

FINAL

Defense Information Systems Agency

Reliability and Engineering Organization

Center for Standards

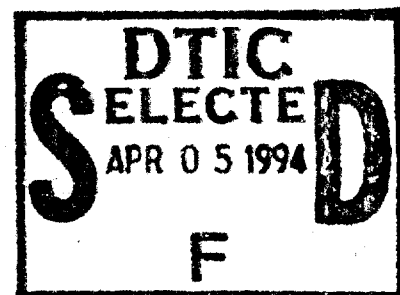
A286 736

Department of Defense

Technical Architecture Framework

for Information Management

Volume 7



Adopted Information Technology Standards (AITS)

Version 2.0

2 August 1994

This document has been approved
for public release and sales its
distribution is unlimited

95-01136

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204 Arlington, VA 22202-4302 and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 29 March 95	3. REPORT TYPE AND DATES COVERED Final		
4. TITLE AND SUBTITLE DoD Technical Architecture Framework for Information Management (TAFIM) Vol 7 - Adopted Information Technology Standards (AITS)		5. FUNDING NUMBERS -		
6. AUTHOR(S) DISA/JIEO/CFS				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) DISA/JIEO/CFS		8. PERFORMING ORGANIZATION REPORT NUMBER -		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) DISA/JIEO/CFS		10. SPONSORING/MONITORING AGENCY REPORT NUMBER -		
11. SUPPLEMENTARY NOTES Field 25 should contain the identifier CIM (Collection), as detailed in A. Washington DTIC-OCS IOM, dated April 11, 1994.				
12a. DISTRIBUTION/AVAILABILITY STATEMENT Available to DoD, other US Gov departments and Agencies, their contractors, and universities		12b. DISTRIBUTION CODE This document has been approved for public release and sale; its distribution is unlimited.		
13. ABSTRACT (Maximum 200 words) This is vol 7 of The Technical Architecture for Information Management (TAFIM). It provides a collection consolidated listing of the DoD Adopted Information Technology Standards (AITS). The AITS is the definitive set of information technology (IT) standards to be used in the DoD.				
14. SUBJECT TERMS TAFIM, CIM (Collection)		15. NUMBER OF PAGES 1		
		16. PRICE CODE -		
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED	

Preface

The *Adopted Information Technology Standards* (AITS) is a product of the Department of Defense (DOD) Defense Information Systems Agency (DISA), Joint Interoperability and Engineering Organization (JIEO), Center for Standards (CFS). It was developed with support from the DOD Commanders-in-Chief (CINCs), Services, and Agencies and was approved by the Standards Coordinating Committee (SCC). Further information on the application of this document can be found in the AITS companion document, the *Information Technology Standards Guidance* (ITSG). Both documents may be obtained from:

Help Desk
Department of Defense
Standards Assistance Directorate
DISA/ JIEO/CFS/ TBD
10701 Parkridge Blvd
Reston, Virginia 22091-4398
e-mail: Helpdesk@jcdbs.2000.disa.mil

Accession For	
NTIS	☒
DTIC	☐
Unannounced	☐
Justification	
By	
Distribution /	
Availability Codes	
Dist	Avail and/or Special
A-1	

Forward: An Executive Summary

This volume of the Technical Architecture Framework for Information Management (TAFIM) provides a consolidated listing of the DOD's AITS. The objective of the AITS is to provide consistent standards guidance across the Enterprise, Mission, Function, and Application levels of the DOD Integration Model as described in Volume 1 of the TAFIM. The AITS is the definitive set of information technology (IT) standards to be used in the DOD. The standards and specifications adopted by the AITS are approved as the standard for satisfying each Base Service Area (BSA) function.

Accompanying implementation guidance is contained in the ITSG. The AITS identifies those standards adopted for common DOD usage. Each standard has been selected from among peer standards with the potential to address the same BSA. The table structure of Volume 7 has been aligned with the Technical Reference Model (TRM) Volume 2. The set of adopted standards extends beyond the architectural goal structure of the TRM to address additional BSAs encompassing other standards outside the scope of the TRM (e.g., process standards). Where an extension to the TRM model is necessary, the extension name appears in the AITS table in italics. The ITSG provides additional, supporting information about the AITS standards. The ITSG also identifies additional standards not contained in the AITS because of deficiencies, lack of maturity, or other factors that preclude their inclusion in the AITS. The ITSG also provides recommendations for specifying standards in system acquisition documents.

The AITS provides the current set of DOD adopted standards mature enough to merit broad scale use across DOD programs. Emerging, or goal, standards that are predictable replacements for adopted standards are identified via footnote or annotation to guide planning decisions as far into the future as possible.

1.0 INTRODUCTION

1.1 PURPOSE

The purpose of the AITS is to guide DOD Enterprise acquisitions and guide the migration of legacy systems. The objective is to provide direction and supporting standards information guidance enabling DOD managers to guide their programs and projects toward a collective DOD Open Systems Environment (OSE). The AITS is the definitive volume of IT standards to be used in the DOD. The goal in providing effective and usable standards guidance is to support the broader TAFIM objectives of:

- Improve user productivity
- Improve development efficiency
- Improve portability and scalability
- Improve interoperability
- Promote vendor independence
- Reduce life cycle costs
- Improve security
- Improve manageability

1.2 SCOPE

The AITS is the definitive set of IT standards to be used in the DOD. The AITS applies to all DOD IT programs and initiatives. The AITS is the common DOD IT standards reference applicable to all Life-Cycle decisions affecting interoperability, portability, and scalability and is to be used to guide in the development of standards profiles. The term *adopted* is used to mean that the standards and specifications in the AITS are approved by DOD as the standards and specifications in the AITS are approved by DOD as the standard method for satisfying each BSA function. This standards guidance is applicable to all systems and programs whether at the leading edge of technology or preserving current operational capability in a long standing legacy system. Migration toward Open System Environments remains an ever present goal, because of the enhancement of competition, interoperability, and portability. The following recent directives and instructions were published to support the goal:

- a. DOD Directive (DODD) 4630.5, *Compatibility and Interoperability of Tactical Command, Control, Communications, and Intelligence Systems*, promulgated in

November, 1992, requires that procedures be established for the development, coordination, review, and validation of compatibility, interoperability, and integration of Command, Control, Communications, and Intelligence (C3I) systems. It further stipulates that all C3I systems developed for use by U.S. forces are considered to be for joint use.

b. DOD Instruction (DODI) 4630.8, also promulgated in November, 1992, directs that the Chairman of the Joint Chiefs of Staff (CJCS) provide amplifying instructions for implementing DODD 4630.5. DODI 4630.8 also stipulates that the CFS is responsible for evaluating program acquisition documents (Mission Need Statements (MNSs), Operational Requirements Documents (ORDs), Test and Evaluation Master Plans (TEMPs)) from an IT standards perspective and that an IT standards profile be developed and submitted for CFS review no later than Milestone II.

c. In January 1993, DODI 8120.2, *Automated Information System (AIS) Life Cycle Management (LCM) Process, Review, and Milestone Approval Procedures*, was promulgated, stipulating that all Automated Information Systems (AISs) programs incorporate standards planning, including the development of IT standards profiles per the TAFIM.

d. The entire policy came together in July, 1993, with the promulgation of CJCS Instruction (CJCSI) 6212.01, implementing DODD 4630.5 per direction by DODI 4630.8. CJCSI 6212.01, replacing MOP 160, effectively combined policies stipulated by DODD 4630.5 and DODI 8120.2 by expanding the scope of the CJCS's responsibility for the development, coordination, review, and validation of compatibility, interoperability, and integration of C4I systems. The fourth "C" (computers) was intended to account for AIS (primarily business systems) under DODI 8120.2.

At this point, DOD policy clearly stipulates that all C4I systems, now covering the entire spectrum of the DOD Enterprise Model, are required to produce IT standards profiles requiring certification by the CFS.

The AITS does not contain data administration policy, standards, or procedures. These can be found in DODD 8320.1, *Data Administration*, September 26, 1991, and DOD 8320.1-M-1, *DOD Data Element Standardization*, March 1994.

The adopted standards in the AITS are derived from a larger volume, the *Information Technology Standards Guidance* (ITSG). The AITS and ITSG work

together, but perform very different roles. The role of the AITS is to provide consistent guidance applicable across the Enterprise, Mission, Function and Applications level of the DOD Integration Model. It is intended to contain summary information only. The role of the ITSG is to provide additional, supporting information to the standards in the AITS. This relationship between the AITS and ITSG is illustrated in the figure below:

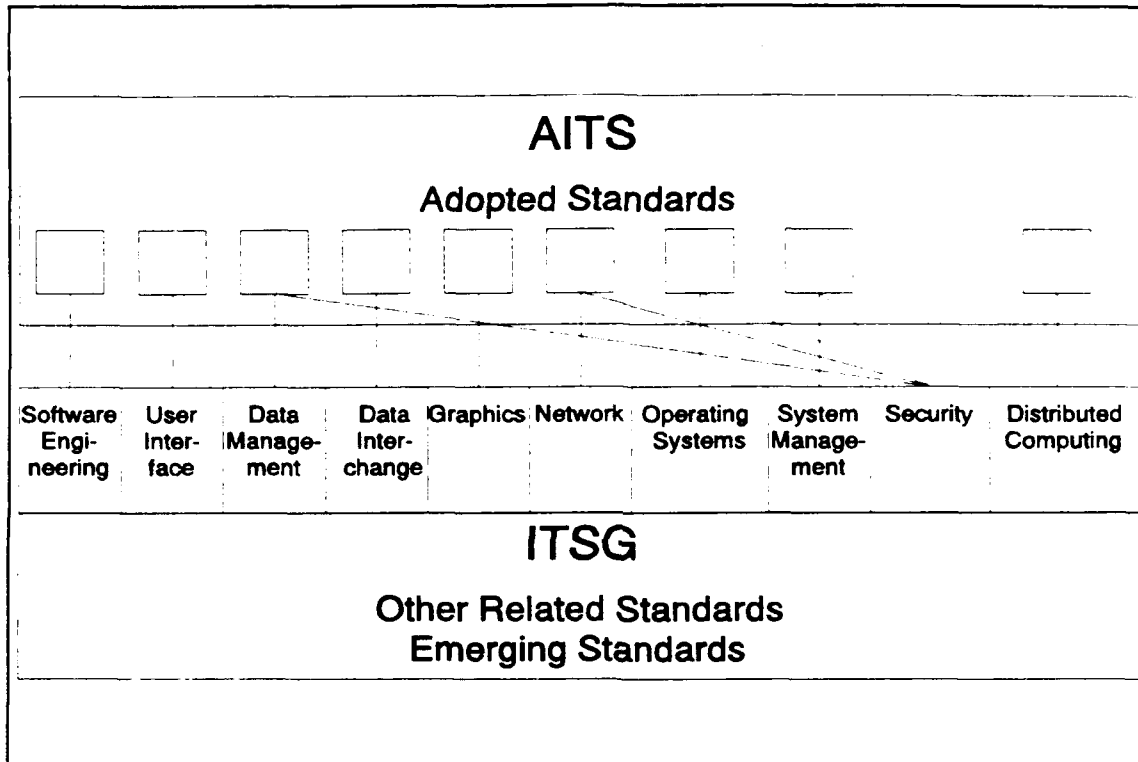


Figure 1. Relationship between AITS and ITSG.

The ITSG identifies additional standards not contained in the AITS because of their lack of maturity, deficiencies, or other exclusionary factors. Supporting information to clarify standard selections made in the AITS can be found in the ITSG such as the standards hierarchy (order of preference) used in the AITS. Future ITSG releases will contain information supporting the AITS such as test system references, known test beds, and known interoperability and related standards information.

1.3 AUDIENCE

The AITS provides adopted DOD standards and the ITSG provides amplifying implementation guidance to:

- a. Organizational policy makers who develop guiding policies.
- b. System managers and resource sponsors who validate requirements.
- c. System architects and planners who identify the functional requirements needed to fulfill the program or system requirements.
- d. Acquisition officials and supporting system engineers who will utilize the AITS in contractual actions.
- e. Implementors who will use the information to assist in development and modernization efforts not supported by system profiles.

1.4 HISTORY

Originally DOD IT standards guidance was promulgated as a chapter of the DOD TRM. The TRM was based upon the National Institute of Standards and Technology (NIST) product called the Application Portability Profile (APP). DISA/ JIEO/ CFS had also embarked on an initiative to provide detailed implementation guidance and develop a consensus based DOD definition of an OSE with the document called "The Open Systems Environment Profile for Imminent Acquisitions (OSE/IA)". The TAFIM initiative has captured the collective guidance and information of all these efforts and is now integrated and promulgated as Volume 7 of the TAFIM, *the Adopted Information Technology Standards*, the AITS. This consensus standards profile is the product of an extensive coordination and review process regulated by the Defense Standardization Program, per DOD 4120.3-M (Defense Standardization Program Policies and Procedures). Its development was accomplished through the support of multiple technical working groups and comprehensive reviews by the CINCs, Services and Agencies.

1.5 FUTURE STANDARDS REQUIREMENTS

The technology within the focus of the AITS and the ITSG is growing and changing dynamically. Additionally, the standards organizations are actively adding to the body of consensus based standardization information. The emerging internationalization of IT requirements is stimulating both harmonization and acceleration of standardization activity to accommodate compatibility and competitiveness in the world arena. To meet the challenges of the fast-paced IT domain and the decentralized decision-making essential to the execution of DOD programs, the AITS and accompanying ITSG are evolving together in a manner consistent with events in standards bodies. They will be published on a regular cycle. CFS, within DISA, is responsible for the evolution of the IT standards policy and is prepared to provide customer assistance in applying the information provided. The consumer of AITS and ITSG information is encouraged to contact CFS for assistance or to identify functional requirements and/or standards not yet incorporated into the document. The CFS will appreciate additional inputs on the use of specific standards, deficiencies, and future needs using the response form found in the ITSG.

1.6 AITS DEVELOPMENT AND COORDINATION PROCESS

The Standards Coordinating Committee (SCC) supports the CFS in carrying out their duties to lead, manage, integrate and coordinate efforts to develop, implement, integrate and coordinate efforts to develop, implement and provide standards guidance in DOD information systems. It supports the CFS in carrying out the DOD 4120.3-M responsibilities under the DOD's Standardization Directory (SD)-1 standardization program. The SCC provides a single DOD focal point to coordinate all DOD IT standards activities including promoting and integrating DOD participation in the non-government standards development process, and integrating DOD standardization activities with non-DOD (e.g., federal, national, and international) standardization activities. This panel promotes the development and use of IT standards within DOD. The SCC is the IT standards issue resolution panel for the Military Communications-Electronics Board (MCEB) and Intelligence Systems Board (ISB). The SCC meets quarterly, or as required, to address issues. The committee is chaired by the Director, JIEO, CFS, who acts as the executive agent for DOD IT standards.

Supporting the SCC and CFS in providing standards guidance are Working Groups (WGs), each focused on an AITS major service area such as graphical user interface or security. These WGs are "open" to all DOD Agencies for resolution of technical

guidance issues surrounding the AITS, generated by AITS distribution to DOD Agencies for coordination. The names of CFS individuals responsible for each AITS major service area can be found in Volume 1 of the ITSG.

This version of the AITS is the first to achieve approval by the SCC after several transformations of the format and degree of supporting information presented. This constitutes a baseline for the collective set of IT standards to be commonly used for DOD systems. With this baseline established all future changes and updates will be accomplished in reference to this baseline. It is acknowledged that a supporting configuration management process needs to be defined and approved to govern the maintenance of the AITS. Accordingly, the CFS has committed to, and undertaken, a project to develop and adopt a configuration management process for the AITS set of standards. This process definition will be reviewed and commented upon by all supporting Working Groups, coordinated with the SCC member organizations, and presented to the SCC for approval.

2.0 OSE PRINCIPLES AND THE AITS

2.1 OPEN SYSTEM DEFINITION

The TRM, AITS, and ITSG together comprise a definition of the service areas supported within the IT domain detailed down to the BSAs. BSAs define fundamental OSE functions. Through the process of standardization upon a consistent and stable framework of BSAs it becomes possible to compare and contrast the efficacy of competing standards. The aggregate definition of functionalities described by the BSAs becomes the DOD definition of an OSE. This OSE provides the consistent framework for describing functional requirements, assessing standardization needs, and supporting development of profiles.

The ITSG includes a definition of the DOD OSE. It is based on the DOD TRM Major Service Areas and an industry accepted definition of an OSE. It extends the current OSE definition to enable identification of required functions and services including those that are not yet supported by standards. Primary TRM definition elements are:

- Application Program Interfaces (APIs); and
- External Environment Interfaces (EIs).

The services are partitioned into BSAs identifying specific OSE functions. The AITS structure expands these definitions beyond those in the TRM to cover additional, more detailed, areas to achieve DOD open system goals. The evolving ITSG's OSE definition adds the following elements to complement those OSE elements above:

- Base Service Areas,
- Procedural Standards,
- Bindings, and
- Environment Transition Paths.

2.2 STANDARDS AS REQUIREMENTS

Within each program using IT to accomplish system functions, the underlying standards comprise a specialized subset of the OSE "Requirements Definition." Standards support the accomplishment of a functional requirement in a manner consistent with common practice, best value, and optimal adaptability to "yet to be identified" requirements. The innovation underway today will be tomorrow's legacy.

Effective use of commonly adopted standards to regulate the implementation of definable functions increases the likelihood of adaptability and interoperability throughout the life-cycle of a system or application. However, total expression of OSE requirements using standards is impractical because of the need to specify requirements where no standards exist.

2.3 DOD INFORMATION TECHNOLOGY STANDARDS MANAGEMENT

In every instance where there is an identified need for adoption of an open commercial standard to support a DOD requirement, there is an accompanying need to ascertain the appropriate DOD role within the related standardization project.

2.3.1 STANDARDS LEADERSHIP AND ADVOCACY SUPPORT ROLE. For those requirements where the technical solution to a DOD requirement falls within the scope of an existing standardization initiative and the technology is relatively mature, it is usually best for DOD's standards representatives to support an existing process and advocate for the unique elements of the DOD requirement. In this way, the DOD requirement becomes aligned with a broadly supported standard and optimizes the opportunity for commercialization of the DOD requirement. The increasing internationalization in the IT market provides greater opportunities for the expression of DOD requirements in a standardization forum where interoperability and compatibility with international allies can be accomplished through open standards.

2.3.2 PRODUCT SELECTION ROLE. For those requirements where the technical solution is at the forefront of technology, standardization has seldom occurred in time to satisfy the DOD implementation requirement. Clear identification of "best practice" by a standardization organization has not been possible due to the immaturity of the technology and emerging innovations. In these cases, it is sometimes in the best interest to select a most probable "best practice." This selection must then be supported by an aggressive and effective advocacy throughout the standard's life-cycle by DOD's standards representatives to ensure its adoption in an appropriate open and consensus-regulated standardization body. The life-cycle requirement may motivate escalation of the standardization initiative to an international forum. The preliminary and rapidly evolving definition of the new standard may require specification via mechanism of lower preference in the hierarchy of standards. As implementations become proven and the technology matures, the DOD goal is to ensure the specification is migrated upward in

preference in the hierarchy of standards through the execution of a life-cycle plan for the standard.

3.0 ADOPTED INFORMATION TECHNOLOGY STANDARDS

3.1 SUPPORTING PROCESS

The evolution of the AITS will see expansion of major and mid-level service areas, BSAs, and updates to the supporting standards. This growth will be guided by the various Working Groups. Working Groups will define DOD requirements and evaluate the technical standardization solutions. The Center for Architecture (CFA) and CFS will integrate their efforts to accomplish the upgrade to the AITS and ensure its timely promulgation through regular updates to the TAFIM.

3.2 DOD INTEGRATION MODEL

The DOD Integration Model, described in Volume 1, is a method for achieving functional and technical integration of business processes and information systems. It describes five integration levels, each building on the levels below.

- a. Level 1 is the Enterprise (or DOD-wide) Level. Level 1 encompasses information management (IM) elements that are mandatory across the DOD. It includes IT and IM policy, procedures, standards, and doctrine. This level also includes standard IT capabilities such as technical and data standards, reference models, and architectures, methods and tools, and shared computing and communications services. The Enterprise Level standards are represented by the AITS.
- b. Level 2, the Mission Level is comprised of major DOD mission-areas such as Command and Control Systems, Intelligence Systems, and Mission Support or Business Systems. At this level, areas of specialization and functional focus emerge and mandatory DOD-wide technical requirements and capabilities are supplemented with mission-area specific requirements and capabilities. Mission Level standards guidance is promulgated in a Mission Area Profile based on the AITS.
- c. Level 3, the Function Level, breaks the Mission areas into the multiple activities and processes of the DOD as identified in DOD 8020.1-M. Architectures and standards are defined for the "to-be" functional practices and processes as based on Mission Level architectures.
- d. Level 4, the Application Level, includes the development, maintenance and operation of individual information systems. In the integration concept each

mission-area application can support a process, an activity, or a complete function. Individual information system profiles are developed in consonance with the applicable Mission and Function Level profiles.

e. Level 5, the Personal Level, includes personal productivity tools and individual tailoring of automated capabilities for the end-users. The tailoring must conform to guidelines and procedures that ensure the integrity of shared resources as well as effective operations.

3.3 STANDARDS SELECTION CRITERIA

The AITS addresses IT standards requirements across the DOD. The adoption of one specification from among several addressing a common function requires thorough consideration of several criteria. Crucial tests for inclusion of a specification at the Enterprise Level in support of the OSE goal include the public availability of the specification and the consensus process regulating control of the specification's life-cycle. The following are the key criteria contributing to the selection of a standard for inclusion in the AITS. These criteria are an expansion of the criteria used to evaluate standards within the NIST APP.

a. Meets DOD requirements. DOD functional requirements will determine the standards that are adopted for DOD use. There is a shift away from military-unique specifications and toward "dual use" of commercial technology. Increasing the use of commercial technologies can lower costs for all concerned. In the case of many "process" and "product" standards, best business practice may also be the optimal solution for DOD, even when 100% of DOD requirements may not be satisfied. However, despite all efforts to identify commercially based specifications, there will continue to be unique military requirements warranting DOD defined specifications.

b. Legal requirements. Requirements based on the law may specifically mandate the use of specific standards. Automated Data Processing (ADP) standards development was excluded from the Federal Standardization Program in 1965 when Public Law 89-306 (the Brooks Act) established a specific program for standardization of ADP. In addition, the Brooks Act has been amended by Public Law 99-500 which expanded the definition of ADP to include certain aspects of telecommunications previously contained in the Federal Telecommunications Standards Program, and by the Computer Security Act of 1987 (P.L. 100-235). The program to standardize ADP, as defined in these public laws, is carried out by the

NIST. Mandatory Federal Information Processing Standards (FIPS) are listed in the *Federal ADP and Telecommunications Standards Index*, Doc. No. KMR-94-1-A, published by the General Services Administration.

- c. Public specification. Consistency with the ultimate goal of an OSE is a key criteria in the selection of standards. Some specifications offer a good technical solution, but are not available in an open public forum for potential bidders or developers to utilize.
- d. Consensus based. The level of consensus, both within industry and across the DOD, is an important consideration. Specifications that are controlled by a single corporate entity, unregulated by a "consensus" processes, are not favored. Acquisition guidance advocates competitiveness in procurement to reduce cost and promote innovation.
- e. Product availability. The degree of market support for specific standards predicts future competitiveness among products implemented upon the standard. Degree of product availability and implementation may influence standard selection on the basis of this criteria.
- f. Maturity of technology. The maturity of the technology and/or the uniqueness of innovative application of a proven technology may impact selection of specific standards. The standards selected for the DOD profile will represent technologies that have matured to the point where standardization is appropriate, but have not reached a point of obsolescence.
- g. Testability. The ability to validate conformance of an implementation with the specified standard may be crucial to the attainment of the required capabilities. This is especially important for those implementations with interoperability requirements. Standards selected from the AITS will be those accompanied by standards which define the procedures by which conformance to the standard are measured. Additional consideration is given to standards which have an existing conformance testing infrastructure in place. There is also a need for test beds which could research, describe, and document degrees of interoperability; perform Operational Test and Evaluation (OT&E) of operational systems to verify the effectiveness and compliance of implemented designs.
- h. Internationalization. Election of one specification over another may be influenced by the extent of internationalization which includes the ability to accommodate different cultural conventions, character sets, and representations.

Requirements for interoperability with allies and foreign suppliers may warrant selection of some specification on the basis of its international sponsor or competitiveness in the international market.

i. Legacy implications. Compatibility with the installed infrastructure is frequently a requirement. Feasibility of retrofit, adaption, or other accommodating strategy must be considered. Some specifications may also be selected over others to preserve or sustain process consistency. Many process specifications invoke issues of personnel training and context consistency crucial to sustainment of other processes.

j. Security. DODD 5200.28, "Security Requirements for Automated Information Systems (AISs)," 21 March 1988, specifies minimum security requirements for AIS. Also, procedures for determining minimum AIS computer-based security requirements are described to determine the minimum evaluation class required for an AIS as defined in DOD 5200.28-STD, "DOD Trusted Computer System Evaluation Criteria," December, 1985.

k. Preference. The preceding criteria constitute technical and economic considerations as described in MIL-STD-970. After consideration of these criteria, standards will be selected for adoption based on a preference listed below. The selection of a standard or specification of lower preference is to be made only when the standards and specifications of higher preference are not technically or economically suitable for use. The order of preference, from top to bottom, is:

- Standards mandated by multi-national treaty or law
- Non-government standards
 - Adopted international standards
 - Adopted U.S. non-government standards
 - Other international or U.S. non-government standards
- Commercial item descriptions
- Performance-based Federal specifications or standards
- Performance-based, fully-coordinated military specifications or standards
- Design-based Federal specifications or standards
- Design-based, fully-coordinated military specifications or standards
- Limited coordinated military specifications or standards
- Locally prepared, one-time-use purchase descriptions.

These criteria are used to select a specific standard for DOD adoption. The priority of each standard selection criteria is determined in the context of the specific system standard solution being evaluated. It is important that the selection criteria used in

each standard selection be documented and available for use in justifying deviations in evolving the profile as the technology and specifications evolve. In addition, it is important to establish a preferred ordering of specifications within an area to support practical standards-based solutions while accommodating legacy investments. With each system developed, improved or updated, it is the overarching objective to consistently move closer to a common, practical OSE solution.

3.4 Adopted Information Technology Standards

The AITS are represented in Appendix A as a high-level tabular matrix organized by the major service areas of the DOD TRM. Each major service area in the TRM is represented in the AITS as a collection of **Mid-level Service Areas**. Mid-level Service Areas are composed of smaller, defined services called **Base Service Areas (BSAs)**. A BSA might contain an **Adopted Standard** selected to meet the functional requirements of the BSA if the adopted standard meets the criteria previously listed.

4.0 APPLICATION OF THE ADOPTED INFORMATION TECHNOLOGY STANDARDS

4.1 OVERVIEW

The AITS provides the Enterprise level OSE guidance which, when applied to DOD systems, will move DOD to an open system environment and facilitate interoperability, transportability, and scalability of applications. Each system must select from and augment the AITS with standards and specifications that apply to the specific functions the system performs. For example, an intelligence system may have a specific set of standards that differs from a finance system, based on required OSE functionalities. But both systems will comply with the AITS.

A system is designed and developed to perform specific functions. The DOD Integration Model, introduced in section 3.1, is based on the fact that systems within a functional area share many common requirements. Interoperability is enhanced by the use of a common foundation of standards within the functional domain.

The AITS provides the Enterprise Level standards guidance for DOD. All upper level profiles must comply with the AITS selected standards to meet specific system functions. Mission profiles address functional requirements common to a mission domain. Mission domain analysis identifies functionality sets to be supported by standards based implementations. Mission area profile development leads to the definition of additional functional areas with supporting standards. The process supporting the AITS life-cycle utilizes these standards efforts to generate standardization projects supporting identified needs.

Functional level profiles provide greater refinement of specific capabilities required to achieve performance objectives. Functional profiles may be applicable in multiple missions and in a repeatable manner throughout the enterprise.

The system designer is encouraged to select standards and specifications for these functions using the amplifying guidance in the ITSG. These standards and specifications together with the standards selected from the AITS will form the system profile. This system profile should be similar to most of the systems within a specific mission and function. Application level profiles include very detailed standards implementation information. As the totality of DOD systems and applications migrate toward the target OSE, the significance of option and features sets will become paramount. Through identification and understanding of these key differences, the "seamless" connectivity solutions will be identified.

4.2 INFORMATION TECHNOLOGY STANDARDS GUIDANCE (ITSG)

The ITSG is a companion document to the AITS, containing additional detail necessary for the selection of Mission, Function and Application-level standards. The ITSG is divided into the TRM major service areas: software engineering, user interface, graphics, data management, data interchange, network, operating system, system management, security, distributed processing and international ization services. The ITSG refines these service definitions, identifying over three hundred and fifty (350) Base Service Areas (BSAs) in the DOD OSE that might be required in a DOD acquisition. These range from broad areas such as programming languages to detailed services such as shared memory, help screens, and object request broker standards. For each service, the ITSG identifies consensus based industry and DOD standards, as well as unilaterally controlled specifications. It discusses deficiencies with competing standards, and identifies related standards areas. It highlights emerging standards expected to effect pre-planned product improvements or technology insertion. Each service description concludes with a DOD consensus recommendation on the standards to be applied if this OSE service is required.

4.3 RESPONSIBILITIES

4.3.1 DISA CENTER FOR STANDARDS

- a. DISA has the responsibility for developing standards and standards guidance for the DOD. This guidance is contained in the AITS and the ITSG. Guidance on the use of standards for OSE functions not covered in the AITS is provided in the ITSG.
- b. DISA will provide assistance in the development of profiles.
- c. DISA will certify profiles for compliance with DOD open system guidance.
- d. DISA will maintain a library of all profiles, particularly those at the mission and function level that form the basis for higher-level profiles.

4.3.2 MISSION/FUNCTIONAL AREA ARCHITECTS. Based on the requirements of their domain, mission and functional area architects will develop profiles that provide guidance for their levels of the integration model. These profiles will be based on the AITS and, in the case of functional profiles, will be based on the respective mission area profile. The developer will submit the profile to DISA for certification.

4.3.3 SYSTEM DESIGNERS. Systems designers will develop their application profile based on specific system requirements and using the relevant functional area profile or profiles as a starting point.

4.3.4 ACQUISITION OFFICIALS. Acquisition officials will use the profile of standards in contractual actions, and ensure that standards required on a contract are consistent with the AITS and the IM integration model hierarchy of profiles.

4.3.5 IMPLEMENTORS. Implementors will baseline their existing systems in preparation for migration to their defined system OSE objectives. Implementors will establish their target OSE definitions and ensure that standards are incorporated in the development and evolution of the system to meet their defined OSE objectives.

4.4 PROCESS

The process for developing a profile begins with an understanding of the OSE requirements of the domain for which the profile applies. Emphasis is to be placed on understanding the differences between this domain and the supporting layers of the integration model (e.g., on what sets tactical command and control apart from other command and control systems; what distinguishes logistics from general mission support applications). This requires an understanding of the underlying architectures and profiles. From this understanding, the architect or designer must identify the set of OSE services required to support the domain. Using appropriate criteria, the developer will select the standards from the AITS and ITSG to include in the profile.

Appendix A: ADOPTED INFORMATION TECHNOLOGY STANDARDS (AITS) TABLE

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
Software Engineering Services	CASE tools and environments	
	Software development environment [The ECMA PCTE standard is in the international standardization process. The replacement will be an ISO standard.]	ECMA 149 (PCTE)
		ANSI/IEEE 1209-1992 (Evaluation and Selection of CASE Tools)
		DOD-STD-1467 (Software Support Environment)
		NIST-ECMA 500-211 (Reference Model for SEE Frameworks)
		MIL-HDBK-782 (Guide for DOD-STD-1467)
	<i>Software life cycle processes</i> [ISO/IEC DIS 12207 Software Life Cycle Processes is currently in the international standardization process.] [2167A, 7935A, and 1703 are currently being revised and consolidated (aka DRAFT MIL-STD-498, Software Development and Documentation). In light of DOD's new policy on MIL-STDs, the project has been moved into the IEEE process.]	
	Configuration management	ANSI/IEEE 828-1990 (Software Configuration Management Plans)
		ANSI/IEEE 1042-1987 (Guide to Software Configuration Management)
		MIL-STD-973 (Configuration Management)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	Documentation [2167A, 7935A, and 1703 are currently being revised and consolidated (aka DRAFT MIL-STD-498, Software Development and Documentation). In light of DOD's new policy on MIL-STDs, the project has been moved into the IEEE process.]	DOD-STD-2167A (Defense System Software Development)
		DOD-STD-7935A (DOD AIS Documentation Standards)
	Joint reviews	ANSI/IEEE 1028-1988 (Software Reviews and Audits)
		MIL-STD-499A (Engineering Management)
		MIL-STD-1521B (Technical Reviews and Audits)
	Software requirements [2167A, 7935A, and 1703 are currently being revised and consolidated (aka DRAFT MIL-STD-498, Software Development and Documentation). In light of DOD's new policy on MIL-STDs, the project has been moved into the IEEE process.] [MIL-STD-490 is pending formal cancellation by the OASD/MMD/Standardization Program.]	ANSI/IEEE 830-1984 (Guide to Software Requirements Specifications)
		MIL-STD-490 (Program-Unique Specifications)
		DOD-STD-2167A (Defense System Software Development)
		DOD-STD-7935A (DOD AIS Documentation Standards)
	Software design [2167A, 7935A, and 1703 are currently being revised and consolidated (aka DRAFT MIL-STD-498, Software Development and Documentation). In light of DOD's new policy on MIL-STDs, the project has been moved into the IEEE process.]	ANSI/IEEE 1016-1987 (Recommended Practices for Software Design Descriptions)
		ANSI/IEEE 1016.1-1993 (Guide for Software Design Descriptions)
		ANSI/IEEE 990-1987 (Recommended Practices for Ada as a Program Design Language)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
		DOD-STD-2167A (Defense System Software Development)
		DOD-STD-7935A (DOD AIS Documentation Standards)
	Software management indicators	ISO/IEC 9126 (Quality Characteristics)
		ANSI/IEEE 982.2-1988 (Guide for the Use of Standard Dictionary of Measures to Produce Reliable Software)
		ANSI/IEEE 1045-1992 (Software Productivity Metrics)
		ANSI/IEEE 1061-1992 (Software Quality Metrics Methodology)
		ANSI/IEEE 982.1-1988 (Standard Dictionary of Measures to Produce Reliable Software)
	Software testing and product evaluation [2167A, 7935A, and 1703 are currently being revised and consolidated (aka DRAFT MIL-STD-498, Software Development and Documentation). In light of DOD's new policy on MIL-STDs, the project has been moved into the IEEE process.]	ANSI/IEEE 829 (Software Test Documentation)
		ANSI/IEEE 1008-1987 (Software Unit Testing)
		NIST FIPS PUB 132 (Guideline for Software Verification and Validation Plans)
		ANSI/IEEE 1059 (Guide for Software Verification and Validation Plans)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
		DOD-STD-2167A (Defense System Software Development)
		DOD-STD-7935A (DOD AIS Documentation Standards)
	Software quality assurance	ISO 9001 (Model for Quality Assurance)
		ISO 9000-3 (Guidelines for Application of ISO 9001)
		ANSI/IEEE 730-1989 (Software Quality Assurance Plans)
		IEEE 1298-1992 (Software Quality Management System)
		DOD-STD-2168 (Defense System Software Quality Program)
		MIL-HDBK-286 (Guide for DOD-STD-2168)
	Software problem categories/priorities [2167A, 7935A, and 1703 are currently being revised and consolidated (aka DRAFT MIL-STD-498, Software Development and Documentation). In light of DOD's new policy on MIL-STDs, the project has been moved into the IEEE process.]	IEEE 1044-1993 (Classification for Software Anomalies)
		DOD-STD-2167A (Defense System Software Development)
		DOD-STD-7935A (DOD AIS Documentation Standards)
	Software safety	MIL-STD-882 (System Safety Program Requirements)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	Software support	ANSI/IEEE 1219-1993 (Software Maintenance)
		MIL-HDBK-347 (Mission-Critical Computer Resources Software Support)
	Programming languages	
	Logic and math functions	IEEE 754 (Floating point)
	Ada [The Ada programming language is MANDATORY for new DOD software development]	ISO 8652 (Ada)
	C	ISO 9899 (C)
	FORTTRAN	NIST FIPS PUB 69-1 (FORTTRAN)
	COBOL	NIST FIPS PUB 21-3 (COBOL)
	JOVIAL	MIL-STD-1589C (JOVIAL)
	MUMPS (aka "M")	NIST FIPS PUB 125 (MUMPS)
	Language bindings	
	Ada bindings [The ECMA PCTE binding standards are in the international standardization process. The replacements will be ISO standards.]	ECMA 162 (Binding to PCTE)
		ISO 9075 (Binding to SQL)
		ISO/ANSI 8651-3 (Binding to GKS)
		ISO 8806-3 (Binding to GKS-3D)
		ISO/ANSI 9593-3 (Binding to PHIGS)

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
		IEEE 1003.5 (Binding to POSIX)
		ANSI X3.168 (Embedded SQL)
	C Bindings [The ECMA PCTE binding standards are in the international standardization process. The replacements will be ISO standards.]	ECMA 158 (Binding to PCTE)
User Interface Services	Client Server Operations	
	Data stream encoding	NIST FIPS PUB 158-1 (X Windows)
	Data stream interface	
	Subroutine foundation library	
	Bitmap distribution format	
	User Interface Management System	
	Communication between GUI client applications	OSF Motif ICCCM (Inter Client Communications Convention) Manual)
	Data interchange format for GUI-based applications	
	Compound text encoding	X/Open CTE (Compound Text Encoding)
	X logical font description	X/Open XLFD (X Logical Font Description)
	Integration with 3-D graphics	NIST FIPS PUB 158-1 (PEX for X Windows)
	Object definition and management	
	GUI internationalization support	X/Open Internationalization Guide
	Interchange format for design tools	COSE Motif Toolkit
	Application programming interfaces	IEEE 1295 (Modular Toolkit Environment, aka Motif)
	Language bindings for bit-mapped GUIs	

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	Style guide	DOD HCI Style Guide, V3.0
	User interface definition language	OSF Motif UIDL (User Interface Definition Language)
	Dialog support	
	Style guide	DOD HCI Style Guide, V3.0
	On-line help	
	Drivability	
	Commands, menus, and dialog services	
	Keyboard device layout	ISO 9995 (Keyboard Layouts for Text/Office Systems)
	Window management	
	Independent window management services	OSF Motif 1.2
	Multiple displays	
	Style guide	DOD HCI Style Guide, V3.0
	On-line help	
Data Management Services	Data management system	
	Basic database services	FIPS PUB 127-2 (SQL)
	Multidatabase APIs	X/Open SAG CLI
	Electronic forms	JIEO-E-2300
	Data dictionary/directory services	
	Data dictionary	NIST FIPS PUB 156 (IRDS)
	Transaction processing	
	Protocol for interoperability in heterogeneous transaction processing systems	ISO 10026 (CCR)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	Transaction manager-to-resource manager interface	X/Open C193 (OSI Distributed TP: The XA Specification)
	Transaction demarcation	X/Open P209 (TX Specification)
	Transaction manager-to-communications manager interface [Complementary standards]	X/Open S214 (XA+ Specification)
		X/Open S216 (XATMI Specification)
		X/Open S218 (TxRPC Specification)
	Recovery/restart services for long running transactions	IEEE 1003.1a (POSIX System API Extensions)
	Distributed queuing	IEEE P1003.15 (POSIX Batch Queuing/Scheduling Extensions)
	<i>Database security</i>	
	Database security	DOD 5200.28-STD (TCSEC) NCSC-TG-021 (TDI)
Data Interchange Services	<i>Characters and symbols</i>	
	Character sets	NIST FIPS PUB 1-2 (Code for Information Exchange)
	Font information exchange	ISO/IEC 9541-1,2 (Font Information Interchange)
	<i>Hardware applications</i>	
	External data representation	ITU (CCITT) X.409 (XDR for X.400)
	Hardware design data exchange	NIST FIPS PUB 172 (VHDL)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	Printer data exchange	ISO/IEC 10180 (Standard Page Description Language)
	Bar coding	MIL-STD-1189B (Standard DOD Bar Code Symbolology)
	Physical interface [Alternative standards; choose all that apply]	NIST FIPS PUB 22-1 (Signalling Rates)
		NIST FIPS PUB 100-2 (DTE/DCE Interface, DTE/DTE Interface)
		NIST FIPS PUB 162 (1200bps two-wire duplex modems)
		NIST FIPS PUB 163 (2400bps two-wire duplex modems)
		NIST FIPS PUB 164 (2400bps four-wire duplex modems)
		NIST FIPS PUB 165 (4800bps four-wire duplex modems)
		NIST FIPS PUB 166 (4800 and 9600bps two-wire duplex modems)
		NIST FIPS PUB 167 (9600bps four-wire duplex modems)
		NIST FIPS PUB 168 (12000 and 14400bps four-wire duplex modems)
		NIST FIPS PUB 169 (Error correction)
		NIST FIPS PUB 170 (Modem data compression)
	<i>Optical Digital Technologies</i>	
	Read-only optical discs	ISO 9660 (Volume and file structure of CD-ROM)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	Write-once optical discs	ISO/IEC 9171-1 (130mm Optical Disk Cartridge, Write Once, Unrecorded Optical Disk Cartridge)
		ISO/IEC 9171-2 (130mm Optical Disk Cartridge, Write Once, Recording Format)
		ANSI X3.191-1991 (130mm Write-Once Sample Servo RZ Selectable-Pitch Optical Disk Cartridge)
		ANSI X3.211-1992 (130mm Write-Once Optical Disk Cartridge Using Continuous Composite Servo)
		ANSI X3.214-1992 (130mm Write-Once Optical Disk Cartridge Using Sampled Servo and 4/15 Modulation)
		ISO/IEC 11560:1992 (130mm Optical Disk Cartridges of the Write-Once, Read Multiple (WORM) Type, Using the Magneto-Optical Effect)
		ANSI X3.220-1992 (130mm Optical Disk Cartridge Using the Magneto-Optical Effect for Write Once Functionality)
		ISO/IEC 10885:1993 (356mm Optical Disk Cartridge, Write Once)
		ANSI X3.200-1992 (356mm Write-Once Optical Disk Cartridge)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	Rewritable optical discs	ISO/IEC 10900:1992(90mm Optical Disk Cartridges, Rewritable and Read Only)
		ISO/IEC 10089:1991(130mm Rewritable Optical Disk Cartridge)
		ANSI X3.212-1992(130mm Optical Disk Cartridge Using the Magneto-Optical Effect and Continuous Composite Servo Format)
	Document interchange	
	Office document exchange [Alternative standards - Adherence to CALS specifications and standards should be maintained to the maximum extent possible, as use of CALS provides maximum interoperability. In the event that a CALS standard cannot convey the technical information of a particular application, only then is the use of a non-CALS standard justified.] [ODA is not strongly supported and has been proposed for deletion from the next version of this profile.]	MIL-M-28001B (CALS SGML)
		NIST FIPS PUB 152 (SGML)
		ISO 8613 (ODA and Interchange Format)
	Electronic Forms interchange	JIEO-E-2300 (FIMS)
	Technical data Interchange	
	Vector graphics data interchange [Alternative standards - see note to Office document exchange]	MIL-D-28000A(1) (CALS IGES)
		NIST FIPS PUB 177 (IGES)
		MIL-D-28003A(1) (CALS CGM)
		NIST FIPS PUB 128-1 (CGM)
		MIL-STD-2301 (NTFS CGM)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	<i>Raster/image data interchange</i>	
	Raster data interchange [See still image compression for more fax standards suitable for raster data interchange.]	MIL-R-28002B(1) (CALS Raster)
		NIST FIPS PUB 150 (Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus)
	Image data interchange [See Still image compression and Graphics data interchange for more standards suitable for image data interchange.]	MIL-STD-2500 (National Imagery Transfer Format (NITF) Version 2.0 for the NITFS)
		MIL-HDBK-1300 (National Imagery Transfer Format Standards (NITFS))
	Product data interchange [Alternative standards - see note to Office document exchange - Currently IGES is the most mature and widely implemented standard for conveying product data information.]	MIL-D-28000A(1) (CALS IGES)
		NIST FIPS PUB 177 (IGES)
		ISO 10303 (STEP)
	Business data interchange	NIST FIPS PUB 161 (EDI)
	<i>DOD applications</i>	
	Military logistics and document support [Alternative standards] [2167A, 7935A, and 1703 are currently being revised and consolidated (aka DRAFT MIL-STD-498, Software Development and Documentation). In light of DOD's new policy on MIL-STDs, the project has been moved into the IEEE process.]	MIL-STD-1840B (Automated Interchange of Technical Information)
		DOD-STD-2167A (Defense System Software Development)
		DOD-STD-7935A (DOD AIS Documentation Standards)
		MIL-STD-1388-1B (Logistic Support Analysis)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	Geospatial data exchange [Alternative standards]	MIL-STD-1388-2B (Logistic Support Analysis Record)
		MIL-STD-600006 (VPF)
		MIL-STD-2401 (World Geodetic System, WGS-84)
		STANAG 3809 (Digital Terrain Elevation Data, DTED)
		Digital Geographic Information Exchange Standard (DIGEST)
		NIST FIPS PUB 173 (SDTS)
		IHO SP-57 (Transfer Standard for Digital Hydrographic Data)
		MIL-STD-2411 (Raster Product Format)
	Symbology graphics [Alternative standards]	MIL-STD-2525 (Symbology Graphics)
		STANAG 2019(1) (Military Symbols for Land Based Systems)
		QSTAG 509 (Military Symbols)
		MIL-STD-1295 (US Army) (Design Criteria for Helicopter Cockpit Electro-optical Symbology)
		MIL-STD-1477B (US Army) (Symbols for Army Air Defense System Displays)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	Exchange of formatted military messages [Alternative standards; choose all that apply.]	MIL-STD-1787A (US Air Force)(Aircraft Display Symbology)
		Joint Pubs 6-04 and 3-56.24 (Message Text Formats)
		Joint Pub 6-01.1 (TADIL Message Standards) (TADIL A, B, and C)
		Joint Pub 6-01.2 (TADIL C Message Standards)
		MIL-STD-188-203A-1 (TADIL A)
		MIL-STD-188-212 (TADIL B)
		MIL-STD-188-203-3 (TADIL C)
		MIL-STD-188-220 (Interoperable Standard for Digital Message Transfer Device Subsystems)
		MIL-STD-2500 (NITFS version 2.0)
		Joint Pub 3-56.20(Joint Multi-TADIL Operating Procedures)
		JIEO Multi-TADIL Data Extraction and Reduction Guide (DERG)
		JIEO Multi-TADIL Interface Design Handbooks (IDHs)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
		Joint Tactical Information Distribution System (JTIDS) Technical Interface Design Plan - Test Edition (TIDP-TE) (TADIL J Message Standard)
		Interim Joint Tactical Information Distribution System (JTIDS) Message Specification (IJMS)
		Interim Joint Tactical Information Distribution System (JTIDS) Message Specification (IJMS) Standing Operating Procedures (SOP)
		Joint Pub 6-01.3 (Army Tactical Data Link-1 (ATDL-1) Message Standard)
		Army Tactical Data Link-1 (ATDL-1) Technical Interface Design Plan (TIDP)
		Variable Message Format (VMF) Technical Interface Design Plan - Test Edition (TIDP-TE)
		Variable Message Format (VMF) Interface Operating Procedures (IOP)
	Tactical communications	MIL-STD-2045-44500 (TACO2 for the NITFS)
	Continuous Acquisition and Life-Cycle Support (CALS) [Note: Some CALS standards are specialized versions of standards and are cited elsewhere.] [Complementary standards]	MIL-STD-1840B (Automated Interchange of Technical Information)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
		MIL-HDBK-59B (CALS Program Implementation Guide)
		MIL-M-87268 (IETM General)
		MIL-D-87269 (IETM Database)
		MIL-Q-87270 (IETM Quality)
		MIL-STD-974 (CITIS)
	<i>Compression</i>	
	Text and data compression	X/Open C203 (part of XPG4) ("pack" and "unpack")
	Graphics compression	Graphics compression standards will appear in the next version of this profile.
	Still image compression [Alternative standards]	NIST FIPS PUB 147 (Group 3 compression)
		NIST FIPS PUB 148 (General facsimile)
		NIST FIPS PUB 150 (Group 4 compression)
		ITU (CCITT) T.4 (Group 3 compression)
		ITU (CCITT) T.6 (Group 4 compression)
		ITU (CCITT) T.81 (JPEG)
		MIL-STD-188-196 (NITFS Bi-Level)
		MIL-STD-188-197 (NITFS ARIDPCM)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
		MIL-STD-188-198A (NITFS JPEG)
		MIL-STD-188-199 (Vector Quantization Decompression for the NITFS)
	Motion image compression	ISO 11172 (MPEG)
	Audio compression	Audio compression standards will appear in the next version of this profile.
	<i>Multimedia data exchange formats and protocols</i>	
	Multimedia standards will appear in the next version of this profile.	
Graphics Services	<i>Raster graphics</i>	
	Raster graphics	see Raster data interchange in Data interchange
	<i>Vector graphics</i>	
	Vector graphics API [PHIGS and GKS are alternative standards. GKS has been proposed for elimination from the next version of this profile.]	NIST FIPS PUB 153 (PHIGS)
		ISO 9592-4 (PHIGS PLUS)
		NIST FIPS PUB 120-1 (GKS)
		ISO 8805 (GKS-3D)
	Vector graphics data interchange	see Graphics data interchange in Data Interchange
	<i>Device interfaces</i>	
	Device interface API	ISO 9636 (CGI)
	<i>Maps</i>	
	DOD symbology	See Symbology graphics under Data Interchange
	Map graphics	See Geospatial data exchange under Data Interchange

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	<i>Graphics search and sort</i>	
	Graphics file formats	See Graphics data interchange under Data Interchange

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
Network Services [Currently the Federal Government is looking at the possible use of selected internet protocols, where appropriate, in future acquisitions. However, at the moment, GOSIP, FIPS 146-1, is mandated for all DOD acquisitions.]	<i>Application-oriented network services</i>	
	File transfer	MIL-STD-2045-17508, Parts 1-3, 6 (FTAM Profile)
	Remote file access	NIST FIPS PUB 146-1 (GOSIP)
	Message transfer	MIL-STD-2045-17501/17502 Parts 1-5 (MHS Profile)
		IEEE 1224.1(X.400 E-mail API)
	Terminal emulation	NIST FIPS PUB 146-1 (GOSIP)
	Remote login	NIST FIPS PUB 146-1 (GOSIP)
	Remote procedure calls	OSF DCE (Distributed Computing Environment) RPC
	Directory services [Complementary standards]	ISO 9594 (X.500 Series Recommendations, SIA-11)
		IEEE 1224.2(Directory Services/Name Space API)
		ISO 8822 (Connection-Oriented Presentation Service Definition)
		ISO 8823 (Connection-Oriented Presentation Protocol, SIA-5.8)
		ISO 8327 (Connection-Oriented Session Protocol, SIA-5.9)
	Addressing	ITU (CCITT) X.500 (ISO 9594) (SIA-11)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
		NIST FIPS PUB 146-1 (GOSIP)
		MIL-STD-2045-14500, Part 1 (Transport Profile)
	Transaction processing	ISO/IEC DISP 12061, Part 1-10 (Transaction Processing ISP) (SIA-15)
	Connection establishment/release	NIST FIPS PUB 146-1 (GOSIP)
		MIL-STD-2045-14500, Parts 1-3 (Transport Profile)
	Translation [Alternative services]	SMTP to X.400 gateway (RFC 1327/1495)
	<i>Transport-oriented network services</i>	
	Routing	NIST FIPS PUB 146-1 (GOSIP)
	Error recovery	NIST FIPS PUB 146-1 (GOSIP)
		MIL-STD-2045-14500, Parts 1-3 (Transport Profile)
	Flow control	NIST FIPS PUB 146-1 (GOSIP)
		MIL-STD-2045-14500, Parts 1-3 (Transport Profile)
	Sequencing	NIST FIPS PUB 146-1 (GOSIP)
		MIL-STD-2045-14500, Parts 1-3 (Transport Profile)
	Data compression	MIL-STD-188-196 (NITFS Bi-Level)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
		MIL-STD-188-197 (NITFS ARIDPCM)
		MIL-STD-188-198A (NITFS JPEG)
	Priority/precedence	MIL-STD-2045-14500, Part 1 (Transport Profile: Reliable End System Transport)
	Time service [Complementary standards]	IEEE 1003.1b(Real-Time Extensions to POSIX)
	Multicast	ITU-TS (CCITT) X.6 (Multicast service definition)
	<i>Security-oriented network services</i>	
	Network Security Models, Architecture, and Frameworks	ISO 7498-2 (OSI Basic Reference Model - Part 2: Security Architecture)
		ISO 10745 (Upper Layers Security Model)
		ISO 10181-2 (Security Frameworks- part 2: Authentication)
		ISO 10181-5 (Security Frameworks- part 5: Integrity)
	Integrity	IEEE 802.10B (SDE)
		ISO 11586-1 (GULS, part 1)
		ISO 11586-4 (GULS, part 4)
	Security Association and Key Management	ISP 421 (SAMP)
		ISO 11586-1 (GULS, part 1)
		ISO 11586-2 (GULS, part 2)
		ISO 11586-3 (GULS, part 3)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	Access control [Complementary standards]	NIST FIPS PUB 179 (GNMP)
		IEEE 802.10B(SDE)
		ISO 10736 (TLSP)
		ISO 11577 (NLSP)
		MIL-STD-2045-18500 (MSP)
	Authentication [Complementary standards]	NIST FIPS PUB 179 (GNMP)
		NIST FIPS PUB 180 (SHS)
		NIST FIPS PUB 186 (DSS)
		IEEE 802.10B(SDE)
		ITU (CCITT) X.509 (X.500 security)
		ISO 10736 (TLSP)
		ISO 11577 (NLSP)
		ISO 11586-1 (GULS, Part 1)
		ISO 11586-2 (GULS, Part 2)
		ISO 11586-3 (GULS, Part 3)
		ISO 11586-4 (GULS, Part 4)
		MIL-STD-2045-18500 (MSP)
	Alarm reporting [Complementary standards]	NIST FIPS PUB 179 (GNMP)
		ISO 10164-7 (Security Alarm Reporting Function)
	Auditing	ISO 10164-8 (Security Audit Trail Function)
	Security management [Complementary standards]	NIST FIPS PUB 179 (GNMP)
		ISO 10164-7 (Security Alarm Reporting Function)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
		ISO 10164-8 (Security Audit Trail)
		ISO/IEC 9595 (CMIS)
	Security labelling [Complementary standards]	ISO 10736 (TLSP)
		ISO 11577 (NLSP)
		NIST FIPS PUB 188 (SSL)
	Encryption	NIST FIPS PUB 46-2 (DES)
		NIST FIPS PUB 185 (EES)
	Traffic flow confidentiality	ISO 11577 (NLSP)
	Non-repudiation	NIST FIPS PUB 186 (DSS)
		NIST FIPS PUB 180 (SHS)
		ISO 11586-1 (GULS, part 1)
		ISO 11586-4 (GULS, part 4)
		MIL-STD-2045-18500 (MSP)
	<i>Subnetwork technologies</i>	
	Local area networks	MIL-STD-187-700
	Distributed queue dual bus	
	Fiber optic	
	Packet switching	
	Integrated services digital networks	
	Combat net radio digital subnetwork	MIL-STD-188-220 (Interoperable Standard for Digital Message Transfer Device Subsystems)
	Point-to-point leased lines	NIST FIPS PUB 146-1 (GOSIP)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
Operating System Services	Kernel operations	
	Memory management	NIST FIPS PUB 151-2 (POSIX.1, C Bindings)
	File management services	
	Device control	
	System operator services	
	Process management and core operating system services	
	Scheduling	
	Environment services	
	Event, error, and exception	IEEE Std 1003.1b-1993 (POSIX.1b, C Bindings)
	Semaphores	
	Shared memory	
	Message queues	
	Threads interface [Complementary standards]	NIST FIPS PUB 151-2 (POSIX.1, C Bindings)
		IEEE 1003.1c (POSIX.1c, C Bindings)
	POSIX.1 language bindings [Alternative standards]	NIST FIPS PUB 151-2 (POSIX.1, C Bindings)
		IEEE Std 1003.5-1992 (POSIX.5, Ada Bindings)
		IEEE Std 1003.9-1992 (POSIX.9, FORTRAN Bindings)

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	<i>Media handling</i>	
	Floppy disk format and handling	NIST FIPS PUB 151-2 (POSIX.1, C Bindings)
	Tape/archiving formats [Complementary standards]	NIST FIPS PUB 151-2 (POSIX.1, C Bindings)
		ISO DIS 9945-2 (POSIX.2/2a, C Bindings)
	<i>Shell and utilities</i>	
	Commands and utilities used in applications and shell scripts	ISO DIS 9945-2 (POSIX.2/2a, C Bindings)
	Printing	
	Language bindings to POSIX.2	
	Shell programming language	
	User-oriented commands and utilities	
	File and program editing services	
	Specialized language and compiler tools	
	Remote shell execution	
	Traditional operating system administration	NIST FIPS PUB 179 (GNMP)
	<i>Real time services and interfaces</i>	
	Real time timers	IEEE Std 1003.1b-1993 (POSIX.1b, C Bindings)
	Priority and preemptive scheduling	
	Semaphores	
	Shared memory	
	Message queues	
	Process memory locking	
	Asynchronous I/O	

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	Asynchronous event notification	
	Synchronized I/O	
	Real time file system	
	POSIX.1b language bindings	
	Memory mapped I/O	
	<i>Operating system security</i>	
	Operating system security services [Complementary standards]	DOD 5200.28-STD(TCSEC)
		NIST FIPS PUB 112 (Password Usage)
	Secure hashing services	NIST FIPS PUB 180 (SHS)
	Entity authentication mechanism services [Complementary standards]	NIST FIPS PUB 112 (Password Usage)
	NIST FIPS PUB 113 (Computer Data Authentication)	
	ISO 9807 (Requirements for Data Authentication)	
Systems Management Services	<i>Systems management</i>	
	Batch scheduling and queuing	IEEE 1003.2(POSIX.2)
	Print management	FIPS 151-2 (POSIX.1, for "lp")
	Software installation	OSF Distributed Management Environment (DME) Software Distribution Service
	Software distribution	
	Host configuration	NIST FIPS PUB 179 (GNMP)
		Network Management Forum (NMF) OMNIPoints 1

**Adopted Information Technology Standards
Version 2.0
August 2, 1994**

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	Fault management [Complementary standards]	NIST FIPS PUB 179 (GNMP)
		Network Management Forum's (NMF) OMNIPoints 1
		OSF Distributed Management Environment (DME) Event Management Services
	Security management [Complementary standards]	NIST FIPS PUB 179 (GNMP)
		Network Management Forum (NMF) OMNIPoints 1
		DOD 5200.28-STD (TCSEC)
		NCSC-TG-005 (TNI)
		NCSC-TG-021 (TDI)
		NIST FIPS PUB 151-2 (POSIX.1)
	Performance management [Complementary standards]	NIST FIPS PUB 179 (GNMP)
		OSF Distributed Management Environment (DME) Subsystem Management Services
		NIST FIPS PUB 144 (User Oriented Performance Parameters)
	License management	OSF Distributed Management Environment (DME) License Management Services
	Storage device management/archiving	OSF Distributed File System (DFS) [Note: OSF is building a gateway to Network File System (NFS).]
	Peripheral device management	

**Adopted Information Technology Standards
Version 2.0
August 2, 1994**

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards Table		Version 2.0 (Aug 94)
Major Service Area	Information Technology Standards Guidance Mid and Base Service Areas	Adopted Standard or Specification
	System startup and shutdown	OSF Distributed Management Environment (DME) Subsystem Management Services
	Accounting management	NIST FIPS PUB 96 (Charging Systems)
Distributed Computing Services	Distributed Data	
	Remote data access	ISO 9579-1.2 (RDA)
	<i>Objects</i>	
	Object request broker	OMG CORBA (Common Object Request Broker Architecture)
	<i>Client/Server</i>	
	Remote procedure call	OSF DCE (Distributed Computing Environment)
	Distributed files	
	Directory	
	Security	
	Timing	
	Threads	
	<i>System Management</i>	
	Software distribution	OSF DME (Distributed Management Environment)
	Event management	
	Subsystem management	
	License management	
	Personal computer services	
	Print management	ISO 10175 (Distributed Printing Standard (DPA))

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Alphabetic Index to Base Service Areas

Access control	36	Data Management Services	23
Accounting management	43	Data stream encoding	22
Ada	21	Data stream interface	22
Ada bindings	21	Database security	24
Addressing	34	Device control	39
Alarm reporting	37	Device interface API	33
Application programming interfaces	22	Device interfaces	33
Application-oriented network services	34	Dialog support	23
Asynchronous event notification	41	Directory	43
Asynchronous I/O	40	Directory services	34
Audio compression	32	Distributed Computing Services	43
Auditing	37	Distributed Data	43
Authentication	37	Distributed files	43
Bar coding	24	Distributed queue dual bus	38
Basic database services	23	Distributed queuing	24
Batch scheduling and queuing	41	Document interchange	27
Bitmap distribution format	22	Documentation	17
Business data interchange	28	DOD applications	28
C	21	DOD symbology	33
C Bindings	22	Drivability	23
CASE tools and environments	17	Electronic forms	23
Character sets	24	Electronic Forms interchange	27
Characters and symbols	24	Entity authentication mechanism services	41
Client/Server	43	Environment services	39
Client Server Operations	22	Error recovery	35
COBOL	21	Event, error, and exception	39
Combat net radio digital subnetwork	38	Event management	43
Commands and utilities used in applications and shell scripts	40	Exchange of formatted military messages	29
Commands, menus, and dialog services	23	External data representation	24
Communication between GUI client applications	22	Fault management	42
Compound text encoding	22	Fiber optic	38
Compression	31	File and program editing services	40
Configuration management	17	File management services	38
Connection establishment/release	35	File transfer	34
Continuous Acquisition and Life-Cycle Support (CALS)	31	Floppy disk format and handling	40
Data compression	35	Flow control	35
Data dictionary	23	Font information exchange	24
Data dictionary/directory services	23	FORTRAN	21
Data interchange format for GUI-based applications	22	Geospatial data exchange	29
Data Interchange Services	24	Graphics compression	32
Data management system	23	Graphics file formats	33
		Graphics search and sort	33
		Graphics Services	33
		GUI internationalization support	22
		Hardware applications	24

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Hardware design data exchange	24	Performance management	42
Host configuration	41	Peripheral device management	42
Image data interchange	28	Personal computer services	43
Independent window management services	23	Physical interface	25
Integrated services digital networks	38	Point-to-point leased lines	38
Integration with 3-D graphics	22	POSIX.1 language bindings	39
Integrity	36	POSIX.1b language bindings	41
Interchange format for design tools	22	Print management	41, 43
Joint reviews	18	Printer data exchange	24
JOVIAL	21	Printing	40
Kernel operations	38	Priority and preemptive scheduling	40
Keyboard device layout	23	Priority/precedence	36
Language bindings	21	Process management and core operating system services	39
Language bindings for bit-mapped GUIs	22	Process memory locking	40
Language bindings to POSIX.2	40	Product data interchange	28
License management	42, 43	Programming languages	21
Local area networks	38	Protocol for interoperability in heterogeneous transaction processing systems	23
Logic and math functions	21	Raster data interchange	28
Map graphics	33	<i>Raster graphics</i>	33
<i>Maps</i>	33	<i>Raster/image data interchange</i>	27
<i>Media handling</i>	40	Read-only optical discs	25
Memory management	38	Real time file system	41
Memory mapped I/O	41	<i>Real time services and interfaces</i>	40
Message queues	39, 40	Real time timers	40
Message transfer	34	Recovery/restart services for long running transactions	24
Military logistics and document support	28	Remote data access	43
Motion image compression	32	Remote file access	34
Multicast	36	Remote login	34
Multidatabase APIs	23	Remote procedure calls	34, 43
<i>Multimedia data exchange formats and protocols</i>	32	Remote shell execution	40
Multiple displays	23	Rewritable optical discs	27
MUMPS (aka "M")	21	Routing	35
Network Security Models, Architecture, and Frameworks	36	Scheduling	39
Network Services	34	Secure hashing services	41
Non-repudiation	38	Security	43
Object definition and management	22	Security Association and Key Management	36
Object request broker	43	Security labelling	38
<i>Objects</i>	43	Security management	37, 42
Office document exchange	27	<i>Security-oriented network services</i>	36
On-line help	23	Semaphores	39, 40
<i>Operating system security</i>	41	Sequencing	35
Operating system security services	41	Shared memory	39, 40
Operating System Services	38	Shell and utilities	40
<i>Optical Digital Technologies</i>	25	Shell programming language	40
Packet switching	38		

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Software design	18	User Interface Services	22
Software development environment	17	User-oriented commands and utilities	40
Software distribution	41, 43	<i>Vector graphics</i>	33
Software Engineering Services	17	Vector graphics API	33
Software installation	41	Vector graphics data interchange	27, 33
<i>Software life cycle processes</i>	17	Window management	23
Software management indicators	19	Write-once optical discs	26
Software problem categories/priorities	20	X logical font description	22
Software quality assurance	20		
Software requirements	18		
Software safety	20		
Software support	21		
Software testing and product evaluation	19		
Specialized language and compiler tools	40		
Still image compression	32		
Storage device management/archiving	42		
Style guide	22, 23		
<i>Subnetwork technologies</i>	38		
Subroutine foundation library	22		
Subsystem management	43		
Symbology graphics	29		
Synchronized I/O	41		
<i>System Management</i>	41, 43		
System operator services	39		
System startup and shutdown	43		
Systems Management Services	41		
Tactical communications	31		
Tape/archiving formats	40		
<i>Technical data Interchange</i>	27		
Terminal emulation	34		
Text and data compression	32		
Threads	43		
Threads interface	39		
Time service	36		
Timing	43		
Traditional operating system administration	40		
Traffic flow confidentiality	38		
Transaction demarcation	24		
Transaction manager-to-communications manager interface	24		
Transaction manager-to-resource manager interface	23		
<i>Transaction processing</i>	23, 35		
Translation	35		
<i>Transport-oriented network services</i>	35		
User interface definition language	23		
User Interface Management System	22		

Adopted Information Technology Standards
Version 2.0
August 2, 1994

Appendix B: GLOSSARY

Base Service Area: Base Service Areas (BSAs) define functionality within the OSE. They also serve as logical placeholder for groupings of standards that share similar attributes of functionality. Each BSA contains a definition, approximated to the collection of standards contained within it. Each BSA parallels an industry accepted information technology "functional " area at a broad system service level. BSA definitions serve to map functional system support software requirements to specific standards through matching the BSA definition to the standards within. BSA definitions are tailored for human comprehension, not to meet a requirement for technical formalism of the OSE.

Consensus based: Making decisions based on the agreement of a large majority of the participants

Open Systems Environment (OSE): A comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of application, data or people, as specified by information technology standards and profiles.

Profile: A set of one or more base standards, along with specific subsets, classes, options, and parameters, necessary for accomplishing a particular function.

Publicly Available: Available to public without restriction to anyone for implementation, sublicensing, and distribution (i.e., sale) of that implementation.

Specifications: A document that prescribes, in a complete, precise, verifiable manner, the requirements, design, behavior, or characteristics of a system or system component. The term is also used to identify additional information that augments a standard.

Sponsor: An advocate for a specific standard or section of a standard who provides significant resources toward the development of the standard.

Standard Selection Criteria: Criteria used in the selection of standards for a profile.

Standard: A document, established by consensus and approved by a government or non-government standards body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order and consistency in a given context.

Appendix C: ACRONYMS

AIS	Automated Information System
AI7S	Adopted Information Technology Standards
ANSI	American National Standards Institute
API	Application Program Interface
APP	Application Portability Profile
ARIDPCM	Adaptive Recursive Interpolative Pulse Code Modulation
ATDL	Army Tactical Data Link
BPS	Bits per Second
BSA	Base Service Area
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
CALS	Continuous Acquisition and Lifecycle Support
CASE	Computer Aided Software Engineering
CCITT	International Telephonic and Telegraphic Consultative Committee
CCR	Commitment, Concurrency and Recovery
CFA	Center for Architecture
CFS	Center for Standards
CGI	Computer Graphics Interface
CGM	Computer Graphics Metafile
CINC	Commander in Chief
CITIS	Contractor Integrated Technical Information Service
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	CJCS Instruction
CLI	Call Level Interface
CMIS	Common Management Information Service
CORBA	Common Object Request Broker Architecture
COSE	Common Open System Environment
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CTE	Compound Text Encoding
DCE	Data Circuit-Terminating Equipment
DCE	Distributed Computing Environment
DERG	Data Extraction and Reduction Guide
DES	Data Encryption Standard
DFS	Distributed File System
DIGEST	Digital Geographic Information Exchange Standard

DIS	Draft International Standard
DISP	Draft International Standardized Profile
DISA	Defense Information Systems Agency
DME	Distributed Management Environment
DMI	Definition of Management Information
DOD	Department of Defense
DODD	DOD Directive
DODI	DOD Instruction
DPA	Document Printing Application
DQDB	Distributed Queue Dual Bus
DSS	Digital Signature Standard
DTE	Data Terminal Equipment
DTED	Digital Terrain Elevation Data
ECMA	European Computer Manufacturers Association
EDI	Electronic Data Interchange
EEI	External Environment Interface
EES	Escrowed Encryption Standard
FDDI	Fiber Distributed Data Interface
FIMS	Forms Interface Management Standard
FIPS	Federal Information Processing Standard
FTAM	File Transfer Access and Manipulation
FTP	File Transfer Protocol
GDMO	Guidelines for the Definition of Managed Objects
GKS	Graphical Kernel System
GKS-3D	GKS for 3 Dimensions
GMI	Generic Management Information
GNMP	Government Network Management Profile
GOSIP	Government Open Systems Interconnection Profile
GUI	Graphical User Interface
GULS	Generic Upper Layer Security
HCI	Human-Computer Interface
ICCCM	Inter Client Communication Conventions Manual
IDH	Interface Design Handbook
IEC	International Electrotechnical Commission
IEEE	Institute for Electrical and Electronics Engineers

IETM	Interactive Electronic Technical Manual
IGES	Initial Graphics Exchange System
IHO	International Hydrographic Organization
IJMS	Interim JTIDS Message Specification
IM	Information Management
IOP	Interface Operating Procedures
IRDS	Information Resources Directory System
ISB	Intelligence Systems Board
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	International Standardized Profile
IT	Information Technology
ITSG	Information Technology Standards Guidance
ITU	International Telecommunications Union
JIEO	Joint Interoperability and Engineering Organization
JPEG	Joint Photographic Experts Group
JTIDS	Joint Tactical Information Distribution System
KMP	Key Management Protocol
LAN	Local Area Network
MCEB	Military Communications-Electronics Board
MHS	Message Handling System
MNS	Mission Need Statement
MPEG	Motion Picture Experts Group
MSP	Message Security Protocol
NCSC	National Computer Security Center
NFS	Network File System
NIST	National Institute of Standards and Technology
NITF	National Imagery Transfer Format
NITFS	National Imagery Transfer Format Standard
NLSP	Network Layer Security Protocol
NMF	Network Management Forum
ODA	Office Document Architecture
ODBC	Open Database Connectivity
ODT	Optical Digital Technologies

OMG	Object Management Group
ORD	Operational Requirements Document
OSE	Open Systems Environment
OSE/IA	OSE Profile for Imminent Acquisitions
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OT&E	Operational Test and Evaluation
PCTE	Portable Common Tools Environment
PEX	PHIGS Extensions to X
PHIGS	Programmer's Hierarchical Interactive Graphics System
POSIX	Portable Operating Systems Interface for Computers
PUB	Publication
RDA	Remote Data Access
RFC	Request for Comment
RPC	Remote Procedure Call
SAG	SQL Access Group
SAMP	Security Association Management Protocol
SCC	Standards Coordinating Committee
SD	Standardization Directory
SDE	Secure Data Exchange
SDTS	Spatial Data Transfer Standard
SEE	Software Engineering Environment
SGML	Standard Generalized Markup Language
SHS	Secure Hashing Standard
SIA	Stable Implementation Agreement
SME	Subject Matter Expert
SMI	Structure of Management Information
SMTP	Simple Mail Transfer Protocol
SOP	Standing Operating Procedures
SQL	Structured Query Language
SSL	Standard Security Label
STANAG	Standardization Agreement
STD	Standard
TACO	Tactical Communication Protocol
TADIL	Tactical Digital Information Link
TAFIM	Technical Architecture Framework for Information Management

TCSEC	Trusted Computer Systems Evaluation Criteria
TDI	Trusted Database Interpretation
TEMP	Test and Evaluation Master Plan
TIDP-TE	Technical Interface Design Plan - Test Edition
TLSP	Transport Layer Security Protocol
TNI	Trusted Network Interpretation
TP	Transaction Processing
TRM	Technical Reference Model
TX	Transaction Demarcation
TxRPC	Transactional Remote Procedure Call
UUCP	Unix to Unix Copy Protocol
UIDL	User Interface Definition Language
VHDL	VHSIC Hardware Description Language
VMF	Variable Message Format
VPF	Vector Product Format
WG	Working Group
WGS	World Geodetic System
XA	X/Open Architecture
XATMI	X/Open Application to Transaction Manager Interface
XA+	X/Open Architecture Plus
XDR	External Data Representation
XLFD	X Logical Font Description
XPG	X/Open Portability Guide