEEE 1012	Standard for Software Verification and Validation Plans	1986	Software development standard outside of scope
IEEE 1016	Recommended Practice for Software Design Descriptions	1987	Software development standard outside of scope
IEEE 1042	Guide to Software Configuration Management	1987	Software development standard outside of scope
IEEE 1045	Standard for Software Productivity Metrics	1992	Software development standard outside of scope
IEEE 1058.1	IEEE Standard for Software Project Management Plans	1987	Software development standard outside of scope
IEEE 1059	Guide for Software Verification and Validation Plans	1993	Software development standard outside of scope
IEEE 1061	Standard for a Software Quality Metrics Methodology	1992	Software development standard outside of scope
IEEE 1063	IEEE Standard for Software User Documentation	1987	Software development standard outside of scope
IEEE 1178	IEEE Standard for the Scheme Programming Language	1990	Software development standard outside of scope
IEEE 1196	Standard for a Simple 32-Bit Backplane Bus: NuBus	1987	Hardware standard outside scope
IEEE 1206	Title: IEEE Standard Methods for Measuring Transmission Performance of Telephone Handsets and Headsets	1994	Not Applicable
IEEE 1209	Recommended Practice for the Evaluation and Selection of CASE Tools	1992	Guideline – not a standard
IEEE 1219	Standard for Software Maintenance	1992	Software development standard outside of scope
IEEE 1224	OSI Abstract Data Manipulation API Language Independent	1993	Low-level standard – below level of current <i>COE</i> detail
IEEE 1228	IEEE Standard for Software Safety Plans	1994	Software development standard outside of scope
IEEE 1295	IEEE Standard for Information Technology X Window System Modular Toolkit Environment (MTE)	1993	Software development standard outside of scope

Standard Name	Standard Title	Standard Date	Rationale
IEEE 1298	Software Quality Management System Part 1: Requirements	1992	Software development standard outside of scope
IEEE 1327	IEEE Standard for Interconnection (OSI) Abstract Data Manipulation C Language Interfaces - Binding for Application Program Interfaces (API)	1993	Low-level standard – below level of current COE detail
IEEE 1328	Standard for Information Technology Test Methods for Measuring Conformance to Open Systems Interconnection (OSI) Abstract Data Manipulation C Language Interfaces Binding for Application Program Interface (API)	1993	Low-level standard – below level of current COE detail
IEEE 1351	IEEE Standard for Information Technology ACSE and Presentation Layer Services Application Program Interface (API) [C Language Independent]	1994	API not standard
IEEE 1364	IEEE Standard Hardware Description Language Based on the Verilog 174; Hardware Description Language	1995	Hardware standard outside scope
IEEE 1394.2	Standard for Serial Express: A Scalable Gigabit Extension to the IEEE Standard Serial Bus	n/a	Hardware standard outside scope
IEEE 1420.1	Software Reuse - Data Model for Reuse Library Interoperability: Basic Interoperability Data Model (BIDM)	1995	Software development standard outside of scope
IEEE 1465	Software Packages - Quality Requirements and Testing	n/a	Software development standard outside of scope
IEEE 1496	IEEE Standard for a Chip and Module Interconnect Bus: SBus	1993	Hardware standard outside scope
IEEE 1754	IEEE Standard for a 32-bit Microprocessor Architecture	1994	Hardware standard outside scope
IEEE 2003.1	IEEE Standard for Information Technology Test Methods for Measuring Conformance to POSIX 174; Part1: System Interfaces	1992	Test standards for IEEE 1003
IEEE 269	IEEE Standard Methods for Measuring Transmission Performance of Analog and Digital Telephone Sets	1992	Hardware standard outside scope
IEEE 730	Software Quality Assurance Plans	1989	Not Applicable
IEEE 771	Programmed Inquiry Learning or Teaching (PILOT)	1989	Not applicable to Project EASI/ED
IEEE 802.10	Interoperable LAN/MAN Security (SILS) Currently Contains Secure Data Exchange (SDE) (Clause 2)	1992	Adopting Federal standards for information system security
IEEE 802.11	Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications	1997	Not applicable to Project EASI/ED
IEEE 802.2	Logical link control	1994	Low-level standard – below level of current COE detail
IEEE 802.5	Token ring access method and physical Layer Specification	1997	Competes poorly with Ethernet

Standard Name	Standard Title	Standard Date	Rationale
IEEE 802.7	Broadband Local Area Networks	1989	Obsolete
IEEE 802.9	Standard for Integrated Services (IS) LAN Interface at the Medium Access Control (MAC) and Physical (PHY) Layers	1994	Low-level standard – below level of current COE detail
IEEE 828	Standard for Software Configuration Management Plans	1990	Software development standard outside of scope
IEEE 829	Standard for Software Test Documentation	1983	Software development standard outside of scope
IEEE 830	Recommended Practice for Software Requirements Specifications	1993	Software development standard outside of scope
IEEE 8802-6	Distributed Queue Dual Bus (DQDB) access method and physical layer specifications	1990/1997	Similar to IEEE 802.6
IEEE P1363	Standard Specifications for Public-Key Cryptography	n/a	Proposed standard; still under development.
IEEE P1596.2	Recommended Practice for Cache Optimizations for Large Numbers of Processors using the Scalable Coherent Interface	n/a	Proposed standard; still under development.
IEEE P2001	Recommended Practice for Internet Practices - Web Page Engineering - Intranet/Extranet Applications	n/a	Proposed standard; still under development
IEEE P730	Standard for Software Quality Assurance Plans	n/a	Proposed standard; still under development
IEEE P802.10	Standard for Interoperable LAN/MAN Security (SILS)	n/a	Proposed standard; still under development.
IEEE P802.10d	Standard for Interoperable LAN Security (SILS) Part D - Security Management	n/a	Proposed standard; still under development
IEEE P802.14	Cable-TV Based Broadband Communication -	n/a	Cable TV technology not relevant to Project EASI/ED
IEEE P802.8	Recommended Practice for Fiber Optic Local and Metropolitan Area Networks	n/a	Proposed standard; still under development
IEEE P828	Standard for Software Configuration Management Plans	n/a	Proposed standard; still under development
IEEE P829	Standard for Software Test Documentation	n/a	Proposed standard; still under development
IEEE P830	Recommended Practice for Software Requirements Specifications	n/a	Proposed standard; still under development
IEEE P8802-5	Token ring access method and physical layer specifications	n/a	Proposed standard; still under development
Internet Standard 0012	Network Time Protocol (NTP) (Version 2) Specification and Implementation	1989	Competes unsuccessfully with DCE 1.1: Time Services Specification.
Internet Standard 0019	NetBIOS Service Protocols. (API)	1987	Low-level standard – below level of current COE detail
Internet Standard 0023	Quote of the Day Protocol	1983	Not Applicable

Standard Name	Standard Title	Standard Date	Rationale
Internet Standard 0026	Time Server Protocol.	1983	Competes with DCE 1.1: Time Services Specification. Less robust.
Internet Standard 0033	The TFTP Protocol (Revision 2)	1992	FTP preferred
Internet Standard 0035	ISO Transport Service on top of the TCP (Version: 3).	1978	Not applicable; used to transition from TCP/IP to ISO-based networks
Internet Standard 0036	Transmission of IP and ARP over FDDI Networks.	1993	FDDI not recommended
Internet Standard 0039	Interface Message Processor: Specifications for the Interconnection of a Host and an IMP (Revised).	1981	Obsolete – original switching node on the ARPANET
Internet Standard 0042	Standard for the transmission of IP datagrams over experimental Ethernet networks.	1984	Experimental
Internet Standard 0045	Internet Protocol on Network System's HYPERchannel: Protocol Specification.	1993	HYPERchannel technology is obsolete
Internet Standard 0046	Transmitting IP traffic over ARCNET networks.	1993	ARCNET technology is obsolete
Internet Standard 0048	Standard for the transmission of IP datagrams over NetBIOS networks.	1993	NetBIOS is nor recommended
Internet Standard 0049	Standard for the transmission of 802.2 packets over IPX networks.	1993	IPX is proprietary and not recommended
Internet Standard 0052	The Transmission of IP Datagrams over the SMDS Service.	1991	SMDS is not recommended
ISO 10005	Quality Management - Guidelines for Quality Plans	1995	Not Applicable
ISO 10303	Product Data Representation and Exchange	1994	Not Applicable
ISO 10744	SGML-based standard for hypermedia documents.	1992	SGML is not recommended because of complexity; PDF and XML are preferred
ISO 11577	Network Layer Security Protocol (NLSP)	1994	Approved Federal security standards are preferred
ISO 13407	Human-centered design processes for interactive systems	1997	Not applicable
ISO 7942	Graphical Kernel System (GKS)	1985	Not applicable – intended for graphics intensive applications

Standard Name	Standard Title	Standard Date	Rationale
ISO 8327	Open Systems Interconnection - Basic connection oriented session protocol specification.	1987	Obsolete – functionality provided through TCP/IP
ISO 8571	Information processing systems - Open Systems Interconnection - File Transfer - Access and Management	1988	Obsolete – functionality provided through TCP/IP
ISO 8602	Information processing systems - Open Systems Interconnection - Protocol for providing the connection-less-mode transport service	1995	TCP/IP is preferred
ISO 8613	Text and Office Systems - Office Document Architecture	1989/1995	ODA is too complex and not applicable
ISO 8649	Information processing systems -- Open Systems Interconnection - Service definition for the Association Control Service Element (ACSE)	1988	TCP/IP is preferred
ISO 8650	Protocol specification for the Association Control Service Element	1988	TCP/IP is preferred
ISO 8652	Programming languages - Ada	1987	Ada is not recommended
ISO 8802-2	Logical Link Control		Similar to IEEE 802
ISO 8859-1	Information processing - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1	1987	Too low-level
ISO 9000	Guidelines for Selection and Use	n/a	Not Applicable
ISO 9001	Model for Quality Assurance in Design/Development, Production, Installation, and Servicing	1994	Not Applicable
ISO 9002	Model for Quality Assurance in Production, Installation and Servicing	1994	Not Applicable
ISO 9003	Quality Systems - Model for Quality Assurance in Final Inspection and Test	1994	Not Applicable
ISO 9004-1	Quality Management and Quality Systems Elements - Part 1: Guidelines	1994	Not Applicable
ISO 9004-2	Quality Management and Quality System Elements - Part 2: Guidelines for Services	1991	Not Applicable
ISO 9004-4	Quality Management and Quality System Elements - Part 4: Guidelines for Quality Improvement	1993	Not Applicable
ISO 9040	Virtual Terminal Basic Class Service and Protocol	1990	TCP/IP is preferred
ISO 9069	SGML support facilities - SGML Document Interchange Format (SDIF)	1988	SGML is not recommended
ISO 9241-10	Dialogue principles	1996	Subordinate of ISO 9241
ISO 9241-15	Command language dialogues	n/a	Subordinate of ISO 9241
ISO DIS 9241-11	Guidance on Usability	n/a	Not Applicable
ISO JTC1/SC21	Conceptual Schema Modeling Facility	n/a	Not Applicable

Standard Name	Standard Title	Standard Date	Rationale
ISO/IEC 10036	Information Technology -- Font Information Interchange	1993	Too low-level
ISO/IEC 10148	Information processing systems - Open Systems Interconnection - Basic Remote Procedure Call (RPC) using OSI Remote Operations	n/a	DCE RPC preferred
ISO/IEC 10166-1	Information Technology-Text and Office Systems-Document Filing and Retrieval (DFR), Part 1: Abstract Service Definition and Procedures	1991	Functionality provided through preferred standard AIIM DMA 1.0
ISO/IEC 10175	Document printing application	n/a	Too low-level
ISO/IEC 10180	Standard Page Description Language (SPDL)	n/a	PDF and XML preferred
ISO/IEC 10206	Information technology - Programming languages - Extended Pascal	1991	C and Java preferred
ISO/IEC 10607	Information technology - International Standardized Profiles AFTnn- File Transfer - Access and Management	1990	TCP/IP protocols preferred
ISO/IEC 10857	Information Technology Microprocessor Systems Futurebus 174	1994	Hardware standard outside scope
ISO/IEC 10861	Information Technology High-performance synchronous 32-bit bus: MULTIBUS II	1994	Hardware standard outside scope
ISO/IEC 11179	Specification and Standardization of Data Elements	1994	Software development standard, outside scope
ISO/IEC 11586-1	OSI Generic upper layers security: Overview	1996	TCP/IP protocols preferred
ISO/IEC 11586-4	OSI Generic upper layers security: Protecting transfer syntax specification	1996	TCP/IP protocols preferred
ISO/IEC 11756	MUMPS	1992	MUMPS not applicable to Project EASI/ED
ISO/IEC 12207	Software Life Cycle Processes	n/a	Software development standard, outside scope
ISO/IEC 13213	Information technology Microprocessor systems Control and Status Registers (CSR) Architecture for microcomputer buses	1994	Hardware standard outside scope
ISO/IEC 13719-1	Portable Common Tool Environment (PCTE) API	n/a	Too low-level for current COE detail
ISO/IEC 13719-2	PCTE Part 2: C programming language binding	1995	Too low-level for current COE detail
ISO/IEC 14252	Guide to the POSIX 174; Open Systems Environment	1996	Guideline – not a standard
ISO/IEC 14575	Information Technology Heterogeneous InterConnect (HIC), (Low-Cost, Low- Latency Scalable Serial Interconnect for Parallel System Construction)	n/a	Hardware standard outside scope
ISO/IEC 1539	Fortran	n/a	C and Java preferred over Fortran

Standard Name	Standard Title	Standard Date	Rationale
ISO/IEC 15802-2	Local and metropolitan area networks - Common specifications - Part 2: LAN/MAN management	1995	Similar to IEEE 802.2
ISO/IEC 15802-4	Local and metropolitan area networks - Common specifications - Part 4: System load protocol	1994	Similar to IEEE 802.4
ISO/IEC 7185	Information technology - Programming languages - Pascal	1990	C and Java preferred over Pascal
ISO/IEC 7498-2	Information technology - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture	1990	Adopting Federal standards for information system security
ISO/IEC 8072	Transport service definition.	1994	TCP/IP protocols preferred
ISO/IEC 8073	Transport Protocol	1992	Functionality provided through preferred standard TCP/IP suite
ISO/IEC 8651-4	Graphical Kernel System (GKS) language bindings - Part 4: C	1995	Only applicable to graphics intensive applications
ISO/IEC 8823-1	Connection-oriented Presentation Protocol specification	1994	Functionality provided through preferred standard TCP/IP suite
ISO/IEC 8824	Specification of Abstract Syntax Notation One (ASN.1)	1990	Not applicable
ISO/IEC 8825	Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)	1990	Not applicable
ISO/IEC 9072	Text communication - Remote Operations	1996	Roll-up
ISO/IEC 9126	Information technology - Software product evaluation - Quality characteristics and guidelines	1991	Not applicable
ISO/IEC 9548	Session connection- less protocol to provide the connection-less-mode session service	n/a	TCP/IP protocols preferred
ISO/IEC 9576	Connection-less -presentation protocol specification.	1991	TCP/IP protocols preferred
ISO/IEC 9579	Remote Database Access (RDA)	1993	Not aligned with FIPS Pub 127-2
ISO/IEC 9594	X.500	1993	ITU X.500 considered
ISO/IEC 9595	Common management information service definition	1991	MIB-II preferred
ISO/IEC 9596	Common management information protocol	1991	Functionality provided through preferred standard SNMP
ISO/IEC 9804	Service definition for the commitment, concurrency and recovery service element	1994	Not widely implemented
ISO/IEC 9805-1	Protocol for the Commitment - Concurrency and Recovery service element - Protocol Specification	1994	Not widely implemented
ISO/IEC 9899	Programming languages - C	1990	Covered by other C standards
ISO/IEC 9945-1	Portable Operating System Interface (POSIX) - Part 1: System Application Programming Interface (API) [C Language]	1996	Similar to IEEE 1003.1
ITU H.324	Terminal for Low Bit Rate Multimedia Communications	1996	Not applicable

Standard Name	Standard Title	Standard Date	Rationale
JIEO-E-2300	Electronic Forms Requirement	1994	DoD specific
NETCDF	Network Common Data Form (NETCDF)	n/a	Software development standard
NIAM	Natural Language Information Analysis Method	n/a	Guidelines – not standard
OSF DME	License management and Distribution services	n/a	Functionality provided through preferred standard CAE Specification C430
PGP	Pretty Good Privacy (PGP)	1991	Does not support PKI and security architecture
Recommendations T.0-T.63-Study Group VIII	CCITT Blue Book, Volume VII-Facsimile VII.3, "Terminal Equipment and Protocols for Telematic Services"		Recommendations – not standards
RFC 1006	ISO Transport Service on top of the TCP Version: 3	1987	Not applicable – intended for transition from TCP/IP to ISO-based networks
RFC 1034	(DNS) Domain Names - Concepts and Facilities	1987	Security extensions – Federal approved security standards preferred
RFC 1049	Content Type Header Field	n/a	Functionality provided through SMTP
RFC 1050	Remote Procedure Call Protocol Specification	1988	Not as good as DCE 1.1: Remote Procedure Call
RFC 1088	A Standard for the Transmission of IP Datagrams over NetBIOS Networks	1989	NetBIOS is not recommended
RFC 1094	NFS: Network File System Protocol Specification	1989	Functionality covered by WebNFS
RFC 1132	A Standard for the Transmission of 802.2 Packets over IPX Networks	1989	IPX is proprietary; TCP/IP is preferred
RFC 1179	Line Printer Daemon Protocol	1990	Too low-level
RFC 1201	Transmitting IP Traffic over ARCNET Networks	1991	ARCNET is obsolete
RFC 1209	The Transmission of IP Datagrams over the SMDS Service	1991	SMDS is not recommended
RFC 1212	Structure of Management Information (SMI)	n/a	Competes poorly with MIB-II
RFC 1274	The COSINE and Internet X.500 Schema	1991	Not applicable
RFC 1305	Network Time Protocol (Version 3)	1992	Timing services corresponding to the operating system should be used. DCE timing services should be specified for distributed systems.
RFC 1356	Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode	1992	X.25 is a legacy standard
RFC 1497	BOOTP Vendor Information Extensions	n/a	Too low-level
RFC 1508	Generic Security Service Application Program Interface	1993	Federal security standards preferred
RFC 1528	Principles of Operation for the TPC.INT Subdomain Remote Printing -- Technical Procedures	1993	Too low-level

Standard Name	Standard Title	Standard Date	Rationale
RFC 1542	Clarifications and Extensions for the Bootstrap Protocol (BOOTP)	1993	Too low-level
RFC 1577	Classical IP and ARP over ATM	1994	Too low-level
RFC 1647	TN3270 Enhancements	1994	Internet Standard 0008 recommended
RFC 1772	Application of BGP In the Internet	1995	Functionality provided through TCP/IP suite
RFC 1779	A String Representation of Distinguished Names	1995	Too low-level
RFC 1808	Relative Uniform Resource Locators	1995	Emerging
RFC 1812	Requirements for IP Version 4 Routers	1995	Hardware specification – not applicable
RFC 1848	MIME Object Security Services (MOSS)	n/a	S/MIME is preferred
RFC 1945	Hypertext Transfer Protocol - HTTP/1	1996	Protocol for delivering hypertext documents on the Web. Provides a uniform protocol for Web access
RFC 1957	Some Observations on Implementations of the Post Office Protocol (POP3)	1996	Does not provide a standard
RFC 2065	Domain Name System Security Extensions	1997	Federal security standards preferred
RFC 2136	Dynamic Updates in the Domain Name System (DNS Update)	1997	A proposed standard which updates RFC 1035.
RFC 2137	Secure Domain Name System Update (DNS)	1997	Federal security standards preferred
RFC 2302	Tagged Image File Format (TIFF) - image/tiff MIME Sub-type Registration	1998	Proposed standard
RFC 2306	Tagged Image File Format (TIFF) - F Profile for Facsimile	1998	Proposed standard
RFC 738	Time Server	1977	Functionality provided through preferred standard Internet Standard 26.
RFC 791	Internet Protocol	1981	Covered by Internet Standard 0005
RFC 793	Transmission Control Protocol (TCP)	1981	Covered by Internet Standard 0007
RFC 821	Simple Mail Transfer Protocol	n/a	Covered by Internet Standard 0010
RFC 822	Standard for the Format of ARPA Internet Text Messages	n/a	Succeeded by SMTP
RFC 854	Telnet Protocol Specification	1983	Covered by Internet Standard 0008
RFC 855	Telnet Option Specifications	1983	Covered by Internet Standard 0008
RFC 919	Broadcasting Internet datagrams	1984	Too low-level
RFC 950	Internet standard subnetting procedure	1985	Not applicable
RFC 951	Bootstrap Protocol (BOOTP)	1985	Too low-level
RFC 974	Mail Routing and the Domain System	n/a	Too low-level
RFC-1042	Transmission of IP Datagrams over IEEE 802 Networks		Too low-level
RFC-1155	Structure of Management Information (SMI)		Too low-level
RFC-1157	Simple Network Management Protocol (SNMP)		Covered by Internet Standard 0015
RFC-1390	Transmission of IP and ARP over FDDI Networks		FDDI not recommended
RFC-1583	Open Shortest Path First Routing Version 2, for unicast routing	1994	Too low-level

Standard Name	Standard Title	Standard Date	Rationale
RFC-1584	Multicast Extensions to OSPF for multicast routing	1994	Emerging
RFC-826	An Ethernet Address Resolution Protocol		Too low-level
RFC-894	Standard for the Transmission of IP Datagrams Over Ethernet Networks		Too low-level
RFC-903	A Reverse Address Resolution Protocol (RARP)		Covered by Internet Standard 0038
RTF	Rich Text Format (RTF)	n/a	PDF and XML preferred
TTY and TDD	Teletype and Telecommunications Devices for the Deaf	n/a	TTY's have been in use since 1960's
WAVE 27	WAVE 27 Waveform Structures (encapsulated as RIFF)	n/a	Covered by RIFF
X.21	The Physical Layer	1976	Legacy
X/Open C180	OSI-Abstract-Data Manipulation (XOM)	1991	API not standard
X/Open C190	API to Directory Services (XDS)	1991	API not standard
X/Open C192	COBOL Language	1991	Covered by ANSI X3.23
X/Open C194	Byte Stream File Transfer (BSFT)	1991	FTP preferred
X/Open C195	IPC Mechanisms for SMB	1992	Guidelines for software development
X/Open C203	Commands and Utilities - Issue 4	1992	Superseded by X/Open C436.
X/Open C204	System Interface Definitions - Issue 4	1992	Superseded by X/Open C434.
X/Open C206	Management Protocol Profiles (XMPP)	1993	MIB-II preferred
X/Open C209	Protocols for X/Open PC Interworking: SMB - Version 2	1992	SMB is not recommended
X/Open C210	Common Programming Interface for Communications (CPI-C)	1992	Superseded by X/Open C419.
X/Open C213	Supplementary Definitions - Issue 3	1992	Defines terminology
X/Open C214	Programming Languages - Issue 3	1989	Programming languages defined elsewhere
X/Open C218	Protocols for X/Open Interworking: XNFS - Issue 4	1992	Defined by other standards
X/Open C303	ACSE / Presentation Services API (XAP)	1993	TCP/IP protocols preferred
X/Open C305	Message Store API	1993	Too low-level
X/Open C306	Management Protocols API (XMP)	1994	Too low-level
X/Open C307	Data Management: SQL Remote Database Access	1993	Subordinate to ANSI SQL
X/Open C309	X/Open DCE: Remote Procedure Call	1994	Superseded by X/Open 706.
X/Open C312	X/Open DCE: Directory Services	1994	Superseded by X/Open C705.
X/Open C317	API to Directory Services (XDS) - Issue 2	1994	API standard not in scope of this COE
X/Open C320	Motif Toolkit API	1995	API standard not in scope of this COE
X/Open C321	Calendaring and Scheduling API (XCS)	1995	XCDE not recommended
X/Open C323	XCDE Services and Applications	1995	XCDE not recommended
X/Open C324	XCDE Definitions and Infrastructure	1995	XCDE not recommended
X/Open C408	Remote Operations Service Element (XAP-ROSE) API	1995	API standard not in scope of this COE

Standard Name	Standard Title	Standard Date	Rationale
X/Open C409	ACSE/Presentation: Transaction Processing API (XAP-TP)	1995	API standard not in scope of this COE
X/Open C415	File Transfer Access and Management (FTAM) API	1996	TCP/IP protocols preferred
X/Open C419	The XCPI-C Specification, Version 2	1995	Superseded X/Open C210.
X/Open C423	Common Management Facilities (XCMF)	1997	Replaced X/Open C421.
X/Open C429	Systems Management: Data Storage Management (XDSM) API	1996	API standard not in scope of this COE
X/Open C432	Common Object Request Broker (CORBA)	1994	Replaced by CORBA v2
X/Open C434	System Interface Definitions - Issue 4 - Version 2	1994	Supersedes X/Open C204
X/Open C435	System Interfaces and Headers - Issue 4 - Version 2	1994	Too low-level
X/Open C437	X/Open Curses, Issue 4	1995	Superseded by X/Open 610.
X/Open C438	Networking Services	1994	X/Open Transport Interface and Sockets are not recommended
X/Open C441	Generic Security Service API (GSS-API) Base	1995	Federally approved security standards preferred
X/Open C449	Data Management: Structured Query Language (SQL), Version 2	1996	References FIPS Pub 127-2
X/Open C453	SNA Transport Provider Using XTI	1994	SNA is legacy
X/Open C501	File System Safe UCS Transformation Format (UTF-8)	1995	Standard for legacy systems
X/Open C502	Systems Management: GDMO to XOM Translation Algorithm	1995	API not standard
X/Open C520	Multiprotocol Transport Networking (XMPTN): Address Mapper	1996	Recommending TCP/IP as only protocol suite
X/Open C521	Multiprotocol Transport Networking (XMPTN): Access Node	1996	Recommending TCP/IP as only protocol suite
X/Open C522	Multiprotocol Transport Networking (XMPTN): Data Formats	1996	Recommending TCP/IP as only protocol suite
X/Open C523	Networking Services - Issue 5	1997	X/Open Transport Interface and Sockets are not recommended
X/Open C529	X/Open Baseline Security Services (XBSS)	1995	Refers to X/Open XS; however, there is no product entry in X/Open XS
X/Open C604	Commands and Utilities - Issue 5	1996	Covered by POSIX
X/Open C605	System Interface Definitions - Issue 5	1996	Covered by POSIX
X/Open C606	System Interfaces and Headers - Issue 5	1996	Covered by POSIX
X/Open C608	API to Directory Services (XDS) - Issue 3	1996	API standard not in scope of this COE
X/Open C609	API to Electronic Mail (X.400) - Issue 3	1996	API standard not in scope of this COE
X/Open C610	X/Open Curses - Issue 4, Version 2	1996	API standard not in scope of this COE
X/Open C611	Structured Transaction Definition Language (STDL)	1996	Not applicable

Standard Name	Standard Title	Standard Date	Rationale
X/Open C614	X/Open Networking: Data Link Provider Interface (XDLPI)	1997	Not applicable
X/Open C615	Transport Provider Interface (XTPI)	1997	Not applicable
X/Open C616	Portable Layout Services: Context-dependent and Directional Text	1997	Not applicable
X/Open D010	Indexed Sequential Access Method	1990	Not applicable
X/Open G110	Guide to the Internet Protocol Suite	1991	A guide, not a standard
X/Open G150	Guide to Selected X.400 and Directory Services APIs	1991	A guide, not a standard
X/Open G207	Systems Management: Reference Model	1993	A guide, not a standard
X/Open G211	ISO and Internet Management: Coexistence and Interworking	1992	A guide, not a standard
X/Open G304	Internationalization Guide - Version 2	1993	A guide, not a standard
X/Open G307	Distributed TP: Reference Model - Version 2	1993	Replaced by DTPv3
X/Open GN	XPG4 Network File System	1992	Functionality provided by preferred standard WebNFS
X/Open PN	XPG4 PC-NFS Server	1992	Functionality provided by preferred standard WebNFS