INFORMATION TECHNOLOGY STANDARDS GUIDANCE (ITSG)

Version 3.1

April 7, 1997

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	7 April 1997	Final

4. TITLE AND SUBTITLE
DOD Information Technology Standards Guidance (ITSG), Version 3.1

5. FUNDING NUMBERS
-

6. AUTHOR(S)
DISA JIEO CFS (JEBEA)
10701 Parkridge Blvd.
Reston, VA 20191-4398

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
DISA JIEO CFS (JEBEA)
10701 Parkridge Blvd.
Reston, VA 20191-4398

8. PERFORMING ORGANIZATION REPORT NUMBER
-

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
DISA JIEO CFS (JEBEA)
10701 Parkridge Blvd.
Reston, VA 20191-4398

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
-

11. SUPPLEMENTARY NOTES
ITSG Version 3.1 supersedes all previous versions

12a. DISTRIBUTION AVAILABILITY STATEMENT
Distribution A: Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE
-

13. ABSTRACT *(Maximum 200 words)*

The DOD Information Technology Standards Guidance (ITSG) defines the DOD Open System Environment (OSE) and provides guidance to meet the requirement for consistent selection of base standards for profiles for DOD Information Technology (IT) acquisitions. It does this by defining the DOD OSE and the target group of IT standards that DOD systems are to use in implementations. The specification of the DOD OSE and the IT standards contained within that environment using the ITSG will guide system convergence toward the DOD-consensus target environment. The ITSG is the foundation document for the Technical Architecture Framework for Information Management (TAFIM) Volume 7, the Adopted Information Technology Standards (AITS). The ITSG is a resource supporting the Joint Technical Architecture (JTA) and the AITS by tracking activity in emerging standards that may someday appear in the JTA or TAFIM Volume 7. The ITSG also provides more detailed information about the standards adopted by the AITS, which is only a list of standards. The ITSG identifies formal and emerging standards, bindings, public domain specifications, and the interrelationships among the recommended standards. It provides useful information on the recommended standards for each service area such as portability guidance and the recommended standard usage.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Standards, Information Technology, Open Systems Environment	118
	16. PRICE CODE
	-

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	-

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

EXECUTIVE SUMMARY

1. This document is approved for use by all Departments and Agencies of the Department of Defense (DOD).

2. Comments (recommendations, additions, deletions) and any pertinent data submitted for improvement of this document is addressable to the Information Processing Directorate (Code JEBE), Center for Standards (CFS), Joint Interoperability and Engineering Organization (JIEO), Defense Information Systems Agency (DISA), 10701 Parkridge Blvd., Reston, VA 20191-4357. E-mail Ms. Angela Bcoker at bookera@ncr.disa.mil or go to the DISA homepage at Http://www.itsi.disa.mil/. Please organize comments into two categories: "Essential" and "Suggested." Please include a recommendation and rationale for each proposed change. (See section 7.1 for complete instructions about commenting on this document.)

3. The Information Technology Standards Guidance (ITSG) is a tool. Its purpose is to define the DOD Open System Environment (OSE) and provide guidance to meet the requirement for consistent selection of base standards for profiles for DOD Information Technology (IT) acquisitions. It does this by defining the DOD OSE and the target group of IT standards that DOD systems are to use in implementations. The specification of the DOD OSE and the IT standards contained within that environment using the ITSG will guide system convergence toward the DOD-consensus target environment.

4. The ITSG is the foundation document for Technical Architecture Framework for Information Management (TAFIM) Volume 7, the Adopted Information Technology Standards (AITS). The ITSG is a resource supporting the Joint Technical Architecture (JTA) and the AITS by tracking activity in emerging standards that may someday appear in the JTA or the TAFIM. The ITSG also provides more detailed information about the standards adopted by the AITS, which is only a list of standards.

5. The ITSG specifies the IT standards available for each OSE base service area (BSA). The ITSG identifies formal and emerging standards, bindings, public domain specifications, and the interrelationships among the recommended standards. It provides useful information on the recommended standards for each service area such as portability guidance and the recommended standard usage.

OVERALL ITSG TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. SCOPE

1.1 Scope. The ITSG is intended for use by system engineers and program managers in planning and procuring an open information technology system by selecting standards profiles. The ITSG identifies the Open System Environment (OSE) Base Service Areas (BSAs) and the type and status of standards and specifications applicable to each BSA. Any BSA can include approved, open consensus, government standards, non-government standards, consortia and industry specifications, and other solutions. It also can include related standards that may be needed for a particular OSE BSA, caveats concerning the standards recommended that could jeopardize application portability, and information about how to tailor procurement specifications to avoid portability problems.

The standards arena is broad and is changing rapidly enough to make the ITSG quickly obsolete. The ITSG represents the consensus DOD target as it was best understood at the time of publication. The OSE defined in the ITSG reflects the considerations and realities of the marketplace and standards community. The goal of the CFS is to facilitate decentralized execution of IT program management leading to accomplishment of an enterprise-wide OSE. To that end, the ITSG will be updated on a recurring basis with sufficient frequency to maintain its relative currency and to expand the thoroughness of its coverage of the IT domain.

2. GENERAL REQUIREMENTS

2.1 Understanding open systems environments.

2.1.1 The role of standards. The fundamental premise of the ITSG is that the implementation of well aligned, standards-based open systems will lead eventually to a higher degree of interoperability and portability. Unfortunately, standards are not yet defined for all the basic services needed for all information technology systems. Additionally, standards usually contain multiple options. Many standards allow options whose use or disuse may result in systems that are compliant with the same standard yet are not interoperable with one another.

Vendors and industry organizations (i.e., consortia) have defined specifications (to augment a standard or to compete with a standard) to fill many gaps in the existing formal standards. These specifications can provide some limited portability and interoperability. Different standards-defining groups' specifications for satisfying the same basic services sometimes overlap and are incompatible even disregarding any options they may have. Identifying the basic services of a system requires a thoughtful and thorough understanding of system requirements for current and future information technology environments. After identifying the basic services, the recommended standards in the ITSG will provide a path toward the DOD consensus open system environment.

2.1.2 Achieving practical, standards-based open systems. A broad base of available standards is the basis for achieving open systems. Just choosing standards neither guarantees portability or interoperability nor guarantees easy integration of multi-vendor systems. Understanding the features and options of standards and knowing how to specify the standards is vital.

Information technology standards are layered in the architecture between the external environment and the platform or application environment. A well conceived architectural framework will list its functional requirements. The ITSG recommends standards intended to meet the functional requirements of the architecture.

2.1.3 Pitfalls of specifying only lists of standards. Profiling, which is a detailed description of the selection of options available within a standard, makes standards practical to use. However, many "open systems profiles" are only lists of standards, lacking the details to allow the standards to be implemented consistently for portability and interoperability.

The specification of lists of standards may indicate that the acquisition requirements have not been identified or considered fully. The use of standards requires the functional requirements of the system architecture be identified thoughtfully. The specification of only existing standards developed in a public consensus standards committees does not take advantage of other potential solutions available to fill other functionality areas with some form of standards implementation where such formal standards do not exist. For example, a Request for Proposal (RFP) may specify certain required Government standards or Non-Government Standards (NGS) and indicate those areas for which the bidder must propose standards. The system design areas that have a

functionality requirement not supported by adopted standards must be evaluated carefully for life cycle implications with respect to the DOD open systems environment objective.

Specification of standards by their names is not sufficient. Requirements exist for the specification, use, and exclusion of specific dependencies, extensions, and features that are implementation-defined, implementation-dependent, undefined, or unspecified within a standard. A standard's libraries, library functions, modes, options, and switch settings used in the product implementation of a standard have portability implications. International Organization for Standardization (ISO) TR-10000 and MIL-HBK-829 cover the requirement for detailed profiles more extensively.

2.1.4 Controlling the use of specific features of IT standards. Standards' features (e.g., options, extensions, levels) must be controlled within system development. Standard features adverse to future system portability must be excluded. The PM must exclude hostile and obsolete features of a standard which will impede future system portability.

2.1.5 Conformance testing. Testing implementations for conformance to a required standard is necessary. Where National Institute of Standards and Technology (NIST) conformance tests exist, validated products lists are available that will indicate the Federal Information Processing Standard (FIPS) and the individual point of contact responsible for the standard's conformance testing program. A NIST report on conformance testing and validated products can be located at ftp://speckle.ncsl.nist.gov/vpl/intro.htm.

The Open Group (X/Open) validates products through its branding program. More information regarding X/Open branded products can be located at URL http://opengroup.org/.

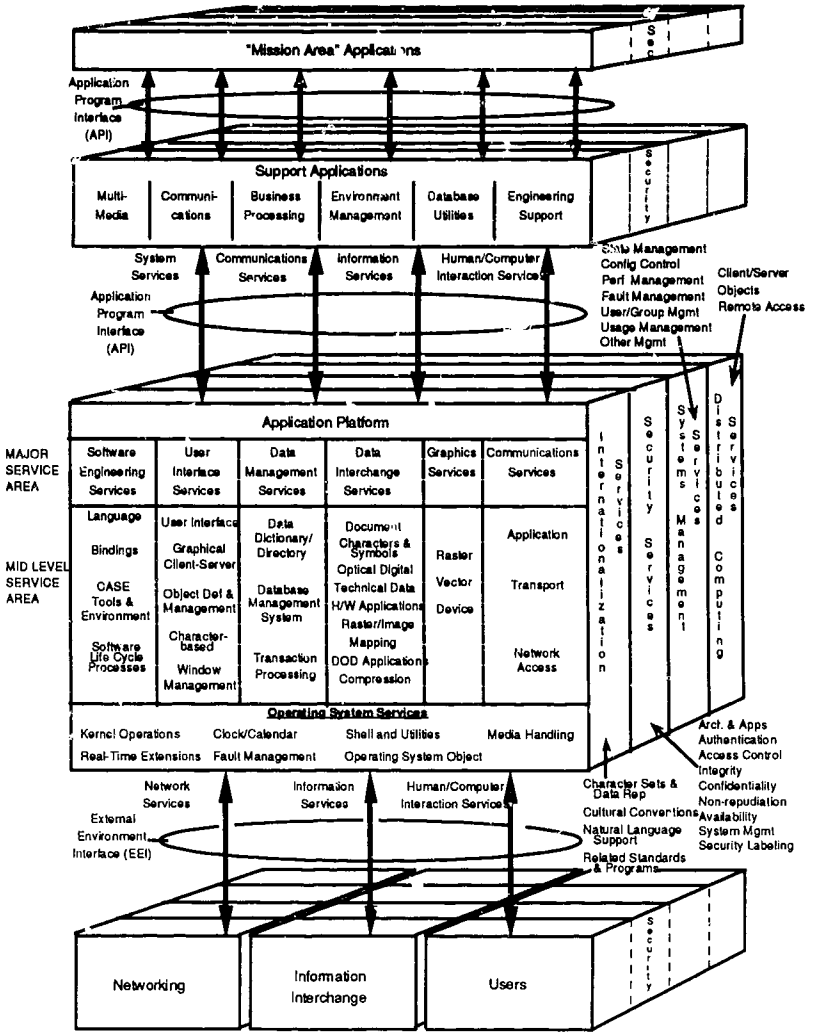
The DOD's Joint Interoperability Test Command (JITC) maintains a list of products it has tested. The list can be located at URL http://jitc-emh.army.mil/register.htm.

2.1.6 Relationship Between ITSG Standards and Weapon System Standards. The standards in the ITSG have a much broader range of applicability than just information processing systems. They are equally applicable to other systems, such as weapon systems. ITSG standards in major service areas such as data interchange, operating systems, and security are as needed by many weapon systems as Mission Critical Computer Resources (MCCR) standards are.

Among the major service areas of the ITSG that contain standards useful to military weapon systems are user interface (e.g., keyboard device layout, user interface style guides), data management (e.g., data dictionary/directory services), data interchange (e.g., physical interface, image data interchange, geospatial data exchange, tactical communications), graphics (e.g., symbology graphics), communications, (e.g., connectionless service), operating systems (e.g., real time services and interfaces), system management (e.g., fault monitoring), and security (e.g., authentication).

2.2 Structure of the ITSG. The ITSG aligns with the major service areas in the reference model in Figure 2.2-1 below, which comes from TAFIM Volume 2, the Technical Reference Model.

FIGURE 2.2-1. DOD Technical Reference Model



The major service areas in the ITSG are covered in detail in Section 3, Detailed Requirements. Because it is so large, Section 3 is divided by major and spanning service areas into separate parts of this document. After reading part one, the Introduction/Guide, the user can treat the ITSG more like an encyclopedia, exploring the standards solutions for service areas of interest. Table 2.2-1 lists the sections and the seven major and six spanning service areas along with the CFS point of contact (POC) for each. ITSG parts 2 through 8 list the major service areas; parts 9 through 14, the spanning service areas. Sections 5.1.4.2 and 5.2.2 contains further information regarding spanning and major service areas.

TABLE 2.2-1 Mapping service areas to parts

Paragraph	Service Area	CFS POC (Name, Office Code)	ITSG Part
1, 2, 3.1, 4, 5, 6, 7	Introduction/Guide	Ms. Angela Booker, JEBEA	1
3.2	Software Engineering	Mr. Jim Barnette, JEBEB	2
3.3	User Interface		3
3.4	Data Management	Dr. Dan Wu, JEBEB	4
3.5	Data Interchange	Mr. Alan Peltzman, JEBEB	5
3.6	Graphics	Mr. Alan Peltzman, JEBEC	6
3.7	Communications and Network	Mr. Ralph Liguori, JEBBD	7
3.8	Operating Systems	Mr. Curtis Royster, JEBEB	8
3.9	System Management	Mr. Larry Spieler, JEBEA	9
3.10	Security	Mr. Jim Barnette, JEBEB	10
3.11	Distributed Computing	Dr. Dan Wu, JEBEB	11
3.12	Multimedia	Dr. Doris Bernardini, JEBEB	12
3.13	Human Factors		13
3.14	Internationalization	Ms. Angela Booker, JEBEA	14

Each major service area in parts 2 through 14 is decomposed into dozens of smaller service areas called BSAs. There are additional services below the base standard, but the ITSG does not attempt to represent them. These lower levels usually involve only small parts of standards, not entire documents. Every BSA within the anticipated DOD Open System Environment is in the ITSG. For a DOD system or architecture to proceed toward an open system goal, the architectural requirements of the system must match up to these BSAs. The BSAs also show

some logical relationships that lead to identifying mid-level service areas within the major service areas.

For example, the Data Management Services major service area breaks down into mid-level service areas as follows:

a. Data management system
b. Data management security
c. Data dictionary/directory services
d. Distributed data
e. Object database
f. Transaction processing.

Within the mid-level service area called "data management system," the ITSG contains the following OSE BSAs. An example of one of these OSE BSAs follows in section 2.3.

a. Basic database services
b. Indexed sequential access
c. Electronic forms
d. Report writer
e. Database administration
f. Menu-driven database access
g. Data storage and archiving
h. Multidatabase APIs.

2.3 How to use the ITSG. The BSA descriptions are the focus of the use of the ITSG. These descriptions are in parts 2 through 14. The major and mid-level service area descriptions are no more than definitions of the logical links binding all the BSAs grouped beneath them.

A BSA is a logical entity within the OSE that requires some form of standards solution although not all BSA descriptions have standards solutions yet. Some standards logically fall within a specific BSA. In other cases, different BSAs sometimes list the same standards because a particular standard satisfies more than one BSA requirement. For each BSA identified, there is a brief definition of the BSA, and the following topics are addressed:

3.X.Y.Z.1 Standards
3.X.Y.Z.2 Alternative specifications.
3.X.Y.Z.3 Standards deficiencies
3.X.Y.Z.4 Portability caveats
3.X.Y.Z.5 Related standards
3.X.Y.Z.6 Recommendations.

In each BSA there are five paragraphs giving additional explanation of the standards listed in the standards table of the first paragraph. The standards listed in the top rows (labeled DOD "mandated" or "adopted") are given primary emphasis. The text is intended to support primarily the mandated standard. Information about the remaining standards provides assistance for the DOD legacy systems that may continue to use other standards during their transition to the DOD OSE target environment. In those sections for which no information can be reported at present, a short statement will appear stating that there is no known or reported information on this topic. Information may be added in future versions of the ITSG. An example of text that corresponds to the example standards table follows in sections 2.3.2 through 2.3.6.

2.3.1 Paragraph one: Standards. The first sub-part of the BSA description is the standards table. The standards table is the key to using the ITSG. These tables include all applicable standards satisfying the BSA. The intent is to list all of the standards that may be used within DOD to prepare for the non-open legacy systems that will be migrating toward open systems. These systems may implement standards other than the recommended ones.

It is important to remember that the standards table is not a stand alone expression of the DOD OSE recommendation. Paragraph six, the recommendation, must also be consulted for the rationale for the recommendation. Each table must be viewed in the context of the additional text provided in the BSA to understand fully the recommendation and its implications.

The following features in the standards table require further explanation:

a. Standards types and hierarchy of standards
b. Standards entries
c. The DOD adopted information technology standard
d. The "Gray Zone."

2.3.1.1 ITSG standards type definition. The ITSG defines standards types using three descriptors. These descriptors define the sc e of the sponsoring body, the availability of the specification, and the method of change control in defining or redefining the specification. This standards type definition is most useful for distinguishing among the many kinds of public specifications that are preferred in the aftermath of the cancellation of MIL-STD-970.

2.3.1.1.1 Scope. This identifies the range of intended applicability of the specification, determined largely by the sponsoring body. The permitted values for the scope descriptor are International, National, Government, Consortium, or Corporate. The latter value identifies specifications created by a single company for their own use but which may be available to others. Examples of this type include data storage formats specific to software products.

2.3.1.1.1.1 International. Standards of international scope are NGS created by accredited international NGSBs. For NGS, there is an order of precedence cited by the IEEE in P1003.0, and adapted here. The order is international standards, regional standards, national standards, draft versions of the preceding, open forum standards (e.g., professional group standards, trade association, industry, consortia), emerging (e.g., committee documents, draft regional or national standards), and de facto. Typical international NGSBs include the International Telecommunications Union (ITU) and International Organization for Standardization (ISO).

2.3.1.1.1.2 National. Standards of national scope are NGS created by accredited national NGSBs. Typical national NGSBs include the Institute for Electrical and Electronics Engineers (IEEE) and American National Standards Institute (ANSI).

2.3.1.1.1.3 Government. Standards of government scope are those standards developed or adopted by departments and agencies of the Federal government. These standards can be and often are identical to existing NGS. At times, the government mandates specific standards by law. The most important part of mandated standards (for ranking purposes) is the source of the mandate, whether by law (FIPS), DOD (JTA or OSD Directive), treaty and/or international military standardization agreement (e.g., NATO STANAG, Air Standardization Coordinating Committee). In this document, the only mandatory standards are those mandated by the JTA, and those JTA mandated standards come first in precedence. (See para. 2.3.2.3.5.1.1 for a description of Mandated status.)

2.3.1.1.1.4 Consortia. Consortia include organizations not formally recognized and accredited to make standards. Suppliers and users of information technology unite to create consortia standards. Increasingly, consortia are defining specifications that provide needed extensions to national and international standards because these standards bodies cannot anticipate users' requirements in all aspects of computing and define standards quickly enough. Sometimes these extensions arise from the NGSBs' inability to agree on a proposed portion of a standard. Consortia specifications also are created in response to the absence of standards for a needed service.

Consortia specifications achieve consensus outside of accredited NGSBs and use a consensus process for their maintenance. This consensus process of creating specifications, while not entirely

open (sometimes open only to trade associations, industry groups, and individual vendors), enables products that support portability and interoperability to be implemented. Many standards-creating consortia use a consensus process to maintain the standard, although the process may not be open. Also, such maintenance decreases the chances the applications and platforms become incompatible.

These specifications frequently become the basis for standards from NGSBs later (e.g., OSF's Motif specification became the basis for IEEE 1295.1). Most consortia specifications are available now, do not overlap with or conflict with an existing NGS or NGS under development, and exercise no restraint (except perhaps cost) on who can use the specifications or how they can use them.

2.3.1.1.1.5 Corporate. Software developers also develop standards for their own use that are not generally consensus standards. These are incorporated in software products, achieve a high degree of popularity, and become known as de facto standards. The specifications for these systems are under proprietary control. A vendor's unilateral change to their corporate standard may make other vendors' products and applications that originally were compatible incompatible. Proprietary or corporate standards are to be used only when no available commercial or government standards will support the requirement. Acquisition policies prohibit using such specifications in the same manner that the other standards in an RFP are used. The ITSG does not recommend nor specify corporate standards.

2.3.1.1.2 Availability. This identifies whether the specification is available to the Public, or if it is Private. In order to be Public, a specification must be available to anyone for a reasonable cost (i.e., for reproduction cost). Specifications that are only available to dues-paying members of a consortium are Private. Payment for a standard on a license basis rather than dues payment to a group also belongs to the Private category.

2.3.1.1.3 Change control. This identifies whether changes are controlled by a Consensus or Non-consensus process. Accredited NGSBs and the government produce standards controlled by a consensus process, since the affected organizations are given a chance to express comments before the standard is approved. A consortium may be considered to have a consensus process if the membership of the consortium is not restrictive (other than by the cost of membership). A specification controlled by a single profit-making organization is not changed by a consensus-based process.

2.3.1.1.4 Abbreviations. Some of the most used standards types will appear in abbreviated form. These types and their abbreviations are:

Corporate Private Non-Consensus (CPN-C)
Consortia Public Consensus (CPC)
Government Public Consensus (GPC)
International Public Consensus (IPC)
National Public Consensus (NPC)

2.3.1.2 Standards entries. This section describes the entries in the different columns of each standards entry in the standards table.

2.3.1.2.1 Standard type. The first column in the standard entry is the standard type as discussed in 2.3.1.1, ITSG standards type definition, above.

2.3.1.2.2 Sponsor. This column identifies the organization sponsoring or controlling changes to the specification or standard. Typical sponsors are ISO, ANSI, IEEE, NIST, or X/Open.

2.3.1.2.3 Standard. This column identifies the standard or specification by name. Many standards with different designations are identical (e.g., standards adopted by multiple standards bodies without changes). A specific example is IEEE Std. 1003.1-1990, which ISO later adopted as ISO/IEC 9945-1:1990, and NIST as FIPS PUB 151-2. The standards tables contain all the references to identical standards in separate rows using each of their different designations. If the specification is the same as, or derived from another standard, the relationship is indicated with comments to the effect in the same column. This approach toward matching standards has been chosen for informative reasons.

2.3.1.2.4 Standard reference. This column contains a formal citation for the standard or specification. The citation must include a version number and date, if necessary to unambiguously identify the specification.

2.3.1.2.5 DOD status (Life Cycle status). This column identifies the status of the specification, from concept to obsolescence. This column identifies both the DOD status and the ITSG life cycle status. The allowable values for each type of status reported are discussed in the sections that follow. All entries in the tables show the life cycle status in parenthesis. DOD status may or may not apply to the standard.

2.3.1.2.5.1 DOD status. This part of the DOD status (Life Cycle status) column refers to the approval for use of a standard in the DOD community according to the JTA or the TAFIM. DOD status terms include mandated, adopted, emerging, legacy, and informational. These terms are discussed in the following subparagraphs.

2.3.1.2.5.1.1 Mandated. The DOD status "Mandated" is used for those standards mandated by the JTA. A standard is mandatory in the sense that IF a service/interface is going to be implemented, it shall be implemented in accordance with the associated standard. If a required service can be obtained by implementing more than one standard, the appropriate standard should be selected based on system requirements. Mandated standards appear in the top rows of the standards tables in the ITSG and are bordered with heavy black lines.

2.3.1.2.5.1.2 Adopted. The DOD status "Adopted" is used to mean that the standard in the ITSG is approved by DOD for use in satisfying each function of the BSA where there exists no JTA mandated standard. Adopted standards may be implemented but shall not be used in lieu of a mandated standard. Adopted standards also appear in the top rows of the standards tables in the ITSG and are bordered with heavy black lines.

2.3.1.2.5.1.3 Emerging. According to the JTA, a DOD "Emerging" status denotes a candidate standard to be added as, or to replace, a mandated standard. This includes standards required to capitalize on new technologies. These candidates will help the program manager determine those areas that are likely to change in the near term (within three years) and suggest those areas in which "upgradability" should be a concern. The expectation is that emerging standards will be elevated to mandated status in the JTA when implementations of the standards mature. Emerging standards may be implemented but shall not be used in lieu of a mandated standard.

2.3.1.2.5.1.4 Legacy. A "Legacy" standard is a standard necessary to achieve or maintain interoperability with legacy systems. Legacy systems are systems that are in current use. Legacy standards are not recommended for future procurements. Legacy standards may be supported until the legacy system is no longer being maintained. An example of a legacy standard is the X.25 packet switching standards.

2.3.1.2.5.1.5 Informational. Informational standards include those remaining standards that fall outside the official DOD statuses of "mandated," "adopted," "emerging," and "legacy."

2.3.1.2.5.2 Life Cycle status. This part of the DOD status (Life Cycle status) column defines the life cycle status of the standard, as established by the originator of the standard.

2.3.1.2.5.2.1 Approved. The specification has been approved and published by its sponsoring body. This status is only meaningful for consensus-based specifications and standards.

2.3.1.2.5.2.2 Superseded. Superseded standards were formerly approved but have now been replaced, either by a later version of the standard or by the progress of technology. Superseded standards are not often desirable, but rank ahead of any non-approved standard. Superseded standards appear only at the bottom of the standards table.

2.3.1.2.5.2.3 Draft. The specification has been defined and is being reviewed. If this is a public, consensus standard, the specification should be available for comment. Draft standards are often subject to significant change before approval.

Further notes are appended to clarify the status of a draft, including the ISO stages of development (e.g., CD, WD, DIS) or if the standard is in ballot.

Draft standards appear only at the bottom of the standards table.

2.3.1.2.5.2.4 Formative. The specification is in the process of being defined. Generally, a committee has been formed to create the standard, but the specification has not stabilized. It is not available to the public. Formative standards appear only at the bottom of the standards table.

2.3.1.3 The top row. The top rows of the standards table contain the DOD mandated or adopted information technology standard satisfying that particular BSA. These standards are surrounded by a heavy black line and the standards are the same ones presented in the Adopted Information Technology Standards (TAFIM Volume 7).

The remaining five parts of the BSA description provide additional and necessary information about the target standard and the other standards listed in the table. The extensive information about the standards population within a specific BSA provides a full perspective of the activity in that area. The standards in the lower rows are provided in case an acquisition cannot use the standard specified in the top row. For example, they may be transitional systems in which a portion of a legacy system will remain unchanged temporarily.

If a standard listed in a lower row is specified in an acquisition, then the acquired system will diverge from the target DOD OSE. Standards listed in the lower rows of the tables diminish the probability of achieving portability and interoperability and may increase the ultimate life-cycle cost required to achieve an open system state.

If a system cannot use the standard specified in the top row, then it would be preferable to use a standard listed in a lower row, but within the standards table if possible. If a standard listed in a lower row is specified, there is risk. This risk is two-fold. If an emerging standard listed in a lower row is specified, the emerging standard may fail to arrive in the marketplace in the same form within a product. If the system implementation uses a declining standard of diminishing use and popularity, there is a risk that the products implementing the standard may be dropped by vendors as they move toward the standard listed in the top row. Projects using standards not consistent with the target standards identified in this document preclude the levels of portability and interoperability required to satisfy these stated DOD requirements. Also, the text accompanying the BSA contains further needed guidance for a solution.

The standards tables of some BSAs show what may be considered a paradoxical situation. There may be more than one "top row" standard. This occurs, for example, in the geospatial data area where different data sets are appropriate to different map scales. This situation shows that more than one standard may be preferred depending on specific architectural requirements. Often these multiple standards are complementary and all could be chosen to achieve the desired results.

2.3.1.4 The bottom area. The contents of every standards table in the ITSG will change as a reflection of industry dynamics as standards become formalized and are drafted, or become obsolete and superseded. The bottom area in the tables depicts this rise and fall of standards. The bottom area can contain standards with life-cycle statuses superseded, formative, and draft with DOD statuses emerging, legacy, or informational. The specification of standards within the bottom area involves risk. These standards are only an option in the case where no suitable NGS is listed in the upper rows. Populated bottom areas tend to show up in established BSAs containing many different standards.

2.3.1.5 Example table. All standards found in the remaining parts of the ITSG are combined under section 3.X.Y.Z.1 into a single table. Table 2.3-1 gives an example of a standards table using a BSA from the example of the ITSG structure in section 2.2. **Note that Table 2.3-1 and figures 2.3-1 through 2.3-5 are to be used as examples and *not* as the official findings of the BSA used in these examples.**

In the example of a standards table below, the top row, or DOD mandated standard, is NIST FIPS 127-2, specifying Database Language SQL. This version of the SQL standard uses ANSI X3.135-1992 and ISO 9075:1992. The mandated standard has precedence over all other entries in the table and should be used. The first entry in the bottom area of the example table is in draft (CD) life-cycle status and is DOD informational. Risk is less for this draft standard than for the DOD informational superseded standard appearing in the bottom area. The superseded life-cycle standard has been replaced and, therefore, involves much risk, if used. (In fact, it should not be used at all.) The last entry in the bottom area has a draft life-cycle status with DOD informational status. As is noted, it may eventually replace SQL2. This last standard will be moved out of the bottom area if and when it is approved by its sponsoring body. If JTA decides to add it to its emerging list, then the DOD status "emerging" will replace the "informational" DOD status. The standard would then appear above the bottom area as DOD emerging with life-cycle status of approved. [Note: Risk factors are usually different for each information system. It is the responsibility of the program manager to determine risk by performing a risk analysis. Risk determination is beyond the scope of the ITSG.]

TABLE 2.3-1 Example table of basic database services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DOD (Life Cycle)
GPC	NIST	Database Language SQL (Adopts ANSI X3.135-1992 and ISO 9075:1992)	FIPS 127-2:1993	Mandated (Approved)
IPC	ISO	Database Language SQL (same as ANSI X3.135-1992)	9075:1992	Informational (Approved)
NPC	ANSI	Database Language SQL (same as ISO/IEC 9075:1992)	X3.135:1992	Informational (Approved)
GPC	NIST	Guidelines for Functional Specifications for Database Management Systems	FIPS 124:1986	Informational (Approved)
CPC	X/Open	Embedded SQL (COBOL and C)	SQL Developers Specification	Informational (Approved)
IPC	ISO	Database Language - Network (NDL)	8907:1987	Informational (Approved)
GPC	NIST	Database Language - NDL (adopts ANSI X3.133-1986)	FIPS 126:1987	Informational (Approved)
NPC	ANSI	Database Language - (NDL)	X3.133:1986	Informational (Approved)
CPC	X/Open	Data Management: Reference Model	G505 (10/95)	Informational (Approved)
IPC	ISO/IEC	Database Language SQL3 (will replace SQL2)	9075	Informational (Draft (CD))
CPC	X/Open	Structured Query Language (SQL)	C201 (1992)	Informational (Superseded)
GPC	NIST	SQL3-Based FIPS	FIPS 127-3	Informational (Formative (FIPS Planned))
NPC	ANSI	Database Language SQL3 (will replace SQL2)	X3H2 Project 0029-R	Informational (Draft)

2.3.2 Paragraph two: Alternative specifications. The "Alternative specifications" section identifies other specifications that can satisfy the BSA. These will often be de facto specifications or vendor products that are de facto standards and other specifications not defined in formal standards groups. The DOD and ITSG's policy is generally NOT to recommend such specifications. The alternative specifications indicate the types of solutions likely to be offered if no other specifications exist.

FIGURE 2.3-1 Alternative specifications text example

The following alternative specifications are available:

a. For data definition, manipulation, query, data integrity, embedded SQL, and dynamic facilities standards: Integrated Database Application Programming Interface (IDAPI), a specification, published by Borland, IBM, Novell, and Word Perfect Corporation, will allow DOS, OS/2, and Windows applications to access a variety of SQL and non-SQL databases transparently.
b. No applicable consortia or de facto SQL integrity constraint specifications are available.
c. For X/Open SQL and the IBM Systems Application Architecture (SAA) SQL support Embedded C.
d. For dynamic facilities the only other available specifications are proprietary.

In the alternative specifications example, several alternatives are mentioned, but they are not appropriate considering the availability of SQL in FIPS 127-2

2.3.3 Paragraph three: Standards deficiencies. This section identifies deficiencies in the standards and recommends how to apply the standard to reduce their impact. "Standards deficiencies" addresses known problems within the standards such as missing features. In those cases where this section is absent, no deficiencies have been identified for inclusion, but does not suggest the standards have no deficiencies.

FIGURE 2.3-2 Standards deficiencies text example

The following deficiencies in the standards have been identified:

a. For data definition, manipulation, query, data integrity, embedded SQL, and dynamic facilities standards:
   (1) No standardized way exists to specify logical database access control, which is important to database security.
   (2) Hashing methods to access data are neither standardized nor in progress.
   (3) SQL1 is inadequate and has failed to be transportable or standardized to be very useful. The upcoming SQL-3 provides an opportunity for DOD requirements to be inserted.
b. For data integrity standards, SQL Integrity Enhancement is a simple capability with no constructs to help programmers maintain data consistency.
c. For Embedded SQL standards, SQL2 supports Embedded SQL in C and Ada. However, products will not be available for some time. International Organization for Standardization (ISO)/American National Standards Institute (ANSI) Embedded SQL does not support the

FIGURE 2.3-2 Standards deficiencies text example (cont'd.)

C programming language. The use of embedded SQL requires a precompiler for each language in which SQL is embedded.

d. For dynamic facilities standards, deficiencies in the existing formal standards are unknown.

e. For SQL environments, the emphasis in this first FIPS for SQL Environments is on profiles for limited SQL interfaces to non-SQL data repositories. Subsequent versions of this FIPS may specify more complete profiles for other products in an SQL environment. The profiles defined by this standard are not complete in and of themselves. The user is required to add information before this standard can be successfully used in a procurement.

In the standards deficiencies example above, several problems with the existing standards have been identified. In this example, no deficiencies in FIPS PUB 127-2 have been identified.

2.3.4 Paragraph four: Portability caveats. "Portability caveats" addresses the features of the standard hindering portability. In those cases where this section is absent, no portability problems have been identified, but the absence of portability caveats does not suggest the standards have no portability problems.

The portability caveats example points out particular problems of the SQL standards: implementation-defined exception code values and the character data type. Additional portability problems arise between the NIST FIPS for SQL and the other versions of the standard as shown in the text. (See Figure 2.3-3).

FIGURE 2.3-3 Portability caveats text example

The following portability caveats apply:

a. For data definition, manipulation, query, data integrity, embedded SQL, and dynamic facilities standards,
   (1) SQL 2's segmentation into multiple levels increases the likelihood of incompatibility between different vendors' SQLs, because different vendors will implement entry level SQL 2, then choose options from other levels.
   (2) The ISO, ANSI, and Federal Information Processing Standard (FIPS) versions of SQL specify state exception code values (called SQLCODE parameters) such as 0 for successful execution, 100 for nonexistent data, and implementation defined code values for particular exception conditions. Different products that conform with SQL have different SQLCODE values for exception conditions. The set of SQL character values for the character data type and collating sequence of characters is defined by the implementor, the implementor, and therefore, nonstandard in products.

b. For data integrity the following portability caveats apply:
   (1) Most vendors' products contain extensions. To maximize portability, reduce the use of extensions as much as possible.
   (2) Different vendors provide locking to different degrees of granularity. Portability and/or interoperability of applications result in locking to the largest degree of granularity.

FIGURE 2.3-3. Portability caveats text example (cont'd.)

c. For dynamic facilities the following portability caveat applies: Although the X/Open and SAA SQLs support dynamic SQL, X/Open SQL is an X/Open-enhanced specification of the 1986 version of Level 1 SQL, while SAA SQL is not fully ISO/ANSI SQL compatible, although it will be. Also, X/Open and SAA dynamic SQL facilities are not fully compatible with each other.

d. For SQL environments, conformance testing for products claiming conformance to one of the profiles specified by FIPS 193 will be achieved by a suitable modification of the existing NIST SQL test suite. This FIPS requires the customer to choose from among the different binding styles already defined by the SQL standards. Two of these styles (CLI and RDA) are expected to be more popular than the others. If a programming language binding style is chosen, then FIPS SQL specifies the parameter passing requirements for each of seven different programming languages.

2.3.5 Paragraph five: Related standards. The related standards section addresses the standards required as a foundation for a particular standard, or other standards relating to the functionality under discussion, or other interfacing standards. A prime example of this would be IEEE Std. 1003.1-1990 as a related standard for using IEEE P1003.1b, which is the real time extension to the 1003.1 standard.

In the related standards example, standards usable to extend SQL functionality have been identified. These standards include Remote Database Access (RDA), and all may be found in the standard tables of other BSAs in section 3.4. (See Figure 2.3-4).

FIGURE 2.3-4 Related standards text example

The following standards are related to basic database services or basic database service standards:

(1) ISO 9579-1: Remote Database Access (RDA) (Generic Model, Service and Protocol) (supports remote database access in client-server environments)
(2) ISO 9579-2: RDA: (SQL Specialization)
(3) SQL Access Group's (SAG's) SQL Access Formats and Protocols (FAP) (1991)
(4) SAG's Call Level Interface (CLI)
(5) X/Open RDA Preliminary Specification (Identical to the SAG's RDA Specification
(6) X/Open's CLI Snapshot Specification (Identical to the SAG's CLI Specification)
(7) Open Systems Interconnection (OSI) CCR (Commitment, Concurrency, and Recovery): ISO/International Electrotechnical Commission (IEC) 9804-3/9805-3
(8) OSI Distributed Transaction Processing (DTP) Protocol: ISO/IEC 10026 Parts 1, 2, and 3.
(9) ISO 1989:1985: COBOL
(10) ANSI X3.9-1978: FORTRAN-77
(11) ANSI X3.159-1989: C
(12) National Institute for Standards and Technology (NIST) FIPS 021-3: COBOL
(13) NIST FIPS 069-1: FORTRAN
(14) NIST FIPS 119, DOD MIL-STD 1815A:1983, ISO 8652: Ada

FIGURE 2.3-4 Related standards text example (cont'd.)

(15) NIST FIPS 160: C
(16) ISO/IEC Draft International Standard (DIS) 10032: Reference Model of Data Management
(17) ISO 12227 SQL/Ada Models Description Language, 1994
(18) X3 SQLIB-1 SQL Information Bulletin Number 1 Interpretation of ANSI X.3.135 - 1989

2.3.6 Paragraph six: Recommendations. "Recommendations" advises which standard is preferred for specification in the procurement for the particular area of functionality and standards. The recommendation will provide suggested wording to use in the procurement when possible. Additional guidance about selection of options and features of a standard is also included as potential solutions to the portability problems identified above.

In these example recommendations, the most current SQL and supporting standards are recommended with details about optional conformance levels and testing. (See Figure 2.3-5).

FIGURE 2.3-5 Recommendations text example

a. The following are related to data definition, manipulation, query, data integrity, embedded SQL, and dynamic facilities standards:
   (1) Consult the wording suggested in the October 1991 General Services Agency (GSA) publication for proposed language for requiring that a database conform to SQL, and consult FIPS 127-2 for guidance on how to structure a Request for Proposal (RFP). The FIPS "flagger" (to flag nonconforming extensions) is optional and must be specified explicitly.
   (2) If interactive SQL is required, a procurement must indicate explicitly whether or not "direct invocation of SQL statements" is required and, if required, which SQL statements are to be directly invocable. If not specified, the default is "CREATE TABLE," "CREATE VIEW," "GRANT privilege," "SELECT" with "ORDER BY" option, "INSERT," "UPDATE:searched," "DELETE:searched," "COMMIT WORK," and "ROLLBACK WORK."
   (3) Explicitly specify sizing constraints for database constructs. The FIPS 127-2 sizing specifications are reasonable to expect vendors to deliver, but are fairly minimal. Since database construct sizing specifications depend on the procurement, a procurement can override them.
   (4) Require the use of NIST conformance tests and/or services to validate conformance to the SQL-based FIPS for required and optional FIPS 127-2 features. Testing applies only to a specific platform, so call for conformance tests for each platform bid. Use the quarterly list of processors validated against FIPS 127-2 by NIST to help evaluate bids.
   (5) Specify the NIST's Transition Level SQL 2 and the SAG's CLI and RDA interfaces and protocols for the following reasons. Most DBMS vendors have no intention of conforming to the Full Level SQL 2:1992 because it is very large and complex. As a result, the time it will take to add the necessary features will probably exceed the time before the SQL 3

FIGURE 2.3-5 Recommendations text example

standard is completed. To ensure portability as well as functionality, users are encouraged to include the following two specifications in their procurement:

(a) NIST's Transition Level SQL 2 (specified in FIPS 127-2), which is a hybrid of Entry Level and higher levels of SQL 2:1992.

(b) SAG's and X/Open's CLI and RDA standards. The SAG specifications are not segmented like SQL '92 and offer a nice balance between the Full Level SQL '92 feature set and what users need now. The SAG specifications include connection management capabilities (which are part of the SQL '93 Full Level), schema manipulation and the CHARACTER VARYING data type (both of which are part of SQL '93 Intermediate Level), and features not included in any level of SQL '92 conformance, including the CREATE INDEX and DROP INDEX statements. SAG's specifications are published jointly with X/Open as X/Open specifications.

(6) Specify SQL2 (and later SQL3) as soon as possible because SQL2/3 contains greater standardized functionality than SQL1. This will reduce the use of nonstandard extensions. SQL2 also standardizes more than 60 SQLCODE exception code values.

(7) Carefully specify and check all sizing constraints for a procurement to meet functionality requirements and avoid portability problems.

(8) Avoid the Network Data Language (NDL), if possible, because it is little used and will not be upgraded.

(9) Specify the ISO RDA standard, and also the X/Open or SAG's RDA and CLI specifications in conjunction with SQL/SQL2 to obtain remote data access capabilities in a distributed environment.

b. The Integrity Constraint feature is optional in SQL and must be specified explicitly for a procurement. Failure to do so means the Integrity Constraint feature is not required. Specify FIPS 127-2, especially if any of the services unique to FIPS 127-2 are needed.
In SQL2, the integrity enhancement feature is mandatory, not optional. Also, SQL2 has better integrity constraints, such as "cascade delete on referential integrity" (in the intermediate SQL Level) and "deferrable integrity constraints" (in full SQL2).

c. For embedded SQL:

(1) Specify embedded SQL in an RFP, although it is optional in the standard. Indicate which programming language is to be supported in references to embedded SQL in a procurement. Failure to do so means that support for any one FIPS language satisfies the FIPS SQL requirement. Indicate whether the language interface is to support the Module Language interface style, the embedded language interface style, or both. Failure to do so means that vendors supporting any one interface style satisfy the FIPS SQL requirement.

(2) Require the use of NIST conformance tests and/or services to validate conformance to every one of the embedded interfaces and module interfaces, and to validate the compilers that will be used with the embedded SQL because SQL testing is independent of the host programming language testing. Testing applies only to a specific platform, so call for conformance tests for each platform bid. Specify FIPS 127-2 if any of the services unique to FIPS 127-2 are needed. Specify that the character data values and collating sequences coincide with the character values and collating sequence of the specific programming languages to be used. Failure to indicate specific character set requirements means that support for representation of the 95-character graphic subset of American Standard Code

FIGURE 2.3-5 Recommendations text example

for Information Interchange (ASCII) (FIPS 1-2) in an implementor specified collating sequence defaults to the minimum requirement, and may not be portable across other procured systems.

d. For dynamic facilities, SQL2 is preferred. Dynamic SQL is an intermediate level SQL2 capability. Either SQL2's dynamic SQL facilities or the SQL2 intermediate level must be specified explicitly in a procurement.

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

2.4. Applicable Documents

2.4.1 Government documents.

2.4.1.1 Specifications, standards, and handbooks. The following specifications, standards, and handbooks form a part of this document to the extent specified. Unless otherwise specified, the issues of these documents are those listed in the issue of the DODISS and its supplement. Other specifications, standards, and handbooks referred to in the text of this document are also included to the extent specified.

DOD Directive 5000.1, Defense Acquisition, 15 March 1996.

DOD Regulation 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs.

DODD 4120.3-M, Defense Standardization Program, 7 July 1993.

2.4.1.2 Other government documents, drawings, and publications. The following other government documents, drawings, and publications form a part of this document to the extent specified herein. Other government documents, drawings, and publications referred to in the text of this standard are also included to the extent that this document specifies.

NIST Special Report 500-230, Application Portability Profile (APP): The U.S. Government's Open System Environment Profile, version 3.0, December 1995.

Technical Architecture Framework for Information Management (TAFIM), version 3.0, April 30, 1996.

DOD, A Framework for Evolution of the Department of Defense Intelligence Information System (DODIIS), July 1991.

Technical Standards for Command and Control Information Systems (CCISs) and Information Technology" by the Army Tactical Command and Control Information System Permanent Working Group, SHAPE, Belgium, Edition 4, 25 February 1994.

Office of Management and Budget (OMB), Federal Participation in the Development and Use of Voluntary Standards, Circular A-119, Revised October 20, 1993.

2.4.2 Non-government publications. The following documents form a part of this document to the extent specified herein. Unless otherwise specified, the issues of the documents adopted by the DOD are listed in the latest issue of the DODISS. Unless otherwise specified, the issues of documents not listed in the DODISS are the issues of the documents cited herein.

IEEE Std 1003.0-1995, Guide to the POSIX Open System Environment (OSE), May 1995.

2.4.3 Standards availability. Unless otherwise indicated, copies of federal and military specifications, standards, and handbooks are available to DOD activities and their contractors from the Commanding Officer, Naval Publications and Forms Center, (ATTN: NPODS), 5801 Tabor Avenue, Philadelphia, PA, 19120-5099. Others must request copies of FIPS from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA, 22161-2171. Non-government standards and other publications are normally available from the organizations that prepare or distribute the documents (see section 2.3). These documents also may be available in or through libraries or other informational services.

2.4.3.1 International Organization for Standardization (ISO) standards. In the United States, ISO standards can be obtained from the American National Standards Institute (ANSI, see below), which is the official United States representative to ISO. ISO standards are also available directly from the ISO office:

1 Rue de Varembe
Case Postale 56
CH-1211, Geneve 20 Switzerland/Suisse

http://www.iso.ch/

2.4.3.2 ANSI standards. ANSI standards are available from the American National Standards Institute at:

11 West 42nd Street
New York, NY 10036

(212) 642-4900 (telephone)
(212) 398-0023 (fax)
(212) 302-1246 (sales fax)

http://www.ansi.org/

2.4.3.3 Institute of Electrical and Electronics Engineers (IEEE) standards. IEEE standards are available from the IEEE Standards Board:

445 Hoes Lane
Piscataway, NJ 08855-1331

http://www.ieee.org/

2.4.3.4 Government standards. MIL standards are available from local publications offices. National Institute of Standards and Technology (NIST) publications are sold by the Government

Printing Office (GPO) and by the National Technical Information Service (NTIS). Order numbers for National Bureau of Standards (NBS)/NIST series numbers, technical notes, or special publications may be obtained from NIST Publications and Program Inquiries at:

E128 Admin
NIST
Gaithersburg, MD 20899
(301) 975-3058

http://www.nist.gov/

Documents then may be ordered by order number from the GPO at:

Superintendent of Documents
U.S. Government Printing Office
Washington, D.C. 20402
(202) 783-3238

Federal Information Processing Standards, NBS/NIST Interagency Reports, and Grant/Contract Reports are available only from:

National Technical Information Service (NTIS)
5285 Port Royal Road
Springfield, VA 22161
(703) 487-4650 information
(800) 336-4700 orders

2.4.3.5 International Telecommunication Union (ITU) Telecommunications Standardization Sector (TSS) standards. Formerly the International Telegraph and Telephone Consultative Committee (CCITT), ITU-TSS documents can be obtained from:

ITU-TSS General Secretariat
International Telecommunications Union
Sales Section
Place des Nations, Ch-1211
Geneve 20, Switzerland/Suisse

41 22 730 5111 (telephone)
41 22 733 7256 (fax)
http://www.itu.ch/

2.4.4 Order of precedence. In general, order of precedence for DOD applications is JTA Mandated followed by JTA Adopted standards. Nothing in this document supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.5. Information Technology Standards Guidance Reference Model

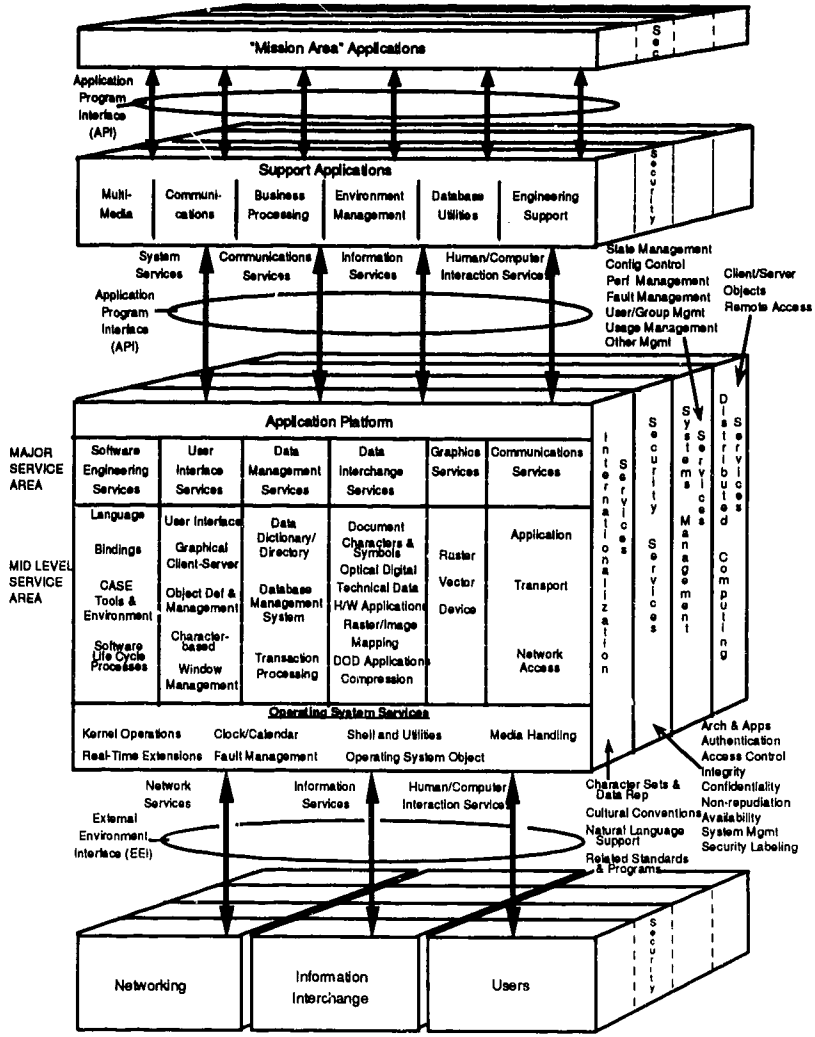
2.5.1 Reference Model.

2.5.1.1 Introduction. This section of Part 1 of the ITSG describes a high-level model for the ITSG that will reduce duplication and assist in coordination. It includes discussion of the overall organization of the ITSG as well as the organization of information internal to a base service area (BSA).

2.5.1.2 Problem. As the Adopted Information Technology Standards (AITS) and ITSG expand beyond the limited areas covered by the original National Institute of Standards and Technology (NIST) Application Portability Profile (APP) and Technical Architecture Framework for Information Management (TAFIM), a growing number of BSA's appear not to fit into a specific area. For example, is Distributed Database a Data Management or Distributed Computing service area? Is Raster Graphics a Data Interchange or Graphics service area? These situations can lead to duplication and the potential for inconsistent guidance. The proliferation of additional overlapping service areas, such as multimedia, visual information, modeling and simulation, or document management will expand the problem. Defense Information Systems Agency (DISA) subject matter experts (SMEs) are responsible for coordinating their recommendations with other related SMEs, but they have a difficult time knowing where coordination is required without global knowledge of all areas. This ITSG model will help reduce duplication and eliminate inconsistency, with little disruption to the existing ITSG and AITS documents.

2.5.1.3 Current ITSG Model. Historically the ITSG has used the Department of Defense (DOD) Technical Reference Model (TRM) shown in Figure 2.5-1 as the base model. The ITSG uses the TRM platform service areas as Major Service Areas, each of which is divided into several Mid-Level Service Areas and ultimately into many BSAs. These service areas are used to classify standards for application programming interfaces (APIs) and external environment interfaces (EEIs). The ITSG also includes standards that do not match either of these definitions (e.g., procedural standards). Several organizations have extended the DOD TRM to handle standards such as hardware and media that are not represented well in the current TRM. Discussions are continuing on how to represent the "horizontal" cross-area services such as security and distributed computing. Additional ITSG volumes have been proposed for areas such as data compression. Before defining additional volumes, the underlying model should be reconsidered to ensure that the ITSG volumes will provide understandable consistent guidance.

FIGURE 2.5-1 DoD Technical Reference Model



2.5.1.4 ITSG Model. The ITSG model is discussed at two levels: global and local. The global level discusses the parts of the ITSG, while the local level discusses the organization internal to a base service area. At the global level, two types of volumes exist, as illustrated by Table 2.5-1, which is described below. The ITSG has seven major service area volumes, one for each of the TRM major service areas, as shown by the vertical boxes at the top of Table 2.5-1. These service areas closely correspond to the service areas from the NIST APP and the Institute of Electrical and Electronics Engineers (IEEE) POSIX.0 open systems reference model, as shown in Table 2.5-2 which describes the major service areas. All other volumes represent cross-area services and are composed of BSAs copied from the major service area volumes. These are illustrated by horizontal boxes in Table 2.5-1. Within Table 2.5-1, the entries BSAxx represent BSAs to show their usage across volumes. Table 2.5-1 is for illustrative purposes only and does not map to any particular BSA.

TABLE 2.5-1 Sample Global view of ITSG Model

Major Service Areas		Part 2: Software Engineering Services	Part 3: User Interface Services	Part 4: Data Management Services	Part 5: Data Interchange Services	Part 6: Graphics Services	Part 7: Communication Services	Part 8: Operating System Services
Foundation BSAs		BSA21 BSA22 BSA31' BSA51'	BSA31 BSA32 BSA33 BSA34	BSA41 BSA42 BSA43	BSA61' BSA51 BSA52	BSA61 BSA62 BSA63	BSA71 BSA72 BSA73 BSA74	BSA81 BSA82 BSA83 BSA84
Cross-area Services	Part 9: System Management	BSA21'	BSA31'	BSA41'		BSA61'	BSA72'	BSA82'
	Part 10: Security		BSA32'	BSA43'			BSA73'	BSA83'
	Part 11: Distributed Computing		BSA33'	BSA42'	BSA51' BSA52'		BSA71' BSA72' BSA73'	BSA82' BSA84'
	Part 12: Multimedia	BSA21'	BSA31' BSA32' BSA33' BSA34'		BSA42' BSA51'	BSA61' BSA62' BSA63'	BSA72' BSA73'	BSA81' BSA82'
	Part 13: Human Factors	BSA21'	BSA31' BSA32'		BSA51'			

Notes: 1. BSAs marked with a prime (') are a "clone" of a foundation BSA.
2. Not a comprehensive list of cross-area services.

Notes:
1. BSAs marked with a prime (') are a "clone" of a foundation BSA.
2. Not a comprehensive list of cross-area services.

2.5.1.4.1 Foundation BSA. Each BSA will be uniquely "grounded" in one ITSG major service area. This BSA is referred to as the "foundation BSA." The foundation BSA may be "cloned" in other volumes in a controlled manner, but the discussion and recommendations must be the same in each area. A clone will consist of a textual copy of the foundation BSA material to make the ITSG volumes easier to use. The configuration management procedures will ensure that the

copies remain consistent. The SME for the foundation BSA is responsible for coordination with the SME for each area in which the BSA is used. A BSA may be cloned in another major service area volume if a BSA is appropriate in multiple areas. The Raster Graphics BSA mentioned earlier (illustrated by BSA51) and language bindings (illustrated by BSA31 and BSA51) are examples of areas in which this is desirable. The major service areas are defined below to minimize this duplication.

2.5.1.4.2 Spanning Service Areas. Spanning service area volumes are constructed for any subject domain that crosses major service areas. The classic examples are system management and security services, but numerous others have been proposed. Spanning service areas are composed entirely of cloned BSAs, as illustrated in Table 2.5-1. If the spanning service area requires a BSA that is not in a major service area volume, then the BSA must be added to an appropriate major service area. The spanning area volume can include introductory material that is specific to the area. All BSAs that relate to the cross-area subject are copied into the volume. For example in Table 2.5-1, BSA32, BSA43, BSA73, and BSA83 relate to security. The clone BSA will contain the same recommendation as the foundation BSA. The spanning service area SME is responsible for coordinating with the foundation BSA's SME for each BSA; the foundation SME is responsible for coordinating with all other SMEs using the foundation BSA. The configuration management process, discussed in a separate document, will be used to resolve any conflicts.

2.5.2 ITSG Major Service Areas. The major service areas, defined to reduce overlap, are listed below.

2.5.2.1 Software Engineering Services. Services that provide the infrastructure used to develop and maintain software, including general purpose computer languages. Does not include languages specific to another service area, such as user interface definition languages or data retrieval languages (e.g., SQL). Does not include language bindings, which are included with the service being supplied by the binding; however, these may be cloned here.

2.5.2.2 User Interface Services. Defines methods by which humans interact with applications, regardless of media (e.g., audio, video). Excludes media-independent formats for the exchange of multimedia objects (e.g., graphics file formats), which are included under Data Interchange, but may be cloned here.

2.5.2.3 Data Management Services. Services related to the management of data independent of a specific application, including data creation, storage, sharing, retrieval, and manipulation, in a single-host or distributed environment. Includes languages and protocols for the manipulation of multi-media objects, as well as all formats and protocols required to extend these services into a distributed environment, and relevant management and security services.

2.5.2.4 Data Interchange Services. Services related to the exchange of information, including the format and semantics of exchange between applications on the same or different platforms. Includes formats for the storage and exchange of multimedia objects, which may be cloned under User Interface or Graphics Services. Does not include communications protocols at OSI layer 6 and below.

2.5.2.5 Graphics Services. Services related to the creation and manipulation of displayed images. Excludes media-independent formats for the exchange of multimedia objects (e.g., graphics file formats), which are included under Data Interchange, but may be cloned here.

2.5.2.6 Communications and Network Services. Services required for data transport without regard for the type of information. Basically includes the services and protocols for OSI layers 6 and below, plus foundation layer 7 services (directory services, mail, file transfer, remote login). All other application layer services and protocols will be included elsewhere. Includes security services related to these base services.

2.5.2.7 Operating System Services. Core services needed to operate and administer the application platform and provide an interface between the applications and the hardware platform. Services related to process management, tasking, memory allocation, and basic file handling. It also includes system-wide management services, such as accounting and user/group management that do not fit under any other service areas. It includes all formats and protocols required to extend these core services into a distributed environment, as well as relevant security services.

Table 2.5-2 relates the ITSG major service areas to service areas defined in the NIST Application Portability Profile and the IEEE Open Systems Reference Model (POSIX.0).

TABLE 2.5-2 ITSG Major Service Areas Related to NIST APP and IEEE OSE/RM

ITSG Major Service Area	NIST APP Service Area	IEEE POSIX OSE Reference Model Service Area
Software Engineering Services	Software Engineering Services	System Services
Operating System Services	Operating System Services	
User Interface Services	Human/Computer Interface Services	Human/Computer Interaction Services
Graphics Services	Graphics Services	
Data Management Services	Data Management Services	Information Services
Data Interchange Services	Data Interchange Services	
Communications and Network Services	Network Services	Communications and Network Services

2.5.3 Proposed Rules. The following rules are proposed for the ITSG reference mode:

(1) The ITSG has two types of volumes. There are seven major service area volumes, and additional (six in version 3.1) spanning service area volumes.

(2) The ITSG Major Service Areas are Software Engineering Services, User Interface Services, Data Management Services, Data Interchange Services, Graphics Services, Communications and Network Services, and Operating System Services.

(3) Each BSA will be uniquely "grounded" in one ITSG major service area. The BSA will be grounded in a "foundation BSA." The BSA may be "cloned" by reference or by copying the text, although the latter is preferred.

(4) Cloned BSAs may appear in more than one major service area volume.

(5) Spanning service area volumes are composed entirely of cloned BSAs. If the spanning service area requires a BSA that is not in a major service area volume, then the BSA must be added to an appropriate major service area. The six spanning service areas, as of version 3.1) are System Management, Security, Distributed Computing, Multimedia, Human Factors, and Internationalization.

(6) The cloned BSA will contain the same recommendation as the foundation BSA.

(7) The SME for the foundation BSA is responsible for coordination with the SME for each area in which the BSA is used.

(8) The cross-area volume SME is responsible for coordinating with the foundation BSA SME for each BSA.

(9) The configuration management process will be used to resolve any conflicts.

2.6 Definitions.

2.6.1 Acronyms used in the ITSG. The acronyms used in the ITSG are defined as follows:

AAP	Association of American Publishers
ACGIH	American Conference of Government Industrial Hygienists
ACL	Access Control List
ACM	Association for Computing Machinery
ACP	Allied Communication Publication
ACP	Association Control Protocol
ACSE	Association Control Service Element
ACVC	Ada Compiler Validation Capability
AD	Addendum (ISO)
AdaIC	Ada Information Clearinghouse
ADMAPS	Automated Document Management and Publishing System
ADP	Automated Data Processing
ADS	Automated Data Systems
ADSIA	Allied Data Systems Interoperability Agency (NATO)
AECMA	Association European des Constructeurs de Material Aerospatial
AEP	Application Environment Profile
AES	Application Environment Specification
AFCEA	Armed Forces Communications and Electronics Association
AFS	Andrew File System (CMU)
AIAA	American Institute of Aeronautics and Astronautics
AIE	Ada Integrated Environment (USAF)
AIS	Automated Information Systems
AIIM	Association for Information and Image Management
AIM	Automatic Identification Manufacturers
AITS	Adopted Information Technology Standards
AJPO	Ada Joint Program Office (DOD)
ALE	Automatic Link Establishment
ALS	Ada Language System (U.S. Army)
AM	Amendment (ISO)
ANS	American Nuclear Society
ANSI	American National Standards Institute
API	Application Program Interface
APP	Application Portability Profile (NIST)
APSE	Ada Programming Support Environment
ARIDPCM	Adaptive Recursive Interpolative Differential Pulse Code Modulation
ARCAS	Army Reserve Component Automation System
ASC	Accredited Standards Committee (ANSI)
ASCII	American National Code for Information Interchange
ASIS	Ada Semantic Interface Specification
ASME	American Society of Mechanical Engineers
ASN	Abstract Syntax Notation

ASR	Ada Software Repository
ASTM	American Society for Testing and Materials
ATA	Air Transport Association of America
ATCCIS	Army Tactical Command and Control Information System
ATIS	A Tool Integration Standard
ATM	Automated Teller Machine
ATMI	Application to Transaction Manager Interface
AV-I	Audio Video - Interleave
BDF	Bitmap Distribution Format
BER	Basic Encoding Rules (ASN)
BMP	Windows Bitmap Format (Microsoft)
BOM	Bit-Oriented Messages
BSA	Base Service Area
BSD	Berkeley Software Distribution
BSFT	Byte Stream File Transfer
BSI	British Standards Institute (UK)
CAD	Computer-Aided Design
CAE	Common Application Environment
CAIS	Common Ada Programming Support Environment (APSE) Interface Set
CALS	Computer-Aided Acquisition and Logistic Support
CAM	Computer-Aided Manufacturing
CASE	Computer Aided Software Engineering
CBEMA	Computer and Business Equipment Manufacturers Association
C3I	Command, Control, Communications, and Intelligence
CCD	Charge Coupled Devices
CCIS	Command and Control Information System
CCITT	Comite Consultatif International de Telegraphique et Telephonique (International Telegraph and Telephone Consultative Committee) (now called the ITU-TSS)
CCR	Commitment, Concurrency, and Recovery
CCS	Continuous Composite Servo
CCTA	Central Computer and Telecommunication Agency (UK)
CD	Committee Draft (ISO)
CD	Compact Disc
CD-I	Compact Disc - Interactive
CD-R	Compact Disc - Recordable
CD-ROM	Compact Disc - Read Only Memory
CD-V	Compact Disc - Video
CD-WO	Compact Disc - Write Once
CD-XA	Compact Disc - Extended Architecture
CDIF	CASE Data Interchange Format
CECOM	Communications-Electronics Command (U.S. Army)
CEDD	Committee for the Exchange of Digital Data (IHO)
CFS	Center for Standards (DISA/JIEO)

CGI	Computer Graphics Interface
CGM	Computer Graphics Metafile
CIA	Central Intelligence Agency
CID	Commercial Item Description
CIE	Comite International de l'Eclairage (International Commission on Illumination)
CIM	Center for Information Management (DISA)
CINC	Commander in Chief
CIS	CASE Integration Services
CJCS	Chairman of the Joint Chiefs of Staff
CLNS	Common LISP Object System
CM	Communication Manager
CMA	Consolidated Management Architecture
CM-API	Consolidated Management API
CMIP	Common Management Information Protocol
CMIS	Common Management Information Services
CMOT	CMIP Over TCP/IP
CMU	Carnegie Mellon University
CMW	Compartmented Mode Workstation
CMYK	Cyan, Magenta, Yellow, and Black
COE	Common Operating Environment
COEWG	Common Operating Environment Working Group
COMPUSEC	Computer Security
CONS	Connection Oriented Network Service
CORBA	Common Object Management Request Broker Architecture
COTS	Commercial Off-the-Shelf
CPC	Consortia Public Consensus
CPC	Cross-Platform Communications (IMA)
CPSC	Consumer Product Safety Commission
CRSS	C3I Reusable Software System
csh	C Shell
CTE	Compound Text Encoding
CUA	Common User Access
DAC	Discretionary Access Controls
DAD	Draft Addendum (ISO)
DAM	Draft Amendment (ISO)
DAP	Document Application Profile
DARPA	Defense Advanced Research Program Agency
DBF	Discrete Block Format
DBMS	Database Management System
DBSSF	Database System Study Group
DCA	Document Content Architecture
DCE	Distributed Computing Environment
DCPS	Data Communications Protocol Standards
DCW	Digital Chart of the World (DMA)

DDE	Dynamic Data Exchange
DDES	Digital Data Exchange Specification
DDF	Data Descriptive File (for Information Interchange)
DDRS	Data Dictionary/Repository System
DEA	Data Encryption Algorithm
DEC	Digital Equipment Corporation
DER	Distinguished Encoding Rules (BER/ASN)
DES	Data Encryption Standard
DFR	Document File and Retrieval
DFS	Distributed File System
DGIWG	Digital Geographic Information Working Group
DIA	Defense Intelligence Agency
DIA	Display Industry Association
DIA	Document Interchange Architecture
DIB	Directory Information Base
DID	Data Item Description
DIF	Data Interchange Format
DIGEST	Digital Geographic Information Exchange Standard
DIS	Draft International Standard (ISO)
DISA	Defense Information Systems Agency (DOD)
DFR	Document Filing and Retrieval
DFS	Distributed File System
DMA	Defense Mapping Agency (DOD)
DME	Distributed Management Environment
DMI	Definition of Management Information
DNI	Detailed Network Interface
DNS	Domain Naming Service
DOAM	Distributed Office Applications Model
DOD	Department of Defense
DODIIS	DOD Intelligence Information System
DODISS	DOD Index of Specifications and Standards
DOS	Disk Operating System
DOT	Department of Transportation
DP	Draft Proposed Standard (ANSI, ISO)
DPA	Document Printing Application
DPS	Digital Production System (DMA)
DSRS	Defense Software Repository System
DSS	Digital Signature Standard
DSSC	Distributed Systems Steering Committee (IEEE)
DSSSL	Document Style Segmentation and Specification Language
DTAM	Document Transfer and Manipulation
DTMP	DCPS Technical Management Panel
DTP	Distributed Transaction Processing
DVI	Digital Video Interactive
DWM	Desqview Window Manager

DXF	Drawing Exchange Format (Autodesk)
EAN	International Article Numbering Association
ECMA	European Computer Manufacturers' Association
EDI	Electronic Document Interchange
EDIF	Electronic Data Interchange Format
EDIFACT	EDI for Administration, Commerce, and Transport
EEC	European Economic Community
EEI	External Environment Interface
EIA	Electronic Industries Association
EMPM	Electronic Manuscript Preparation and Markup
EPA	Environmental Protection Agency
EPHOS	European Procurement Handbook for Open Systems
ES-IS	End System to Intermediate System
EWOS	European Workshop for Open Systems
FAA	Federal Aviation Administration
FAP	Formats and Protocols (SQL)
FDDI	Fiber Distributed Data Interface
4GL	Fourth Generation Language
FIMS	Form Interface Management System
FIPS	Federal Information Processing Standard (NIST)
FIPS PUB	Federal Information Processing Standard Publication
FM	Field Manual
FTAM	File Transfer, Access, and Management
FTP	File Transfer Protocol (Internet)
FY	Fiscal Year
GDMO	Guidelines for the Definition of Managed Objects
GDSII	Graphic Design System II
GIF	Graphics Interchange Format
GIS	Geographic Information System
GKS	Graphical Kernel System
GKS-3D	Graphical Kernel System for Three Dimensions
GMI	Generic Management Information
GNMP	Government Network Management Profile
GOSIP	Government Open Systems Interconnection Profile
GOTS	Government Off-the-Shelf
GPC	Government Public Consensus
GPC	Graphics Performance Characterization Committee
GPEF	Generic Package of Elementary Functions
GPO	Government Printing Office
GPPF	Generic Package of Primitive Functions
GRACE	Generic Reusable Ada Components for Engineering
GUI	Graphical User Interface

GULS	Generic Upper Layer Security
HCI	Human-Computer Interface
HDL	Hardware Description Language
HDLC	High-Level Data Link Control
HDTV	High Definition Television
HF	High Frequency
HFS	Human Factors Society
HLHSR	Hidden Line/Hidden Surface Removal
HOL	High Order Language
HP	Hewlett Packard
HPDL	Hewlett-Packard Page Description Language
HYTIME	Hypermedia/Time-based Structuring Language
IAB	Internet Architecture Board
IBM	International Business Machines Corporation
ICAM	Integrated Computer-Aided Manufacturing
ICASE	Integrated Computer-Aided Software Engineering
ICC	International Color Consortium
ICCCM	Interclient Communications Conventions Manual
ICCD	Integrated Charge Coupled Devices
ICR	Intelligent Character Recognition
IDEF	Integrated Definition
IDEF	ICAM Definition Language
IDHS	Intelligence Data Handling System
IDL	Interface Definition Language
IDT	Interactive Design Tools
IDTIF	Interactive Design Tool Interchange Format
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
I4DL	Interface, Inheritance, Implementation, and Instantiation Definition Language
IFF	Interchange File Format
IGES	Initial Graphics Exchange Specification
IHO	International Hydrographic Organization
IM	Information Management
IMA	Interactive Multimedia Association
IMA	International MIDI Association
I/O	Input/Output
IOH	Integrated Open Hypermedia
IP	Information Processing
IPC	International Public Consensus
IPC	Interprocess Communications
IPO	IGES/PDES Organization
IPSC	Information Processing Standards for Computers

IR	Interim Report
IRDS	Information Resource Dictionary System
IS	International Standard (ISO)
ISAM	Indexed Sequential Access Method
ISDN	Integrated Services Digital Network
ISEE	Integrated Software Engineering Environment
IS-IS	Intermediate System to Intermediate System
ISO	International Organization for Standardization
IT	Information Technology
ITPB	Information Technology Policy Board (DOD)
ITSEC	Information Technology Security Evaluation Criteria
ITSG	Information Technology Standards Guidance
ITU	International Telecommunications Union
ITU-R	International Telecommunications Union - Radiography (formerly the CCIR)
ITU-TSS	International Telecommunications Union - Telecommunications Standardization Sector (formerly the CCITT)
JBIG	Joint Bi-Level Imaging Group
JCALS	Joint Computer-Aided Acquisition and Logistic Support
JIEO	Joint Interoperability Engineering Organization
JPEG	Joint Photographic Experts Group
JTA	Joint Technical Architecture
JTC1	Joint Technical Committee One (ISO/IEC)
KBPS	Kilobytes per Second
KMP	Key Management Protocol
LAN	Local Area Network
LM	License Management
LMS	Logistics Management System
LS	License Management System
LSA	Logistic Support Analysis
LSAR	Logistic Support Analysis Records
LWER	Light Weight Encoding Rules (BER/ASN)
LZW	Lempel-Ziv-Welsh (data compression algorithm)
MAC	Mandatory Access Controls
MAC	Media Access Control
MAC	Message Authentication Code
MAP	Manufacturing Automation Protocol
MB	Megabyte
MCCR	Mission Critical Computer Resources
MHEG	Multimedia/Hypermedia Experts Group
MHS	Message Handling System
MHz	Megahertz

MIB	Management Information Base
MICR	Magnetic Ink Character Recognition
MIDI	Musical Instrument Digital Interface
MIL-STD	Military Standard
MIS	Management Information System
MIT	Massachusetts Institute of Technology
MMFS	Manufacturing Message Format Standard
MMI	Man-Machine Interface
MMS	Manufacturing Message Standard
MO	Magneto-Optical
MO:DCA	Mixed Object Document Content Architecture (IBM)
MOOLIT	Motif/Open Look Toolkit Intrinsics
MOTIS	Message Oriented Text Interchange System
MOSS	Map Overlay Statistical System (Autometric)
MPC	Multimedia Personal Computer
MPEG	Motion Pictures Expert Group
MS	Microsoft
MSP	Message Security Protocol
MTA	Message Transfer Agent
MTF	Message Text Formats
MTF	Message Transfer Facility
MUI	Management User Interface
MVL	Multivalue Logic System
MWM	Motif Window Manager
NAPLPS	North American Presentation Level Protocol Syntax
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NBS	National Bureau of Standards (now NIST)
NBSIRNBS	Interim Report
NCGA	National Computer Graphics Association
NCSC	National Computer Security Center
NCSL	National Computer Systems Laboratory (NIST)
NDL	Network Data Language
NeL	Network Event Logger
NetLS	Network License System
NFS	Network File System
NGCR	Next Generation Computer Resources
NGS	Non-Government Standards
NGSB	Non-Government Standards Body
NIMA	National Imagery and Mapping Agency (formerly DMA)
NISO	National Information Standards Organization
NIST	National Institute of Standards and Technology
NISTIR	NIST Interim Report
NITF	National Imagery Transmission Format

NITFS	National Imagery Transmission Format Standard
NIUF	National ISDN Users' Forum
NIUG	National IGES User's Group
NLSP	Network Layer Security Protocol
NMF	Network Management Forum
NMSIG	Network Management SIG
NPC	National Public Consensus
NPESA	National Printing Equipment and Supply Association
NSA	National Security Agency
NSC	National Safety Council
NSEP	National Security Emergency Preparedness
NSI	Non-Standard Interface
NT	New Technology (MS-Windows)
NTF	National Transfer Format (BSI)
NTIS	National Technical Information Service
NTSC	National Television System Committee (US)
OCR	Optical Character Recognition
OCR-MA	Optical Character Recognition- Matrix
ODA	Office Document Architecture
ODIF	Office Document Interchange Format
ODL	Office Document Language
ODMG	Open Database Management Group
ODP	Open Distributed Processing
ODT	Optical Digital Technologies
OIM	Object Information Management
OIW	OSE Implementors' Workshop (NIST)
OLE	Object Linking and Embedding
OLIT	Open Look Intrinsics Toolkit
OLTP	Online Transaction Processing
OLWM	Open Look Window Manager
OMG	Object Management Group
ONC	Open Network Computing
OSD	Office of the Secretary of Defense
OSE	Open System Environment
OSF	Open Software Foundation
OSHA	Office of Safety and Health Administration
OSI	Open Systems Interconnection (ISO)
PAL	Phase Alternation Line
PAR	Project Authorization Request (IEEE)
PART	POSIX/Ada Real-Time project
PBX	Private Branch Exchange
PC	Personal Computer
PCF	Portable Compiled Format

PCIS	Portable Common Interface Set (NATO)
PCMCIA	Personal Computer Memory Card Industry Association
PC/NFS	Personal Computer/Network File System
PCTE	Portable Common Tools Environment (ECMA)
PDAD	Preliminary Draft Addendum (ISO)
PDAM	Preliminary Draft Amendment (ISO)
PDDI	Product Data Definition Interface
PDES	Product Data Exchange Using STEP
PDI	Picture Description Language
PDL	Page Description Language
PEL	Picture Element
PER	Packed Encoding Rules (BER/ASN)
PERMS	Personnel Electronic Records Management
PEX	PHIGS Extension to X
PHIGS	Programmer's Hierarchical Interactive Graphics System
PHIGS+	Programmer's Hierarchical Interactive Graphics System Plus Lumier and Surfaces (PLUS)
PICS	Protocol Implementation Conformance Statement
PIF	Page Image Format
PIK	Programmer's Imaging Kernel
PLPS	Presentation Level Protocol Syntax
PLUS	Plus Lumier und Surfaces (see PHIGS)
PM	Program Manager
POSIX	Portable Operating System Interface for Computer Environments
PRC	Planning Research Corporation
RAPID	Reusable Ada Products for Information Systems Development
RDA	Remote Database Access
RFC	Request for Comment
RFP	Request for Proposal
RFS	Remote File System
RGB	Red, Green, Blue
RLE	Run Length Encoding
RODE	Remote Open Document Editing
ROP	Remote Operations Protocol
ROSE	Remote Operations Service Elements
ROSEP	Remote Operations Service Elements Protocol Definition
ROSES	Remote Operations Service Elements Service Definition
RPC	Remote Procedure Call
RRIP	Rock Ridge Interchange Protocol
RSA	Rivest-Shamir-Adelman
RTCP	Real-Time Communication Protocols
RTSE	Reliable Transfer Service Element
SAA	Systems Application Architecture

SAE	Society of Automotive Engineers
SAG	SQL Access Group
SAME	SQL Ada Module Extensions
SAMEDL	SAME Description Language
SBIS	Sustaining Base Information System
SCCS	Source Code Control System
SCD	Stock Control and Distribution (SYSTEM)
SCO	Santa Cruz Operation
SDD	Software Design Document
SDF	Standard Delay File Format
SDIF	SGML Document Interchange Format
SDNS	Secure Data Network Systems
SDO	Standards Developing Organization
SDTS	Spatial Data Transfer Standard
SDU	Software Development Utilities
SECAM	Systeme Electonique Couleur Avec Memoire
SEE	System Engineering Environment
SEI	Software Engineering Institute
SE-ODP	Support Environment for Open Distributed Processing
SGML	Standard Generalized Markup Language
SIF	Standard Interchange Format (Intergraph)
SIG	Special Interest Group
SIGADA	Ada Special Interest Group (ACM)
SIGGRAPH	Graphics Special Interest Group (ACM)
SII	System Internal Interface
SILS	Standard for Interoperable LAN Security
SMDL	Standard Music Description Language
SMB	Server Message Block
SMD	Standardized Military Drawing
SME	Society of Manufacturing Engineers
SME	Subject Matter Expert
SMI	Structure of Management Information
SMIGS	Standard Military Graphics Symbols
SMP	Simple Management Protocol
SMPTE	Society of Motion Picture and Television Engineers
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNDCF	Subnetwork Dependent Convergence Facility
SNF	Server Normal Format
SNI	Simple Network Interface
SNMP	Simple Network Management Protocol
SP	Security Protocol
SP	Special Publication (NIST)
SP	Standardization Profile
SPC	Software Productivity Consortium

SPDL	Standard Page Description Language
SPI	System Programming Interface
SPM	Software Programmer's Manual
SQL	Structured Query Language
SS	Sampled Servo
SSC	Standards Systems Center
STANAG	Standardization Agreement (NATO)
STARS	Software Technology for Adaptable, Reliable Systems
STD	Standard
STDL	Standardized Transaction Definition Language
STL	Standard Textual Language
STEP	Standard for Exchange of Product Model Data
SUSP	System Use Sharing Protocol
SVID	System V Interface Definition
SVRn	System V Release n (USL)
TACO-2	Tactical Communication Protocol 2
TADIL	Tactical Digital Information Link
TAE	Transportable Application Environment
TAE+	Transportable Application Environment Plus
TAR	UNIX Transfer Tape Format
TBD	To Be Determined
TCL	TAE Command Language
TCOS	Technical Committee on Operating Systems (IEEE)
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSEC	Trusted Computer Systems Evaluation Criteria
TDI	Trusted Database Interpretation
TEI	Text Encoding Initiative
TFA	Transparent File Access
TFTP	Trivial File Transfer Protocol
TGA	Targa Image Format
TIFF	Tagged Image File Format
TIGER	Topographically Integrated Geographical Encoding and Referencing (U.S. Census Bureau)
TLI	Transport Layer Interface
TLSP	Transport Layer Security Protocol
TNI	Trusted Network Interpretation
TNT	The News Toolkit
TOP	Technical and Office Protocol
TOSCA	Text and Office Systems Color Architecture (ISO)
TP	Transaction Processing
TR	Technical Report
TRIF	Tiled Raster Interchange Format (DOD)
TS	Timer Services
TSR	Terminate and Stay Resident

TSS	Telecommunications Standardization Sector (ITU)
UCC	Uniform Code Council
UDT	Unstructured Data Transfer
UEF	User Exchange Format
UFS	Unix File System
UI	Unix International
UIDL	User Interface Definition Language
UIL	User Interface Language (OSF)
UIMS	User Interface Management Services
UISRM	User Interface System Reference Model (NIST)
UK	United Kingdom
UPC	Uniform Product Code
USGS	United States Geological Survey
USL	Unix Systems Labs
USMTF	United States Message Text Format
USS	Uniform Symbology Specification
UUCP	Unix-to-Unix Copy Protocol
VDI	Virtual Device Interface
VDM	Virtual Device Metafile
VDT	Video Display Terminal
VHDL	VHSIC Hardware Description Language
VMF	Variable Message Format
VMUIF	Voice Messaging User Interface Forum
VOXEL	Volume Element
VPF	Vector Product Format
VPS	Vector Product Standard
VQ	Vector Quantization
VT	Virtual Terminal
WAN	Wide-Area Network
WD	Working Draft (ISO)
WDAD	Working Draft Addendum (ISO)
WDAM	Working Draft Amendment (ISO)
WG	Working Group
WMO	World Meterological Organization
WORM	Write-Once Read Many
WWMCCS	World-Wide Military Command and Control System
WYSIWYG	What You See Is What You Get
XAPIA	X.400 API Association
XAP-TP	X/Open API- Transaction Processing
XCDR	X/Open CD ROM
XDR	External Data Representation
XDS	X/Open Directory Services

XDSF	X/Open Distributed Security Framework
X11Rn	X Windows version 11, Release n
XLFD	X Logical Font Description
XMOG	X/Open Managed Object Guide
XMP	X/Open Management Protocol
XMPP	X/Open Management Protocol Profiles
XNFS	X/Open Network File System
XOM	X/Open OSI Abstract Data Manipulation
XPG	X/Open Portability Guide
XTI	Transport Independent Interface
XVT	Extensible Virtual Toolkit

2.6.2 Terms used in the ITSG. The following definitions align as closely as possible to the standard IEEE Computer Society definitions and come from a myriad of standards bodies. Be careful to understand the terms commonly used inside and outside this document. Different standards bodies often use different words for the same meaning or may use the same word with an assumption of a slightly different meaning. For example, the American National Standards Institute (ANSI) used the term "levels" (meaning "level 1," "level 2," and "Core") to signal a particular implementation's varying conformance level; however, this usage is parallel to the IEEE POSIX's usage of "fully conforming" and "conforming with extensions."

Abstraction: An abstraction denotes the essential characteristics of an object that distinguish it from all other kinds of objects, providing crisply defined conceptual boundaries, relative to the perspective of the viewer. (See Object-Based and Object-Oriented Language).

Accredited Standards Development Organization: An organization recognized as a standards development organization by ISO, IEC, ITU-T, or recognized as a standards development organization by one of the member bodies of one of these three organizations.

Adopted: The DOD status "Adopted" is used to mean that the standard in the ITSG is approved by DOD for use in satisfying each function of the BSA where there exists no JTA mandated standard. Adopted standards may be implemented but shall not be used in lieu of a mandated standard. The word adopted refers to standards included in the TAFIM.

Application: "The use of capabilities provided by an information system specific to the satisfaction of a set of user requirements." (IEEE Std 1003.0-1995)

Application Environment Profile (AEP): "A profile, specifying a completed and coherent specification of the Open System Environment (OSE), in which the standards, options, and parameters chosen are necessary to support a class of applications." (IEEE Std 1003.0-1995)

Application Platform: "A set of resources, including hardware and software, that support the services on which application software will run. The application platform provides services at its interfaces that, as much as possible, make the specific characteristics of the platform transparent to the application software." (IEEE Std 1003.0-1995)

Application Program Interface (API): "The interface between the application software and the application platform, across which all services are provided." (IEEE Std 1003.0-1995)

Application Software: "Software that is specific to an application and is composed of programs, data, and documentation (IEEE Std 1003.0-1995)

Approved: The specification has been approved and published by its sponsoring body.

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.

Base Standard: "An approved international standard, technical report, ITU-T Recommendation, or national standard." (IEEE Std 1003.0-1995)

Base Standard Profile: A profile, or listing, of applicable base standards. (See Profile of Standards.)

Class: A set of objects with a common structure and behavior.

Communication Interface: "That part of the API devoted to communications with other application software, external data transport facilities, and devices." (IEEE Std 1003.0-1995)

Component Profile: "A profile that is made up of a formally defined subset of a single standard." (IEEE Std 1003.0-1995)

Conditional feature: A feature or behavior referred to in a standard not essential on all conforming implementations.

Conformance: "A statement of conformance to a POSIX standard is based on a completed test of the target system using POSIX.3 conforming test methods, where for each POSIX.3 assertion for that standard, there is a correctly assigned test result code." (IEEE Std 1003.3-1991)

Conformance Documentation: "A formal record of the testing of a product for conformance to a particular standard." (ISO/IEC 9945-1)

Consortia (Standards): Standards developed by industry associations, consortia, and other public bodies not recognized as formal standards bodies.

Criteria for Inclusion: Qualities considered to determine whether a standard will be included.

Cross-Category Services: "A set of tools and/or features that has a direct effect on the operation of one or more components of the OSE, but is not in and of itself a stand-alone component." (IEEE Std 1003.0-1995)

De facto: Indicating the use of the product or specification in reality that is tantamount to being legally constituted as a standard.

De jure: Indicating that a specification has undergone the standardization process of a formal standards body.

Deficiency: A functionality needed, but not provided, by the standard.

Dependency: One standard requiring the support of other standards to create a valid implementation.

Detailed Profile: see Standard Profile.

Distributed (System, Processing): A system or process consisting of interdependent software or hardware/software entities separated either physically or chronologically.

Emerging Standard: According to the JTA, a DOD "Emerging" status denotes a candidate standard to be added as, or to replace, a mandated standard. This includes standards required to capitalize on new technologies. These candidates will help the program manager determine those areas that are likely to change in the near term (within three years) and suggest those areas in which "upgradability" should be a concern. The expectation is that emerging standards will be elevated to mandated status in the JTA when implementations of the standards mature. Emerging standards may be implemented but shall not be used in lieu of a mandated standard.

Encapsulation: The process of hiding all of the details of an object that do not contribute to its essential characteristics. (See Object-Based and Object-Oriented Language).

Explicit Services: "Services that can be accessed from an application program (via an API) and generally are only provided when requested." (IEEE Std 1003.0-1995)

External Environment: "A set of entities external to the application platform with which services are provided. External entities include people, exchangeable media that is not mounted in the platform, communication wiring, and other platforms." (IEEE Std 1003.0-1995).

External Environment Interface (EEI): "The interface between the application platform and the external environment across which services are provided. The EEI is defined primarily in support of system and application interoperability. The primary services present at the EEI comprise:

a. Human/Computer Interaction Services
b. Information Services
c. Communication Services" (IEEE Std 1003.0-1995)

Extension: An addition to the core specifications of a standard.

Formal Standards Body: "Formally recognized standards bodies responsible for definition and dissemination of public standards." (IEEE Std 1003.0-1995)

Hardware: "Physical equipment used in data processing, as opposed to programs, procedures, rules, and associated documentation." (IEEE Std 1003.0-1995).

Harmonization: "The process of ensuring that profiles do not overlap or conflict." (IEEE Std 1003.0-1995).

Hierarchy: A ranking or ordering of abstractions. (See Object-Based and Object-Oriented Language).

Hostile Standard Feature: Any feature of a standard that could impede transportability or requires additio cost to transport.

Human/Computer Interface (HCI): "The boundary across which physical interaction between a human being and the application platform takes place." (IEEE Std 1003.0-1995).

Implementation Defined: "An indication that the implementation shall define and document the requirements for correct program constructs and correct data of a value or behavior." (ISO/IEC 9945-1)

Implementation Dependent: Indicates that each implementor may define that portion of the application at will.

Implicit Services: "Services that the platform provides without a direct request." (IEEE Std 1003.0-1995)

Information Technology: Technology related to computer hardware and software for the processing, storage, and transfer of information.

Informational: Informational standards include those remaining standards that fall outside the official DOD statuses of "mandated," "adopted," "emerging," and "legacy."

Interface: "A shared boundary between two functional entities. A standard specifies the services in terms of the functional characteristics and behavior observed at the interface. The standard is a contract in the sense that it documents a mutual obligation between the service user and provider and assures stable definition of that obligation." (IEEE Std 1003.0-1995)

Internationalization: "The process of designing and developing an implementation with a set of features, functions, and options intended to satisfy a variety of cultural environments." (IEEE Std 1003.0-1995)

Interoperability: "The ability of two or more systems to exchange information and to use the information that has been exchanged." (IEEE Std 1003.0-1995)

Language-Binding API specification: "A specification that documents the source code method, consistent with a specific programming language, used by an application to access services provided by an application platform." (IEEE Std 1003.0-1995)

Language-Independent Service Specification: "A specification that defines a set of required functional semantics independent of the syntax and semantics of a programming language." (IEEE Std 1003.0-1995)

Locale: "The definition of the user environment that depends on language and cultural conventions." (IEEE Std 1003.0-1995)

Loss-less Compression: A compression technique that compresses data (or an image) without losing any bits or deteriorating the resolution of an image. Compression ratios are not tremendously high in this type of compression.

Lossy Compression: A compression technique that compresses data (or an image) but loses bits in the process. The quality of the image may deteriorate; however, extremely high compression ratios may be obtained in this type of compression.

Local Adaptation: "The process of modifying a product that is specific to one culture to make it specific to another culture." (IEEE Std 1003.0-1995)

Localization: "The process of utilizing the internationalization features to adapt an internationalized product to a specific cultural environment." (IEEE Std 1003.0-1995)

Major Service Area: A major service area (MSA) is one of the basic categories of services required by information systems. The MSAs are Software Engineering, User Interface, Data Management, Data Interchange, Graphics, Communications and Network, and Operating System Services.

Mandated Standard: The DOD status "Mandated" is used for those standards mandated by the JTA. A standard is mandatory in the sense that IF a service/interface is going to be implemented, it shall be implemented in accordance with the associated standard. If a required service can be obtained by implementing more than one standard, the appropriate standard should be selected based on system requirements.

Modularity: The property of a system that has been decomposed into a set of cohesive and loosely coupled modules. (See Object-Based and Object-Oriented Language)

Object (Instance, Software Object): An object is a software entity that has state, behavior, and identity; the structure and behavior of similar objects are defined in their common class; the terms instance and object are interchangeable.

Object-Based Language: Any programming language that supports some but not all of the characteristics of Abstraction, Encapsulation, Modularity, and Hierarchy.

Object-Oriented Language: Any programming language that fully supports the characteristics of Abstraction, Encapsulation, Modularity, and Hierarchy.

Obsolescent: An indication that a certain feature may be considered for withdrawal in future revisions of a standard.

Open Specifications: "Specifications that are maintained by an organization that uses an open, public consensus process to accommodate new technologies and user requirements over time." (IEEE Std 1003.0-1995)

Open System: "A system that implements sufficient open specifications or standards for interfaces, services, and supporting formats to enable properly engineered applications software:

a. To be ported with minimal changes across a wide range of systems from one or more suppliers
b. To interoperate with other applications on local and remote systems
c. To interact with people in a style that facilitates user portability" (IEEE Std 1003.0-1995)

Open System Application Program Interface: "A combination of standards-based interfaces specifying a complete interface between an application program and the underlying application platform." (IEEE Std 1003.0-1995)

Open System Environment (OSE): "A comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles." (IEEE Std 1003.0-1995)

Option: "A portion of the specification within a standard that is not required to be present in a conforming implementation." (See also Conditional Feature.) (IEEE Std 1003.3-1991)

Performance: "A measure of a computer system or subsystem to perform its functions; for example, response time, throughput, number of transactions per second. The efficiency of a system in accomplishing pieces of work is an attribute of performance." (IEEE Std 1003.0-1995)

Performance Requirement: "A requirement that specifies a performance characteristic that a system or system component must possess; for example, speed, accuracy, frequency." (IEEE Std 1003.0-1995)

Platform Internal Interface (PII): "The interface between application platform service components within that platform." (IEEE Std 1003.0-1995)

Platform Profile: "A profile whose focus is on functionality and interfaces for a particular type of platform, which may be a single processor shared by a group of applications or a large distributed system with each application dedicated to a single processor." (IEEE Std 1003.0-1995)

Portability (application software): "The ease with which application software and data can be transferred from one application platform to another." (IEEE Std 1003.0-1995)

POSIX (Portable Operating System Interface for Computer Environments): The term "POSIX" has been evolving into a term with a number of different meanings. POSIX is sometimes

used to denote the formal standard ISO/IEC 9945-1:1990, sometimes to denote that standard plus related standards and drafts emerging from IEEE PASC working groups, and sometimes to denote the groups themselves. This guide refers to the original POSIX standard by its standard designation, ISO/IEC 9945-1:1990, and not by the term POSIX.

The IEEE groups developing standards related to IEEE P1003 are called IEEE P1003.n working groups. Examples are the IEEE working groups P1003.2 and P1003.3, etc. The names of the groups are sometimes abbreviated POSIX.2, POSIX.3, etc., but this convention is not used by this guide; confusion could result when the IEEE P1003 decimal number does not match the ISO/IEC 9945 part number (such as with P1003.7 and ISO/IEC 9945-3). Furthermore, other IEEE open systems working groups such as P1224 do not use the POSIX prefix. Therefore, all IEEE projects and working groups are referred to uniformly as Pnnnn.

The standards emerging out of the POSIX working groups are referred to by their formal names (e.g., IEEE Std. 1003.2-1992 or IEEE P1003.10/D9) and are called either POSIX Base Standards or POSIX Standardized Profiles (POSIX SPs). (IEEE Std 1003.0-1995)

POSIX Standardized Profile (POSIX SP): "A Standardized Profile that specifies the application of certain POSIX base standards in support of a class of applications and does not require any departure from the structure defined by the Reference Model for POSIX systems." (IEEE Std 1003.0-1995)

Process: "An address space and one or more threads of control that execute within that address space, and their required system resources." (IEEE Std 1003.0-1995)

Product Implementation: The usable, binary loadable code sold by vendors and, in some cases, bundled with hardware.

Profile: "A set of one or more base standards, and, where applicable, the identification of chosen classes, subsets, options, and parameters of those base standards, necessary for accomplishing a particular function." (IEEE Std 1003.0-1995)

Profile, Standard's: A listing of the specific set of options from a standard that will be implemented to satisfy a system's requirements.

Profile of Standards: A list of the standards to be applied in a given system or functional area.

Programming Language API specification: "The interface between applications and application platforms traditionally associated with programming language specifications, such as program control, math functions, string manipulation." (IEEE Std 1003.0-1995)

Proprietary Specification: A specification developed and marketed by a company having exclusive rights to modify and sell it. The specification may be changed at will by the owner without going through a standards body consensus process.

Protocol: "A set of semantic and syntactic rules that determine the behavior of entities that interact." (IEEE Std 1003.0-1995)

Public Specifications: "Specifications that are available, without restriction, to anyone for implementation, sublicensing, and distribution (i.e., sale) of that implementation." (IEEE Std 1003.0-1995)

Reference Model: "A structured collection of concepts and their relationships that scope a subject and enable the partitioning of the relationships into topics relevant to the overall subject and that can be expressed by a common means of description." (IEEE Std 1003.0-1995)

Scalability: "The ability to provide functionality up and down a graduated series of application platforms that differ in speed and capacity." (IEEE Std 1003.0-1995)

Security: "The protection of computer resources (e.g., hardware, software, and data) from accidental or malicious access, use, modification, destruction, or disclosure. Tools for the maintenance of security are focused on availability, authentication, accountability, confidentiality, and integrity." (IEEE Std 1003.0-1995)

Single-standard Profile: "A single-standard profile (such as FIPS Publication 151-2) may consist of a subset of a particular standard or a single standard where parameters and options have been selected. This type of profile is often used when there is a wide range of options and parameters in a base standard and specifying these options can focus implementation efforts. It is important to be aware that some base standards reference other base standards normatively even when defining a singe-standard profile." (IEEE Std 1003.0-1995)

Software: "The programs, procedures, rules, and any associated documentation pertaining to the operation of an information processing system." (IEEE Std 1003.0-1995)

Spanning Service Area: Spanning service area volumes, as used in this ITSG, are constructed for any subject domain that crosses major service areas.

Specification: "A document that prescribes, in a complete, precise, verifiable manner, the requirements, design, behavior, or characteristics of a system or system component." (IEEE Std 1003.0-1995)

Standard: "A document, established by consensus and approved by an accredited standards development organization, 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." (IEEE Std 1003.0-1995)

Standard Feature: "A function provided in a standard. Either a single facility or behavior, or, one of a pair of alternative facilities or behaviors, required by a standard that is always present on a conforming implementation." (IEEE Std P1003.2-1991)

Standard Profile: A profile of standards, not necessarily having gone through a process as a standardized profile.

Standardized Profile: "A balloted, formal, harmonized document that specifies a profile." (IEEE Std 1003.0-1995)

Standard Development Organization: "An accredited organization that formally develops and coordinates standards for use by a community. (IEEE Std 1003.0-1995)

Standards Implementation: A product that implements a standard.

Standard's Profile: see Profile, Standard's.

Supported: A condition regarding optional functionality. (ISO/IEC 9945-1)

System Documentation: "All documentation provided with an implementation, except the conformance document." (ISO/IEC 9945-1)

Tailoring Guidance: Guidance concerning a specific information processing standard on the specific features, modes, switch settings, functions, areas of deficiencies, extensions, levels, and options. This information is provided to tailor the specification for use to exploit it best for eventual transportability at the source code level.

Thread: "A single flow of control within a process." (IEEE Std 1003.0-1995)

Transaction: "A unit of work consisting of an arbitrary number of individual operations, all of which will either complete successfully or abort with no effect on the intended resources. A transaction has well-defined boundaries. A transaction starts with a request from the application program and either completes successfully (commits) or has no effect (abort). Both the commit and abort signify completion of a transaction." (IEEE Std 1003.0-1995)

Transaction Application Program: "Transactions have boundaries (start points and end points) that are determined by the action of the transaction application program. The transaction application program can request either to commit or roll back the work done in the transaction when it identifies the end point. The system will complete a commit operation only if all operations performed during the transaction can complete successfully. Otherwise, the system will abort the transaction (roll back the work done by it) and notify the transaction application program of this action." (IEEE Std 1003.0-1995)

Undefined: "An indication that a part of the standard imposes no portability requirements on an application's use of an indeterminate value on its behavior with erroneous program constructs or erroneous data." (ISO/IEC 9945-1)

Unspecified: "An indication that a part of a standard imposes no portability requirements on applications for correct program constructs or correct data regarding a value on behavior."

(ISO/IEC 9945-1)

Validation: "The process of testing an application or system to ensure that it conforms to its specification." (IEEE Std 1003.0-1995)

2.7 Notes.

2.7.1 Comments. The Center for Standards solicits comments on the ITSG and experiences in using standards from users of this document. Use of a standard format for submitting a change proposal will expedite the processing of changes. The following format is suggested for use in responding with comments or other useful information about specific instances of use of standards.

a. Point of Contact Identification
   (1) Name:
   (2) Organization and Office Symbol:
   (3) Street:
   (4) City:
   (5) State:
   (6) Zip Code:
   (7) Area Code and Telephone #:
   (8) Area Code and Fax #:
   (9) E-mail Address:

b. Document Identification
   (1) Volume Number:
   (2) Document Title:
   (3) Version Number:
   (4) Version Date:

c. Proposed Change #1
   (1) Section Number:
   (2) Page Number:
   (3) Title of Proposed Change:
   (4) Wording of Proposed Change:
   (5) Rationale for Proposed Change:
   (6) Other Comments:

d. Proposed Change #2
   (1) Section Number:
   (2) Page Number:
   (3) Title of Proposed Change:
   (4) Wording of Proposed Change:
   (5) Rationale for Proposed Change:
   (6) Other Comments:

e. Proposed Change #n
   (1) Section Number:
   (2) Page Number:
   (3) Title of Proposed Change:
   (4) Wording of Proposed Change:
   (5) Rationale for Proposed Change:
   (6) Other Comments:

The preferred method of proposal receipt is via e-mail in ASCII format, sent via the Internet. If not e-mailed, the proposed change, also in the format shown, on both paper and floppy disk, should be mailed. As a final option, change proposals may be sent via fax; however, delivery methods that enable electronic capture of change proposals are preferred. Address information for proposing comments is shown below.

Internet:	bookera @ ncr.disa.mil	or	jpratt@logicon.com
Mail:	DISA/JIEO/CFS Code: JEBEA (Angela Booker) 10701 Parkridge Blvd Reston, VA 20191-4357	or	Logicon Attn: John Pratt 1831 Wiehle Avenue, Suite 300 Reston, VA 20190-5241
Fax:	703-735-3257	or	703-318-1098
Voice:	703-735-3536		

The status of comments on the ITSG are recorded in a database, and the comments themselves are distributed to working groups for resolution.

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 1 of 14 parts)

INTRODUCTION/GUIDE

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

3.1 Introduction/Guide. The detailed requirements sections for each service area are located in separate parts of the ITSG. Refer to Table 2.2-1, section 2.2, to view the major and spanning service areas and the part of the ITSG document in which these service areas are located.

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 2 of 14 parts)

SOFTWARE ENGINEERING SERVICES

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

TABLE OF CONTENTS

LIST OF TABLES

3.2 Software engineering services. Software engineering services cover all Open System Environment (OSE) services related to the support of information systems development. These services include, but are not limited to, Computer Aided Software Engineering (CASE), software life cycle processes, programming languages, and language bindings.

NOTE: Throughout Part 2, all tables shall have abbreviations listed under the column Standard Type as follows:

a. National Public Consensus = NPC.
b. International Public Consensus = IPC.
c. Government Public Consensus = GPC.
d. Consortia Public Consensus = CPC.
e. Corporate Private Non-Consensus = CPN-C.

For the standard reference column of the table an "R" before the date indicates "reaffirmed."

3.2.1 Software engineering environments. Software Engineering Environments (SEE) provide a set of services across one or more life cycle phases (e.g., requirements, implementation) and support development activities (e.g., design and coding). A SEE consists of resources (hardware, software, tools) and an integration mechanism (e.g., operating system or framework), and is designed around a set of supporting standards and interfaces. The identified SEE standards and interfaces are intended to facilitate the passing of information and data internal and external to the SEE, as well as to provide access to required services. In this document, emphasis is placed on the standards, interfaces, metadata formats and guides that provide the basis for integration, expansion and tailoring of the SEE, its tools and resources.

3.2.1.1 CASE/software development environment. The environments and tools considered are inclusive of all integrated CASE environments. The identified documents support extensive and diverse environments containing numerous integrated software development tools that span the software life cycle. These environments include sets of tools, firmware devices and hardware necessary to support the development and design of software. The tools span a broad range of services and may include, but are not limited to analysis tools, design and test tools, simulation and prototyping tools, code generators and analyzers, and other management tools used in SEEs.

3.2.1.1.1 Standards. Table 3.2-1 presents standards for software development environments.

TABLE 3.2-1 CASE/software development environment standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	Recommended Practice for the Evaluation and Selection of CASE Tools	1209:1993	Adopted (Approved)
IPC	ECMA	Portable Common Tool Environment (PCTE) - Abstract Specification	149 (1994)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	Standard Reference Model for Computing System Engineering Tool Interconnections	1175:1992	Informational (Approved)
NPC	EIA	CDIF interim standards (CASE Data Interchange Format)	PN2387, 2389, 2329	Informational (Approved)
IPC	ISO	Portable Common Tool Environment (PCTE) - Part 1: Abstract Specification (ECMA 149:1990)	13719-1:1995	Informational (Approved)
NPC	ANSI	CASE Tool Integration Messages (CTIM) X3.273	(X3H6)	Informational (Draft)

ECMA 149, Portable Common Tools Environment (PCTE) was developed by the European Economic Community (EEC), ECMA, and European regional standards organizations. ECMA 149 is an abstract specification of a tool portability interface. The document has matured, with international collaboration, and is incorporated in ISO 13719-1:1994.

The IEEE standard 1175 is a Standard Reference Model for Computing System Engineering Tool Interconnections. The core of this standard is the Semantic Transfer Language (STL), which describes concepts such as data, conditions, events, and states, as well as transformation, control-transition, and state-transition operations. This standard supports both textual and graphical forms.

CASE Data Interchange standards, such as the Electronics Industries Association's (EIA) CASE Data Interchange Format (CDIF), (eventually to become three ISO standards) for the exchange of information between CASEs. The three standards address: a framework standard, a syntax standard, and a semantic standard. When completed these standards will provide data interchange among CASE tools used in an integrated CASE environment.

3.2.1.1.2 Alternative specifications. No alternative specifications are known.

3.2.1.1.3 Standards deficiencies. Implementations of existing standards are scarce. PCTE has only two known environment implementations (TRANSTAR and PORTOS). A previous implementation of PCTE, Emeraude, is now called TRANSTAR. Many tools requiring encapsulation into the PCTE framework already exist and have been integrated into the UNIX environment. Customers using these tools and wanting to migrate into the PCTE world would have to encapsulate something that already has been integrated into a potential environment on the UNIX side. The latter would be an inefficient means of integrating a tool into the PCTE side of the house, despite the need for the existence of such (especially if the user already has these tools resident within his UNIX environment). The increased popularity of the CORBA specification may preclude PCTE usage and obviate the need for such.

3.2.1.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.2.1.1.5 Related standards. The following list contains additional references:

a. Reference Model for SEE Frameworks (NIST SP-500-211/ECMA TR/55).

b. Next Generation Computer Resources for Project Support Environments V2.0 (RM PSE) NIST SP-500-213.

c. Other related integrated software development services, such as A Tool Integration Standard (ATIS), have been proposed in the U.S., (by the CASE Integration Services Committee (CIS) working with ANSI), and Europe.

3.2.1.1.6 Recommendations. ANSI/IEEE 1209 is the recommended standard for CASE/software development, but additional definitions can be found in NIST SP 500-213. To ensure uniformity and consistency of service definitions between vendors, contractors, tools, integrators, etc., NIST SP 500-211, Reference Model for SEE Frameworks, is a technical report containing an extensive set of service descriptions and definitions for a SEE framework from which tools may be selected. The report presents consensus definitions of services and is intended to assist individuals in communicating and identifying information relative to SEE services for making comparisons, adjudicating differences in implementations, and resolving issues. It is recommended when defining framework and software engineering services. The document was developed with the participation from ECMA and DOD, with a corresponding version published by ECMA for the European community.

3.2.1.2 Reusable source code libraries. Emerging and maturing reusable source code libraries are collections of components that can be compiled for reuse on different machines with different applications. A number of government agencies and commercial enterprises are currently involved in reusable libraries. Use of the term library is intended to imply certification of the reusable components. Reusable components include models, design, architectural structures, requirements, code, documentation, and other reusable entity.

3.2.1.2.1 Standards. Table 3.2-2 presents standards for reusable source code libraries.

TABLE 3.2-2 Reusable source code libraries standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OMG	Object Management Group (OMG) Object Class Libraries	Object Management Group (OMG) Object Class Libraries	Informational (Formative)

3.2.1.2.2 Alternative efforts. The following libraries are available:

a. DOD Reuse Libraries:
- Army Reuse Center Library and Catalog (ARC)
- C2MUG Software Catalog (mathematics and various Ada functions)
- Common Ada Missile Components (CAMC)
- Software Technology for Adaptable, Reliable Systems Repository (STARS)
- Defense Software Repository System (DSRS) includes nodes at DISA, the Army and Air Force.
- Comprehensible Approach to Reusable Defense Software (CARDS)
- Air Force Reuse Center Library and Catalog
- NASA's Electronic Services and Application (ELSA)
- Asset Source for Software Engineering Technology (ASSET)
- CECOM Weapon System Software Catalog
- Reuse Information Clearinghouse
- Army Topographic Engineering Center (TEC)

b. Commercial Reuse Libraries:
- Booch's Software Components for Ada 95
- EVB Generic Reusable Ada Components for Engineering (GRACE)
- NETLIB Repository at University of Tennessee (UTK)

3.2.1.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.1.2.4 Portability caveats. This is a high portability risk area because no standards exist.

3.2.1.2.5 Related standards. Related standards are unknown. Reusable source code standards have yet to be developed. However, companion standards to software reuse are DOD-STD-498

and EIA/IEEE J-STD-016, since any reuse guidelines must be consistent with them. Furthermore, in the absence of formal, adopted standards, the following reuse guides and documents may be of assistance in addressing the reuse issues:

a. DOD Software Reuse Vision and Strategy, July 1992, DOD Technical Report 1222-04-210/40, NTIS Accession No. ADA 260109.

b. Glossary of Software Reuse Terms, NIST Special Publication 500-222, December 1992.

c. STARS ASSET Documents:
- CARDS Technical Concept, STARS-AC-04107A/001/001, 22 March 1993.
- Standards and Guidelines for Repository Deliverables, DTIC AD-A240478, 17 March 1989.
- Repository Specifications, DTIC AD-A228467, 16 February 1990.
- Repository Standards and Guidelines, DTIC AD-A228484, 17 March 1989.
- CARDS Program Document, Engineer's Handbook, complements DOD-STD-498.

3.2.1.2.6 Recommendations. Standards on reuse libraries are emerging and lag behind other standards. Reuse libraries should be evaluated to identify components that meet functional requirements and are cost effective over the life of the system. Effective reuse of components can be achieved if early system life cycle requirements and domain analysis are performed to identify potential reuse components for inclusion into a repsoitory.

3.2.1.3 Specialized language and compiler tools. Specialized language and compiler tools are a collection of traditional operating system-based tools to update, maintain, and regenerate programs, develop system software, and provide sophisticated pattern matching functions.

Operating system-based software development tools are a collection of traditional tools to support standardized software development, maintenance, management, and version control.

3.2.1.3.1 Standards. Table 3.2-3 presents standards for specialized language and compiler tools.

TABLE 3.2-3 Specialized language and compiler tools standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification (Spec. 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C436 (9/94)	Emerging (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (adopts ISO/IEC 9945-2:1993)	FIPS PUB 189:1994	Informational (Approved)
NPC	IEEE	POSIX, Part 2: Shell and Utilities - (Additional Utilities)	P1003.2b	Emerging (Draft)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.2.1.3.2 Alternative specifications. The following specifications are also available:

a. X/Open (formerly a USL specification): SVR4.

b. Berkeley 4.3 Unix.

c. GNU Tools, debuggers, other utilities, compilers, and specialized languages (programs from the Free Software Foundation).

d. BISON YACC PD work alike from GNU.

e. FLEX LEX PD work alike.

f. Mortice Kern Systems' LEX and YACC tools.

g. AFLEX and YACC (ACADIA PROJECT tools that generate Ada code).

h. OSF: OSF/1's "lint" (C language program checker), "m4" (Expand macro definitions), "ld" (Link editor for object files), "as" (Assembler).

3.2.1.3.3 Standards deficiencies. IEEE 1003.2/ISO/IEC 9945-2 lacks most of the programming language and compiler facilities present in XPG4, SVID, and OSF/1, such as the link editor ("ld"), macro definition expander ("m4"), the assembler ("as"), the C language program checker ("lint"), and the C program beautifier ("cb"). These utilities are important enough that most of them are supported by the consortia.

Operating system-based software development tool standards lack most traditional UNIX-based software development utilities. More than 40 of these software development utilities exist. IEEE1003.2 and 1003.2a combined support only seven utilities.

POSIX lacks the most important, most widely desired of the software development utilities -- the Source Code Control System (SCCS) for version control.

The SVID supports a large number of software development utilities not existing in X/Open or OSF/1.

3.2.1.3.4 Portability caveats. The IEEE 1003.2 standard method for calling the compiler to compile standard C programs is "c89" compared to the "cc" command traditionally used to call the compiler.

Incompatibility errors due to inconsistent data types may creep into programs and reduce their portability across different machines and with different applications because the IEEE 1003.2 standard does not support "lint," the traditional C language program data-type checker. Although C language program checkers may be bundled with different vendors' systems, user portability is reduced, because no standard interface exists for invoking or using these program checkers.

The POSIX "awk" utility differs from traditional awk implementations and specifications because of POSIX changes made to support internationalized programs.

The options specified in the IEEE 1003.2 "awk" are different from any specified by X/Open, the SVID, and OSF/1. X/Open and the SVID specify the same options, but these are not the same as those specified by OSF/1.

Most of the UNIX-based tools related to software development are licensed by AT&T, while the others are based on Berkeley UNIX and licensed from U.C. Berkeley. These tools are not necessarily compatible. The incompatibility almost always affects the interfaces and programmer portability, but does not necessarily affect source code portability.

3.2.1.3.5 Related standards. The NIST Integrated Software Engineering Environment (ISEE) reference model discusses operating system-based software development tools.

3.2.1.3.6 Recommendations. ISO/IEC 9945-2 as profiled by FIPS 189 is recommended for language and compiler tools.

3.2.2 Software life cycle processes. The standards listed below identify the software life cycle process. This is the process that begins when a software product is conceptualized and ends when the software is no longer available for use. It includes a set of activities, methods, practices, and transformations that are used to develop and maintain software and the associated products (e.g., project plans, design documents, code, test cases, and user manuals). The software life cycle typically includes a concept phase, requirements phase, design phase, implementation phase, test phase, installation and checkout phase, operation and maintenance phase, and eventually the retirement phase.

3.2.2.1 Software life cycle. This section presents standards for the overall process rather than concentrating on single aspects of the cycle.

3.2.2.1.1 Standards. Table 3.2-4 presents standards for software life cycle processes.

TABLE 3.2-4 Software life cycle standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Software Life Cycle Processes	12207:1995	Adopted (Approved)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
NPC	ANSI/IEEE	Developing Software Life Cycle Processes	1074:1992	Informational (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
GPC	DOD	Defense System Software Development	DOD-STD-2167A	Informational (Superseded)
GPC	DOD	DOD Automated Information Systems (AIS) Documentation Standards	DOD-STD-7935A	Informational (Superseded)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

3.2.2.1.2 Alternative specifications. No other specifications are known.

3.2.2.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.2.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.2.1.5 Related standards. The NIST ISEE reference model discusses operating system-based software development tools.

3.2.2.1.6 Recommendations. The adopted standards are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

3.2.2.2 Software configuration management. (This BSA appears both in part 2 and part 9.) Configuration management is the process of applying administrative and technical procedures throughout the software life cycle to identity, define, and baseline configuration items for software in a system; control modifications and releases of the items; record and report the status of the items and modification requests; ensure the completeness and correctness of the items; and control storage, handling, and delivery of the items. This includes activities employed by the developer to identify entities (such as computer files, documents, Computer Software Configuration Items) whose version and status are to be tracked and controlled, to apply such controls, to keep records of these controls, and to audit that these controls are being applied.

3.2.2.2.1 Standards. Table 3.2-5 presents standards for software configuration management.

TABLE 3.2-5 Software configuration management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
NPC	EIA	National Consensus Standard for Configuration Management	IS-649	Adopted (Approved)
NPC	ANSI/IEEE	Software Configuration Management	1042:1987	Informational (Approved)
NPC	ANSI/IEEE	Software Configuration Management Plans	828:1990	Informational (Approved)
GPC	NIST	Guideline for Software Documentation Management	FIPS PUB 105:1984	Informational (Approved)
GPC	DOD	Configuration Management	MIL-STD-973(I3): 1995	Informational (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

3.2.2.2.2 Alternative specifications. The following additional guidance document is also available: Guidelines for Configuration Management (MIL-HDBK-761), although it is used with MIL-STD-973(I3): 1995, which will most likely be canceled.

3.2.2.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.2.2.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.2.2.5 Related standards. None.

3.2.2.2.6 Recommendations. The adopted standards are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

3.2.2.3 Documentation standards. Documentation standards provide the process for recording information produced by a life-cycle process or activity. The process contains the set of activities that plan, design, develop, edit, distribute, and maintain those documents needed by managers, engineers, and users of the system or software for configuration management and system life cycle support.

3.2.2.3.1 Standards. Table 3.2-6 presents standards for documentation.

TABLE 3.2-6 Documentation standards standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
GPC	NIST	Guideline for Software Documentation Management	FIPS PUB 105:1984	Informational (Approved)
IPC	ISO	Documentation Symbols and Conventions for Data, program and System Flowcharts, Program Network Charts, and System Resources Charts	5807:1985	Informational (Approved)
IPC	ISO	Program Flow for Processing Sequential Files in Terms of Record Groups	6593:1985	Informational (Approved)
NPC	IEEE	Software Test Documentation	829:1983	Informational (Approved)
IPC	ISO	User Documentation and Cover Information for Consumer Software Packages	9127:1988	Informational (Approved)
IPC	ISO	Program Constructs and Conventions for Their Representation	8631:1989	Informational (Approved)
NPC	ANSI/IEEE	Recommended Practice for Software Design Descriptions	1016:1987	Informational (Approved)
NPC	IEEE	Taxonomy for Software Engineering Standard	1002:1987	Informational (Approved)
IPC	ISO	Guidelines for the Documentation of Computer-based Application Systems	6592:1985	Informational (Approved)
NPC	ANSI/ANS	Guidelines for the Documentation of Digital Computer Systems	10.3:1986	Informational (Approved)
NPC	IEEE	Software User Documentation	1063:1987	Informational (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
GPC	DOD	Defense System Software Development	DOD-STD-2167A	Informational (Superseded)
GPC	DOD	DOD Automated Information Systems (AIS) Documentation Standards	DOD-STD-7935A	Informational (Superseded)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Defense System Software Quality Program	MIL-STD-2168	Informational (Canceled)

3.2.2.3.2 Alternative specifications. No other specifications are known.

3.2.2.3.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.2.3.4 Portability caveats. Although they do not provide software portability, these standards can be used to facilitate program and design portability, as well as facilitating the development of user documentation.

3.2.2.3.5 Related standards. None.

3.2.2.3.6 Recommendations. The adopted standard is recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

3.2.2.4 Joint reviews. Joint reviews are processes or meetings involving representatives of both the acquirer and the developer, during which the developer presents the status and software products of a life-cycle activity or a phase of a project to the acquirer for comment and approval. Joint reviews are conducted at both the management and technical levels throughout the life of the contract.

3.2.2.4.1 Standards. Table 3.2-7 presents standards for joint reviews.

TABLE 3.2-7 Joint reviews standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
NPC	ANSI/IEEE	Software Reviews and Audits	1028:1988	Adopted (Approved)
NPC	IEEE	Trial USE Standard for Applications and Management of the Systems Engineering Process	1220:1994	Informational (Approved)
NPC	EIA	Systems Engineering	632:1994	Informational (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

3.2.2.4.2 Alternative specifications. No other specifications are known.

3.2.2.4.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.2.4.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.2.4.5 Related standards. None.

3.2.2.4.6 Recommendations. The adopted standards are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base

standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

For other related information, consult ANSI/IEEE 1028.

3.2.2.5 Software requirements. Software requirements standards cover the creation, manipulation, and representation of requirements. They may include software capabilities, data elements, internal and external software interfaces, system software and hardware configuration items that communicate with software components, and system states and modes within which the specific software executes. A software requirement is a condition or capability that must be met by software that a user needs to solve a problem or achieve an objective.

3.2.2.5.1 Standards. Table 3.2-8 presents standards for software requirements.

TABLE 3.2-8 Software requirements standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
NPC	ANSI/IEEE	Software Requirements Specifications	830:1984	Adopted (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
GPC	DOD	Defense System Software Development	DOD-STD-2167A	Informational (Superseded)
GPC	DOD	DOD Automated Information Systems (AIS) Documentation Standards	DOD-STD-7935A	Informational (Superseded)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

3.2.2.5.2 Alternative specifications. No other specifications are known.

3.2.2.5.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.2.5.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.2.5.5 Related standards. None.

3.2.2.5.6 Recommendations. The adopted standards are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC

12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

For other related information, consult ANSI/IEEE 830.

3.2.2.6 Software design. These software design standards provide the capability to capture, represent, create, analyze, and refine the design attributes of the software components of a system or subsystem. Their attributes can be the structure or functionality of the software or other characteristics such as user interface design or performance considerations. Software designs are typically dependent on a set of requirements. They describe interrelationships of software components, including interfaces, invocation parameters, data elements, and the states and modes within which the specific software sub-components execute. The outcome of the software design includes definition of the software components and subcomponents.

3.2.2.6.1 Standards. Table 3.2-9 presents standards for software design.

TABLE 3.2-9 Software design standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
NPC	[illegible]	Trial Use Standard - Standard for Information Technology [illegible]ife-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
NPC	IEEE	[illegible] for Software Design Descriptions	1016.1:1993	Informational (Approved)
NPC	ANSI/IEEE	Reco[illegible]ctice for Software Design Descriptions	1016:1987	Informational (Approved)
NPC	ANSI/IEEE	[illegible] Practices for Ada as a Program Design Language	990:1987	Informational (Approved)
GPC	DOD	Defense System Software Development	DOD-STD-2167A	Informational (Superseded)
GPC	DOD	DOD Automated Information Systems (AIS) Documentation Standards	DOD-STD-7935A	Informational (Superseded)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

3.2.2.6.2 Alternative specifications. No other specifications are known.

3.2.2.6.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.2.6.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.2.6.5 Related standards. None.

3.2.2.6.6 Recommendations. The adopted standard is recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

3.2.2.7 Software management indicators. (This BSA appears both in part 2 and part 9.) Software management indicators aid in managing the software development process. Various measurements of both software products and software processes are available. Product measures(such as lines of code, function points, etc.) are often associated with the product specification and should be used as management indicators throughout the product life cycle. Process measures(such as software trouble reports) should be tracked to determine whether the software development process is within statistical control limits. Key indicators should be identified in the software development plan, and the developer should then collect, analyze, interpret, take corrective actions, and report on the selected key management indicators.

3.2.2.7.1 Standards. Table 3.2-10 presents standards for software management indicators.

TABLE 3.2-10 Software management indicators standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
IPC	ISO/IEC	Quality Characteristics and Guidelines for Their Use	9126:1991	Adopted (Approved)
NPC	IEEE	Use of Standard Measures to Produce Reliable Software	982.2:1988	Informational (Approved)
NPC	IEEE	Standard Dictionary of Measures to Produce Reliable Software	982.1:1988	Informational (Approved)
NPC	IEEE	Software Productivity Metrics	1045:1992	Informational (Approved)
NPC	IEEE	Software Quality Metrics Methodology	1061:1992	Informational (Approved)
IPC	ISO/IEC	Software Life Cycle Processes	12207:1995	Informational (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

3.2.2.7.2 Alternative specifications. For additional metrics information, consult the following documents:

a. Metrics for I-CASE Pilot Project (MIPP) Program, Metrics Reporting Guidebook, (prepared by Mitre Corporation, 27 May 1994, for DISA/JIEO/CIM/TXEM).

b. Practical Software Measurement: A Guide to Objective Program Insight, Draft 12 April 1995.

c. Streamlined Integrated Software Metrics Approach (SISMA) Guidebook; Application of STEP Metrics, (prepared by Software Productivity Solutions, Indialantic, FL 32903, 12 July 1993, for the U.S. Army).

d. Software Measurement Guidebook, (prepared by the Software Productivity Consortium Services Corporation, December 1992, Herndon VA, for DARPA).

3.2.2.7.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.2.7.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.2.7.5 Related standards. Related software management guidance can be found in the Software Engineering Institute's Capability Maturity Model (CMM). The Software Engineering Institute's CMM provides guidance on how to gain control of the software development and maintenance processes. The CMM has defined an evaluation procedure, the CMM Based Appraisal (CBA), as a means of identifying the risks associated with potential contractor performance. Diagnostic tools based on the CMM have been deployed. One of those tools, the Software Capability Evaluation(SCE), is designed to be used by an acquiring organization to either identify process risks associated with a particular proposal during the source selection or to monitor the risk-reducing process improvements during the contract execution.

3.2.2.7.6 Recommendations. The adopted standards are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. MIL-STD-498 contains requirements for security and privacy for software development and documentation. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for

transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

For other related information, consult ISO/IEC 9126. Appropriate standards should be selected based on software metrics requirements.

3.2.2.8 Software testing and product evaluation. Software testing and evaluation standards support the test and evaluation of software systems. Testing is performed on individual software components (unit testing), on collections of software components (integration testing), and on complete software systems (system testing). Evaluation includes in-process software evaluation, final software product evaluation, and independent evaluation activities to ensure the functional completeness of the configuration items against their requirements and the physical completeness of the configuration items (whether its design and code reflect an up-to-date technical description).

3.2.2.8.1 Standards. Table 3.2-11 presents standards for software testing and product evaluation.

TABLE 3.2-11 Software testing and product evaluation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
NPC	ANSI/IEEE	Software Verification and Validation Plans	1012:1987	Adopted (Approved)
NPC	ANSI/IEEE	Software Test Documentation	829:1983 (R1991)	Adopted (Approved)
NPC	ANSI/IEEE	Software Unit Testing	1008:1987	Adopted (Approved)
NPC	IEEE	Guide for Software Verification and Validation Plans	1059:1993	Informational (Approved)
GPC	NIST	Guide for Verification and Validation Plans (Adopts ANSI/IEEE 1012:1987)	FIPS PUB 132:1987	Informational (Approved)
IPC	ISO/IEC	Software Life Cycle Processes	12207:1995	Informational (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
GPC	DOD	Defense System Software Development	DOD-STD-2167A	Informational (Superseded)
GPC	DOD	DOD Automated Information Systems (AIS) Documentation Standards	DOD-STD-7935A	Informational (Superseded)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

3.2.2.8.2 Alternative specifications. No other specifications are known.

3.2.2.8.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.2.8.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.2.8.5 Related standards. None.

3.2.2.8.6 Recommendations. The adopted standards are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

For other related information, consult ANSI/IEEE 829, ANSI/IEEE 1008, and ANSI/IEEE 1012.

3.2.2.9 Software quality assurance. Software quality assurance standards provide a planned and systematic pattern of all actions necessary to provide adequate confidence that a software work product conforms to established technical requirements. Further, it provides a set of activities designed to evaluate the process by which software work products are developed and maintained.

3.2.2.9.1 Standards. Table 3.2-12 presents standards for software quality assurance.

TABLE 3.2-12 Software quality assurance standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
IPC	ISO	Model for Quality Assurance in Design, Development, Production, Installation and Servicing	9001:1994	Adopted (Approved)
NPC	ANSI/IEEE	Software Quality Assurance Plans	730.1:1989	Adopted (Approved)
IPC	ISO	Quality Management and Quality Assurance Standards - Part 3: Guidelines for Application of ISO 9001 to the Development, Supply and Maintenance of Software	9000-3:1991 (Corrected and Reprinted - 1993)	Adopted (Approved)
NPC	IEEE	Software Quality Management Systems, Part 1: Requirements	1298:1992	Adopted (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
GPC	DOD	Defense System Software Development	DOD-STD-2167A	Informational (Superseded)
GPC	DOD	DOD Automated Information Systems (AIS) Documentation Standards	DOD-STD-7935A	Informational (Superseded)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)
GPC	DOD	Defense System Software Quality Program	MIL-STD-2168	Informational (Canceled)

3.2.2.9.2 Alternative specifications. No other specifications are known.

3.2.2.9.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.2.9.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.2.9.5 Related standards. None.

3.2.2.9.6 Recommendations. The adopted standards are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

For other related information, consult ANSI/IEEE 730, ISO 9001, ISO 9000-3 and IEEE 1298.

3.2.2.10 Software problem categories/priorities. These standards provide the developer with a structured format to prepare a corrective action and process improvement system for software development. They also provide a procedure for handling all problems detected and changes recommended in development products after they have been released for software product evaluation. This includes the classification by category and priority of such problems.

3.2.2.10.1 Standards. Table 3.2-13 presents standards for software problem categories and priorities.

TABLE 3.2-13 Software problem categories/priorities standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
NPC	IEEE	Classification for Software Anomalies	1044:1993	Adopted (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
GPC	DOD	Defense System Software Development	DOD-STD-2167A	Informational (Superseded)
GPC	DOD	DOD Automated Information Systems (AIS) Documentation Standards	DOD-STD-7935A	Informational (Superseded)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

3.2.2.10.2 Alternative specifications. No other specifications are known.

3.2.2.10.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.2.10.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.2.10.5 Related standards. None.

3.2.2.10.6 Recommendations. The adopted standards are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC

12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

For other related information, consult ANSI/IEEE 1044.

3.2.2.11 Software safety. (This BSA appears in both Part 2: Software Engineering and Part 9: System Management.) These standards provide procedures for identifying as safety-critical those CSCIs or portions thereof whose failure could lead to a hazardous system state (one that could result in death, injury, loss of property, or environmental harm). The developer shall develop a safety assurance strategy, including both tests and analyses, to assure that the requirements, design, implementation, and operating procedures for the identified software minimize or eliminate the potential for hazardous conditions. The objective is to eliminate hazards, and reduce the associated risk to a level of acceptability to the managing activity.

3.2.2.11.1 Standards. Table 3.2-14 presents standards for software safety.

TABLE 3.2-14 Software safety standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	System Safety Program Requirements	MIL-STD-882C: 1996	Adopted (Approved)
NPC	IEEE	Software Safety Plans	1228:1994	Informational (Approved)

3.2.2.11.2 Alternative specifications. No other specifications are known.

3.2.2.11.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.2.11.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.2.11.5 Related standards. None.

3.2.2.11.6 Recommendations. MIL-STD-882C is recommended.

3.2.2.12 Software support. The standards listed below identify those activities that take place to ensure that software installed at user sites continues to perform as intended and fulfill its intended role in system operation. Software support includes software maintenance, aid to users, and related activities.

3.2.2.12.1 Standards. Table 3.2-15 presents standards for software support.

TABLE 3.2-15 Software support standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
NPC	IEEE	Software Maintenance	1219:1993	Adopted (Approved)
GPC	NIST	Guideline on Software Maintenance	FIPS PUB 106:1984	Informational (Approved)
GPC	DOD	Mission Critical Computer Resources Software Support	MIL-HDBK-347:1990	Informational (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

3.2.2.12.2 Alternative specifications. No alternate specifications are known.

3.2.2.12.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.2.12.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.2.12.5 Related standards. MIL-HDBK-347, Mission- Critical Computer Resources Software Support, provides related information.

3.2.2.12.6 Recommendations. The adopted standards are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base

standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

For other related information, consult ANSI/IEEE 1219.

3.2.2.13 Software distribution. (This BSA appears both in part 2 and part 9.) Software distribution and installation services comprise utilities for packaging, installing, and distributing software for use on heterogeneous and potentially incompatible systems. These services will enable network managers to transmit software to any stand-alone or networked system, regardless of the media used for distribution. Standards for software distribution in a system provide a standardized layout for distributing and installing software in a single system or network. They explicitly define each phase of software distribution, installation, and configuration--covering such distribution media as disks, tapes, and CD-ROM.

3.2.2.13.1 Standards. Table 3.2-16 presents standards for software distribution.

TABLE 3.2-16 Software distribution standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	POSIX System Administration - Part 2: Software Administration (former P1003.7.2)	1387.2:1995	Adopted (Approved)
CPC	X/Open	Single UNIX Specification (Spec. 1170)	T908: 1995	Emerging (Approved)
CPC	X/Open	Systems Management: Distributed Software Administration (XDSA)	P429:1997	Informational (Approved)

3.2.2.13.2 Alternative specifications. The following specifications are also available:

a. Hewlett-Packard: "swinstall" and "swpackage" systems.
b. USG: SVR4-based "pkgadd" system.
c. Santa Cruz Operation (SCO): "custom+" system.

3.2.2.13.3 Standards deficiencies. IEEE 1387.2 does not provide for acting upon log files in remote file systems. No Ada bindings are available for software distribution standards.

3.2.2.13.4 Portability caveats. Although the IEEE 1387.2 standard is based on Hewlett-Packard's "swinstall" and "swpackage" systems, the standard has modified the specifications so that they are not exactly like the HP systems.

3.2.2.13.5 Related standards. The following standards are related to software distribution or software distribution standards:

a. ISO/IEC JTC1 IS 9595:1991: Common Management Information Service (CMIS).

b. ISO/IEC JTC1 IS 9596:1991: Common Management Information Protocol (CMIP).

c. ISO/IEC IS 11578: 1996, Information Technology - Open Systems Interconnection - Remote Procedure Call (RPC).

d. Internet RFC 1155 (STD 17): Structure and Identification of Management Information for TCP/IP-based Internets.

e. Internet RFC 1157 (STD 15): A Simple Network Management Protocol.

f. Internet RFC 1213 (STD 17): Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

g. Network Management Forum: OMNIPoint 1.

3.2.2.13.6 Recommendations. IEEE 1387.2 is recommended.

A new version of the X/Open Single UNIX Specification (Spec. 1170) is expected to be issued in 1997.

3.2.2.14 Software license management. (This BSA appears in both part 2 and part 9.) License management addresses the problem of tracking software licenses in a distributed systems environment. The DME licensing technology includes models that assist users in keeping track of how many software copies are needed and who is using it once it is purchased. Software license management for a system provides license administration, monitoring, and enforcement services that allow more detailed, firm and equitable licensing terms for users, and better protection against illegal software usage for vendors.

3.2.2.14.1 Standards. Table 3.2-17 presents standards for software license management.

TABLE 3.2-17 Software license management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	POSIX System Administration - Part 2: Software Administration (former P1003.7.2)	1387.2:1995	Adopted (Approved)
CPC	X/Open	Systems Management: Distributed Software Administration (XDSA)	P429:1997	Informational (Approved)
CPC	OSF	Distributed Management Environment (DME): License Management (LM) Service	DME LM	Informational (Historic (Not recommended))

3.2.2.14.2 Alternative specifications. The following specifications are also available:

a. Hewlett-Packard: Network License System (NetLS) Version 2.0 on which OSF's DME License Management System (LS) is based.

b. Gradient Technologies: PC Client libraries for license management and PC Ally server, on which DME's License Management PC component is based.

3.2.2.14.3 Standards deficiencies. No Ada bindings exist for any of the configuration management standards or consortia specifications.

3.2.2.14.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.2.2.14.5 Related standards. The following standards are related to license management or license management standards:

a. ISO/IEC JTC1 IS 9595:1991: Common Management Information Service (CMIS).

b. ISO/IEC JTC1 IS 9596:1991: Common Management Information Protocol (CMIP).

c. ISO/IEC IS 11578: 1996, Information Technology - Open Systems Interconnection - Remote Procedure Call (RPC).

d. Internet RFC 1155 (STD 17): Structure and Identification of Management Information for TCP/IP-based Internets.

e. Internet RFC 1157 (STD 15): A Simple Network Management Protocol.

f. Internet RFC 1213 (STD 17): Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

g. Network Management Forum: OMNIPoint 1.

3.2.2.14.6 Recommendations. IEEE 1387.2 is recommended.

3.2.3 Programming languages. Programming languages include all languages represented by the ISO, the European Computer Manufacturers' Association (ECMA), the International Electrotechnical Commission (IEC), the American National Standards Institute (ANSI), the IEEE, NIST, or DOD standards, as well as those used by DOD but not represented by standards. Quotes regarding the number of languages used by DOD range from 50 to 300; however, this volume only includes languages playing major roles in DOD systems and those supporting DOD-Wide goals of economy, interoperability, and portability.

Certification of conformance to the source language specification results in a higher degree of portability across platforms for all languages. Test suites to validate source language standards conformance are available from the NIST, the IEEE, and the Ada Joint Program Office (AJPO). Specific conformance test suites will be addressed for each language covered in this document.

3.2.3.1 Programming language framework. Coverage of language standards is currently limited to those Higher Order Languages (HOL) deemed to represent the majority of Commercial Off The Shelf (COTS) and custom applications used within the DOD. The relevant standards will be listed along with coverage of Standards Deficiencies, Portability Cavects, Tailoring Guidance, Alternative Specifications, Related Standards, and Recommendations for use.

Public Law (PL) 102-172 states, "Notwithstanding any other provisions of law, after 1 June 1991, where cost effective, all Department of Defense software shall be written in the programming language Ada, in the absence of special exemption by an official designated by the Secretary of Defense." The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I) has been designated as the DOD Ada Waiver review authority, with some responsibilities delegated to the services and the Defense Intelligence Agency. (ASD(C3I) Memorandum, 17 April 1992, "Delegations of Authority and Clarifying Guidance on Waivers from the Use of the Ada Programming Language") Software used by the DOD includes Commercial Off-the-Shelf (COTS), Government Off-the-Shelf (GOTS), and new DOD-developed software. New DOD-developed software includes custom applications as well as software to integrate COTS and GOTS. Ada is the preferred software development language for all new and revised DOD-developed software.

3.2.3.1.1 Standards. Table 3.2-18 presents standards for programming languages.

TABLE 3.2-18 Programming language framework standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Ada (Adopts ANSI/ISO/IEC 8652: 1995)	FIPS PUB 119-1: 1995	Adopted (Approved)
NPC/IPC	ANSI/ISO/IEC	Ada-95	8652:1995	Adopted (Approved)
GPC	NIST	Pascal (Adopts ANSI/IEEE 770 X3.97-1983/R1990)	FIPS PUB 109:1985	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	MUMPS (Adopts ANSI/MDC X11.1-1990)	FIPS PUB 125-1:1993	Informational (Approved)
GPC	NIST	BASIC (ANSI X3.113-1987/R1993, reflects major changes, improvements and additions to the BASIC specifications.)	FIPS PUB 68-2:1987/R1993	Informational (Approved)
GPC	DOD (USAF)	JOVIAL (J73)	MIL-STD-1589C: 1996	Informational (Approved)
IPC	ISO/IEC	Ada	8652:1987	Informational (Approved)
NPC/IPC	ANSI/ISO	Programming Languages: C	9899:1992	Informational (Approved)
GPC	NIST	C (Adopts ANSI/ISO/IEC 9899:1992)	FIPS PUB 160:1992	Informational (Approved)
IPC	ISO	FORTRAN-90	1539:1991	Informational (Approved)
NPC	ANSI	FORTRAN-77	X3.9-1978 (R1989)	Informational (Approved)
NPC	ANSI	COBOL	X3. 23: 1993	Informational (Approved)
NPC	ANSI/IEEE	Pascal	770X3.97-1983 (R1990)	Informational (Approved)
IPC	ISO	Pascal	7185:1983	Informational (Approved)
NPC	ANSI	COBOL	X3. 23a: 1989	Informational (Approved)
GPC	NIST	COBOL (adopts ANSI X3.23a: 1989 and X3.23b: 1993)	FIPS PUB 21-4:1995	Informational (Approved)
GPC	DOD (AJPO)	Ada Programming Language	MIL-STD-1815A:1983	Informational (Approved)
IPC	ISO/IEC	C++	SC22 WG22, X3J16	Informational (Draft)
NPC	ANSI/X3J13	Common LISP (X3.226 Programming Language Common LISP)	X3J13/92-101	Informational (Draft)
GPC	NIST	Ada	FIPS PUB 119:1985	Informational (Superseded)

3.2.3.1.2 Alternative specifications. Although many language standards exist other than HOLs listed above, the coverage of languages in this document is limited to those HOLs that represent the most significant percentage of DOD applications.

3.2.3.1.3 Standards deficiencies. Each programming language has its own strengths and weaknesses. Details containing specific language strengths and weaknesses are contained in language rationale, comparison documents, and dissertations external to the standards and this document.

3.2.3.1.4 Portability caveats. Despite the existence of programming language standards, each vendor and platform implementation may contain features not included in the standard. Furthermore, conformance to the standard generally is neither verified nor regulated by the standards community. Therefore, portability of applications written in a specific language depends upon these factors:

a. The extent of conformance of a particular implementation to the standard.
b. The range of operating systems for implementations of the language.
c. The range of hardware suites for implementations of the language.

In all cases, the extent to which application programmers employ nonstandard features is a major factor in determining portability across platforms. Portability across languages also is affected by the factors mentioned, because translation from one source language to another requires more human-intensive effort if nonstandard features are employed. In addition, different source languages often provide different mechanisms for abstracting data and operating on data, and employ different approaches toward interaction with the operating system and hardware. For this reason, when transitioning from any source language to another, reverse engineering from the current specifications is preferred over simple source code translation.

3.2.3.1.5 Related standards. A number of standards exist or are in the definition process for Ada bindings to other components of open systems. Section 3.2.4.1 includes a table which lists these standards.

3.2.3.1.6 Recommendations. The adopted standards are recommended. The following order of preference applies to developing or modifying DOD software applications:

a. Reuse existing government-owned code without modification where significant savings in maintenance and development can be identified.

b. Use COTS software that is conformant with DOD-adopted standards without modifications, where significant savings in maintenance costs can be documented, although DOD will not maintain COTS software.

c. Modify existing Ada code.

d. Develop new code using Ada. Develop or modify non-Ada legacy code.

If a COTS software product is being procured, rather than a software product being developed, the programming language used by the developer of the COTS product is not of vital concern, unless it is expected the COTS product will be included as part of another application. If the COTS software will be incorporated into a larger application, one must carefully consider the extent of dependency upon the COTS-provided functions and have an understanding of the options in the event the vendor terminates support for the application.

3.2.3.2 Ada. Ada is a general purpose and systems programming language designed with an emphasis on reliability, readability, and maintainability. Originally intended for embedded, real-time systems development, use of Ada has extended into the MIS community and is appropriate for a broad range of applications areas. Ada is a language that enforces modern software engineering principles of data abstraction, information hiding, and modularity. Ada supports reusability though several features of the language: explicit support for program units; separation of interface specifications from the hidden body; strong, user definable typing of data and operators; overloading of function and procedure names; and generic units to supply parameterized code templates. The Ada standard (Ada-95) brings the language into line with newer software engineering concepts including extensions to improve support for real-time systems, object-oriented features, and mega-programming.

3.2.3.2.1 Standards. Table 3.2-19 presents standards for Ada.

TABLE 3.2-19 Ada standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Ada (Adopts ANSI/ISO/IEC 8652: 1995)	FIPS PUB 119-1: 1995	Adopted (Approved)
NPC/IPC	ANSI/ISO/IEC	Ada-95	8652:1995	Adopted (Approved)
IPC	ISO/IEC	Ada	8652:1987	Informational (Approved)
GPC	DOD (AJPO)	Ada Programming Language	MIL-STD-1815A:1983	Informational (Approved)
GPC	NIST	Ada	FIPS PUB 119:1985	Informational (Superseded)

3.2.3.2.2 Alternative specifications. No other specifications are known.

3.2.3.2.3 Standards deficiencies. The most significant deficiencies in Ada-83 which have been addressed by Ada-95 are the inclusion of objects into the language, a more robust treatment of tasking, more flexible response to interrupts, an explicit definition of higher mathematical functions, and the explicit inclusion of bindings to other languages. All documented deficiencies in the Ada-83 standard are included in the Ada-95 Project Report, which is available through the Ada Information Clearinghouse.

3.2.3.2.4 Portability caveats. Within the limits of the features tested under the ACVC, Ada source code is completely portable across all compilers and hardware/operating system platforms. Portability problems will be more likely to exist when changing compiler vendors than when moving across platforms supported by a single compiler vendor. In particular, vendor-to-vendor portability problems can result from the use of Ada language components which are specified as implementation dependent (e.g., PRAGMAs). Special purpose libraries (e.g., support for DOS functionality) also are a major source of portability problems. In general, automated source translation software exists to resolve the major portion of these remaining incompatibilities.

Efforts are underway to increase the depth and breadth of future releases of the ACVC so as to further reduce compiler and platform dependencies.

3.2.3.2.5 Related standards. SPC-91061-N, Ada Quality and Style: Guidelines for Professional Programmers, Version 2.01.01, 1991, is related to Ada. Similar to other programming languages, Ada style guides are desirable for their contribution to the quality and consistency of Ada code. The AJPO has endorsed this Software Productivity Consortium (SPC) publication as a suggested Ada Style Guide for DOD programs. This guide, available from the Ada Joint Program Office, contains more information on the handling of implementation-dependent features.

3.2.3.2.6 Recommendations. The use of the Ada (ANSI/ISO/IEC 8652: 1995, as adopted by FIPS PUB 119-1: 1995) programming language (Ada-95) is mandated for new procurement. (See section 3.2.3.2 for details). Initially, there may be productivity limitations due to the absence of bindings and support tools for Ada-95. Transition of software from Ada-83 will not be required unless the availability of Ada-83 compilers becomes a problem or additional functionality supported by Ada-95 is required by the target system.

Implementation-defined features and other features which are not standard to the Ada programming language must be avoided. The Ada Quality and Style: Guidelines for Professional Programmers, available from the AJPO, contains more information on the handling ofimplementation-dependent features. This guideline can be used as a tailoring reference for many of the areas discussed in the following sections about Ada.

Although upward compatibility was a major design consideration for Ada-95, incompatibilities are likely betweer Ada-83 and Ada-95. When considering the transition to Ada-95, the Ada-83 system design and implementation should be assessed in view of the final documented incompatibilities. Discrepancies between Ada-83 and Ada-95 have been identified and suggested coding practices and source code modifications have been identified and tested, allowing recompilation of existing Ada-83 code by Ada-95 compilers. Information on these coding practices can be found in the Ada Style Guide and the Ada-95 Project Report, both available from the AJPO. A comprehensive transition to Ada-95 cannot be undertaken until Ada-95 compilers pass validation testing.

Despite these limitations, the ASD C3I in a Memorandum of 9 March 1994, encourages early use of Ada9X (Ada-95). The use of available unvalidated Ada-95 compilers is encouraged. Unvalidated Ada-95 compilers may be used for:

a. Research and development programs (6.1, 6.2, and 6.3A appropriations).

b. Proof of concept prototypes, so long as any subsequent system is delivered using validated Ada-95 compilers.

c. System development programs, so long as the systems are delivered using validated Ada-95 compilers, in accordance with the validation procedures issued by the AJPO.

Early use of Ada-95 provides access to the language's many enhancements, including full support for object-oriented programming, enhancements for realtime programming, and interfacing to other languages.

In systems where COTS software is to be used extensively, the amount of non-COTS code to be developed and the interfaces to the COTS software need to be considered when evaluating the long-term cost/benefits of using another HOL versus Ada as a development language. In most cases, developing Ada links to existing bindings has proven to be an effective development method. Furthermore, in applications where concurrent processing is required, the inherent implementation of concurrent methods by Ada is preferable to another HOL, since concurrent processing in other HOLs is handled often by invoking operating system calls. The concurrency methods in Ada are independent of the operating system.

3.2.3.3 C, C++. C is a systems programming language which has been adopted for widespread use as a general purpose language in developing commercial applications. C is a relatively "low level" language which deals with basic computer objects, such as characters, numbers, and addresses, and does not inherently provide operations to deal with composite objects, such as strings, sets, lists. Library units have been added to the language to partially support functionality of such objects. ANSI C is strongly typed and is an implicitly integer language, i.e., untyped functions and variables are assumed to be integer. The popularity of C derives from its support for low level control and interaction with peripherals and the operating system, the highly efficient code which is generated by modern C compilers, and the wide availability of such compilers.

C++ is an Object-Oriented Programming (OOP) superset of the C language. Existing C context is fully supported by C++ compilers, with additional support for data abstraction, encapsulation, object classes, inheritance (and multiple inheritance), polymorphism, and overloading. While considered a general purpose language, its core area of application is systems programming. C++ was developed to encourage good software engineering practice and the development of reuse libraries in the development of larger applications.

3.2.3.3.1 Standard. Table 3.2-20 presents standards for C.

TABLE 3.2-20 C, C++ standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC/IPC	ANSI/ISO	Programming Languages: C	9899:1992	Adopted (Approved)
GPC	NIST	C (Adopts ANSI/ISO/IEC 9899:1992)	FIPS PUB 160:1992	Adopted (Approved)
IPC	ISO/IEC	C, Amendment 1: Integrity Addendum	9899:1994 PDAM	Informational (Draft)
IPC	ISO/IEC	C++	SC22 WG22, X3J16	Informational (Draft)

3.2.3.3.2 Alternative specification. The original definition of the C language by Kernighan & Ritchie (K&R) is considered by many as "THE" specification of the C language. This specification is NOT coincident with the ANSI/ISO/IEC standard.

3.2.3.3.3 Standard deficiencies. While there is an existing ISO standard for the C language that supports and is supported by the IEEE 1003.1 C Language Binding to POSIX, the intrinsically low level nature of C and lack of direct support for modern software engineering approaches and discipline make it an undesirable language for the development of large, general purpose DoD software applications. C can offer benefits when used specifically for systems level programming, when required for especially compact or efficient code, or when used at an interfacing level where direct bindings to high level languages do not exist. The use of C in general purpose applications is often justified by a large population of "trained" C programmers; however, useful C code on

large projects can only be developed by those few, highly self-disciplined, virtuoso, software engineers.

C++ is an emerging language with no current standard, although AT&T's Bell Labs, where the language originated and where development has continued, have produced defining documentation for the language, including The C++ Programming Language by Bjarne Stroustrup, one of the principal developers of the language. The lack of a current compiler standard makes C++ source code portability problematic. This is further complicated by the current popularity of C++ in the development of Graphical User Interface (GUI) based applications, which rely heavily on compiler vendor-specific interface libraries. Because the mechanics of the C language are embedded in C++, it is susceptible to many of the above noted difficulties with C, despite the introduction of OOP software engineering into the language.

3.2.3.3.4 Portability caveats. Differences between ANSI C and K&R C can be significant and can affect portability. Furthermore, the lack of a current compiler standard makes C++ source code portability problematic.

3.2.3.3.5 Related standards. No related standards to C or C++ are known.

3.2.3.3.6 Recommendations. ANSI/ISO/IEC 9899:1992 and FIPS PUB 160:1992 are the recommended standards for legacy systems written in C and C++ languages. Use of C++ for the development of critical systems applications is not recommended.

3.2.3.4 FORTRAN. FORTRAN, which is an acronym for FORMula TRANslating system, is a programming language originated in 1954 and designed to support scientific and engineering applications requiring calculation-intense computing. FORTRAN is the oldest surviving HOL and existing applications may have been developed in several dialects of the language: FORTRAN IV dates to 1962 and was standardized in 1966 (sometimes called FORTRAN 66) due to the large number of non-portable variants of FORTRAN IV which had been developed; FORTRAN 77 was a major extension to FORTRAN which introduced C and Pascal control structures into the language to limit the FORTRAN "spaghetti code" problem; and FORTRAN 90 is a further extension to the language to include flexible, modern data structures into FORTRAN. Most FORTRAN legacy programs have been developed under FORTRAN IV and FORTRAN 77. FORTRAN 90 has not gained wide spread acceptance within the FORTRAN programming community.

FORTRAN supports data typing by providing primarily numeric data types (INTEGER, REAL, DOUBLE PRECISION, COMPLEX), LOGICAL, and CHARACTER to support characters and strings (as arrays of CHARACTERs). Through FORTRAN 77, arrays were the only composite data type supported. More advanced data types are supported in the FORTRAN 90 standard. FORTRAN 77 does not support dynamic data structures or address pointers. I/O library by FORTRAN includes extensive I/O capabilities explicitly in the definition of the language. Additionally, a standard defining a FORTRAN 77 binding to POSIX has been developed by the IEEE as the 1003.9 standard. FORTRAN has explicit support for high level mathematical functionality, unlike C and Ada, where mathematical library units are defined externally to the base language. Basic logical operations are fully supported in FORTRAN. The LOGICAL type is functionally equivalent to the Boolean type in Ada. The "ELSE" construct was not supported in FORTRAN prior to FORTRAN 77. A CASE or SWITCH logical control mechanism is not supported in FORTRAN. Fixed point arithmetic is not explicitly supported in FORTRAN. Floating point is supported though the REAL and DOUBLE PRECISION types. FORTRAN supports implicit typing of REAL and INTEGER variables. Timing functionality, either simple or for concurrent operation, is not supported by FORTRAN. FORTRAN contains no object-oriented capabilities, though work in this area is being pursued by ANSI.

FORTRAN is included in the ITSG discussion of programming languages in deference to the large amount of available legacy engineering and scientific software written in the language.

3.2.3.4.1 Standards. Table 3.2-21 presents standards for FORTRAN.

TABLE 3.2-21 FORTRAN standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI	FORTRAN-90	X3.198-1992	Adopted (Approved)
IPC	ISO	FORTRAN-90	1539:1991	Adopted (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	FORTRAN-77 (adopts ANSI X3.9)	FIPS PUB 69-1: 1985	Adopted (Approved)
NPC	ANSI	FORTRAN-77	X3.9-1978 (R1989)	Adopted (Approved)
NPC	ANSI	Object FORTRAN	TBD	Informational (TBD)

3.2.3.4.2 Alternative specifications. The so-called "VAX Extensions" to FORTRAN 77 are widely supported. The IBM Systems Application Architecture (SAA) FORTRAN binding to SQL is also available, but is proprietary.

3.2.3.4.3 Standards deficiencies. FORTRAN 90 has not gained widespread acceptance in the FORTRAN programming community. Vendors have selectively implemented FORTRAN 90 attributes into their compilers. The few existing FORTRAN bindings to OSE component subsystems are based upon FORTRAN 77. FORTRAN 77 does not supply a fully modern set of data types, control statements, and modularity support. In FORTRAN, the EQUIVALENCE statement can be used to break explicit typing of data.

Because of the nature of the language, the IEEE 1003.9 specification of the FORTRAN binding to POSIX is less stringent and more vendor and implementation dependent than IEEE 1003.1 and 1003.5 (C and Ada bindings, respectively).

3.2.3.4.4 Portability caveats. Older versions of FORTRAN, particularly FORTRAN IV, exhibit many portability problems, hence, the advent of FORTRAN 77. Legacy software written in versions of FORTRAN earlier than FORTRAN 77 can be expected to be difficult to port between platforms or operating systems. Modern compilers have been selective in "choosing" features of FORTRAN 90 to implement. This can cause obvious portability difficulties.

Numeric precision of REAL and DOUBLE PRECISION data types has been a historical trouble spot for porting of FORTRAN source code between platforms. The FORTRAN 77 standard addresses this problem. However, older FORTRAN IV applications may still exhibit these problems.

The use of special features for I/O, such as I/O handling features specific to the hardware, compiler or operating system, can lead to portability problems. FORTRAN IV legacy software can contain OS specific I/O.

Portability of FORTRAN across different operating system and hardware suites is subject to errors brought about by differences between FORTRAN compiler implementations and hardware/operating system internal numerical representations.

3.2.3.4.5 Related standards. Other than the standards referenced above, there are no other standards applicable to FORTRAN for compiler or user-defined data typing. The only standard related to math functions is the IEEE 754 floating point standard.

3.2.3.4.6 Recommendations. ISO1539:1991/ANSI X3.198:1992 and NIST FIPS PUB 69-1/ANSI X3.9:1978 (R1989) are the recommended standards for FORTRAN-based legacy systems. NIST FIPS PUB 69-1 is the recommended standard for legacy FORTRAN development. FORTRAN has been used traditionally for scientific processing. Although FORTRAN-90 contains added capability over FORTRAN-77, it does not contain any capabilities making it preferable to Ada for DOD applications. FORTRAN should not be chosen for the development of new DOD applications and should be used only to maintain legacy software. I/O based on the IEEE 1003.9 specified library is preferred for OSE systems.

3.2.3.5 COBOL. COBOL, an acronym for COmmon Business Oriented Language, is a programming language for use in financial and accounting applications. Created during the early 60s, COBOL is the most widely used language for data processing applications and has an extensive software legacy. It was intended as a design for a common language that would enable programs and programming techniques to be easily shared and transferred between machines. Despite this design goal, COBOL programs are verbose and not truly self documenting, and are difficult to maintain and tend toward "bugginess." COBOL is strictly for data processing applications and has no role as a more general language.

Only two types of variables are recognized by COBOL, numeric and non-numeric. Arrays and records are supported via the COBOL table and record description entry constructs. Dynamic structures are not supported. COBOL has a strong set of file manipulation functions for data processing applications. These functions are intrinsic to the language. COBOL supplies a minimal set of logical and mathematical operations. No advanced mathematical functions are supported. Logical variables are supported in COBOL via testable conditions. IF - ELSE control and relational test operators are supplied. Basic mathematical operations to support financial calculations are supported by COBOL. COBOL is not a real time language. It supports neither simple nor complex (e.g., concurrent) timing functionality. COBOL contains no object-oriented capabilities, though work in this area is being pursued by ANSI.

3.2.3.5.1 Standards. Table 3.2-22 presents standards for COBOL.

TABLE 3.2-22 COBOL standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	COBOL (adopts ANSI X3.23a: 1989 and X3.23b: 1993)	FIPS PUB 21-4:1995	Adopted (Approved)
IPC	ISO	COBOL	1989:1985	Adopted (Approved)
NPC	ANSI	COBOL	X3. 23: 1985	Adopted (Approved)
NPC	ANSI	COBOL	X3. 23a: 1989	Informational (Approved)
NPC	ANSI	COBOL	X3. 23: 1993	Informational (Approved)
NPC	ANSI	Object COBOL	TBD	Informational (Formative)

3.2.3.5.2 Alternative specifications. No other specifications are known.

3.2.3.5.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.3.5.4 Portability caveats. The COBOL language has a design goal of transparent portability of data across platforms. Portability of COBOL across different operating system and hardware

suites is subject to errors brought about by differences between COBOL compiler implementations and hardware/operating system internal numerical representations.

3.2.3.5.5 Related standards. The emerging standard for Object COBOL is referenced in the table above.

3.2.3.5.6 Recommendations. NIST FIPS PUB 21-4/ISO 1989/ANSI X3.23 are the recommended standards for COBOL. COBOL should be included in an OSE only to maintain legacy software. However, Ada has been shown to be effective in these applications as well as less costly to maintain than existing COBOL software. Furthermore, Ada includes features, such as fixed point arithmetic, that have been identified as the cause of usability and portability problems in COBOL legacy applications. The reengineering of COBOL programs to Ada has been proven to be more cost-effective than maintaining the existing systems in the long term.

3.2.3.6 JOVIAL. JOVIAL (Jules' Own Version of the International Algebraic Language) is an ALGOL-like scientific and engineering programming language developed by Jules Schwartz of Systems Development Corp. for the USAF in the 1960s. JOVIAL was the Air Force's solution to the need for a better structured and more stable mathematical language than FORTRAN long before the advent of Ada. JOVIAL includes unique data types for expressing real values.

3.2.3.6.1 Standards. Table 3.2-23 presents standards for JOVIAL.

TABLE 3.2-23 JOVIAL standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD (USAF)	JOVIAL (J73)	MIL-STD-1589C: 1996	Adopted (Approved)

3.2.3.6.2 Alternative specifications. No other specifications are known.

3.2.3.6.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.3.6.4 Portability caveats. Portability problems related to the existing specification are unknown.

3.2.3.6.5 Related standards. No other specifications are known.

3.2.3.6.6 Recommendations. MIL-STD-1589C is the recommended standard for JOVIAL based legacy systems and software. JOVIAL has been used traditionally for real time and scientific processing. The availability of Ada compilers and cross-compilers make Ada a cost-effective alternative. In fact, the USAF has undertaken a policy of converting all useful, existing JOVIAL software into Ada.

3.2.3.7 MUMPS. MUMPS (Massachusetts General Hospital Utility MultiProgramming System) is an advanced, high-level programming language and integrated database used for business applications. It has extensive string handling functionality, making it suitable for databases with large text entries. MUMPS, renamed M during 1993, has been widely used for the computing needs of the medical community. Two major federal systems implemented with MUMPS are the Veterans Affairs' Decentralized Hospital Computer Program (DHCP) and the DOD Composite Health Care System (CHCS). MUMPS originated in 1965 and is based upon the 127 ASCII characters. MUMPS adopts ANSI/MDC X11.1-1995 and is currently being revised. A MUMPS validation suite is available from NTIS.

3.2.3.7.1 Standards. Table 3.2-24 presents standards for MUMPS.

TABLE 3.2-24 MUMPS standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	MUMPS (Adopts ANSI/MDC X11.1-1990)	FIPS PUB 125-1:1993	Adopted (Approved)
NPC	ANSI/MDC	MUMPS	X11.1-1995	Informational (Approved)

3.2.3.7.2 Alternative specifications. No other specifications are known.

3.2.3.7.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.3.7.4 Portability caveats. The MUMPS language is supported on a limited number of platform/operating system combinations.

3.2.3.7.5 Related standards. No other specifications are known.

3.2.3.7.6 Recommendations. The FIPS PUB 125-1 standard is recommended for MUMPS based legacy systems and software. MUMPS provides unique large record length database capabilities not found in other languages. However, currently underway is a development activity to provide a library of Ada units which can supply MUMPS like functionality to software developed in Ada.

3.2.3.8 Simulation languages. Simulation is the representation of selected characteristics of the behavior of one physical or abstract system by another system. In a digital computer system, simulation is done by software; for example, the representation of physical phenomena by means of operations performed by a computer system or the representation of operations of a computer system by those of another computer system.

3.2.3.8.1 Standards. Table 3.2-25 presents standards for simulation langauges.

TABLE 3.2-25 Simulation languages standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
TBD	TBD	GPSS	TBD-GPSS	Informational (TBD)
TBD	TBD	Simscript	TBD-Simscript	Informational (TBD)
TBD	TBD	Simula	TBD-Simula	Informational (TBD)

3.2.3.8.2 Alternative specifications. No other specifications are known.

3.2.3.8.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.3.8.4 Portability caveats. No portability of code can be assumed in the use of these existing specialty simulation languages.

3.2.3.8.5 Related standards. No other specifications are known.

3.2.3.8.6 Recommendations. No standards are recommended for simulation languages. Special simulation languages allow for rapid prototyping and development of quick use simulation tools. Generally such software is not readily maintainable. Use should be limited to proof of concept rapid prototyping, novel algorithm development and demonstration, and limited use simulations which require an extremely short development cycle. Major simulation efforts which require a high order language should be implemented in Ada.

3.2.3.9 Artificial intelligence languages. Artificial Intelligence (AI) languages are a subfield within computer science concerned with developing a technology to enable computers to solve problems (or assist humans in solving problems). The LISP (LISt Processing) language is the most popular one for research in AI. LISP is a high-level, non-numeric language with the syntactic distinction that there is no difference between the treatment of data and instructions. LISP was developed in 1960 and its current, standardized version is referred to as Common LISP.

3.2.3.9.1 Standards. Table 3.2-26 presents standards for artificial intelligence languages.

TABLE 3.2-26 Artificial intelligence languages standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	PROLOG	TBD-PROLOG	Informational (Draft)
NPC	ANSI/X3J13	Common LISP (X3.226 Programming Language Common LISP)	X3J13/92-101	Informational (Draft)
NPC	IEEE	AI-ESTATE	SC 20, PAR 1232	Informational (Draft (CD))
NPC	ANSI	Common LISP Object System (CLOS)	TBD	Informational (Dreft (CD))
NPC	IEEE	Interoperability of Knowledge-Based Systems	TBD-Interoperability of Knowledge-Based Systems	Informational (Formative)

3.2.3.9.2 Alternative specifications. No other specifications are known.

3.2.3.9.3 Standards deficiencies. Deficiencies in the existing standards are unknown. Currently standards are being developed for Common LISP and PROLOG. Common LISP is more popular in the United States and PROLOG is more popular in England and Europe, posing potential interoperability problems.

3.2.3.9.4 Portability caveats. No portability of software written with these languages can be guaranteed.

3.2.3.9.5 Related standards. No other specifications are known.

3.2.3.9.6 Recommendations. No standards are recommended for artificial language standards. The current generation of artificial intelligence languages are laboratory tools useful in the study of AI concepts. Generally such software is not readily maintainable. Use should be limited to proof of concept rapid prototyping, novel algorithm development and demonstration, and general AI research activities.

3.2.3.10 Fourth generation languages. Fourth generation languages (4GLs) are designed to improve the productivity achieved by HOL (third generation) languages and to make computing power available to non-programmers. Features typically include an integrated database management system, query language, report generator, and screen definition facility. Addition features support function, financial modeling, spreadsheet capability, and statistical analysis functions.

3.2.3.10.1 Standards. Table 3.2-27 presents standards for fourth generation languages.

TABLE 3.2-27 Fourth generation languages standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.2.3.10.2 Alternative specifications. The only available specifications are proprietary.

3.2.3.10.3 Standards deficiencies. All 4GLs are proprietary. Therefore, 4GLs have not been standardized, and creation of a 4GL standard is not planned. Furthermore, 4GLs often lack the functionality to define a complete system within their specification language. They are not integrated, making them incapable of linking the various parts of the system. They make inefficient use of machine resources, and are very expensive in terms of hardware requirements and/or software license fees.

3.2.3.10.4 Portability caveats. Portability problems relating to the existing specification are unknown.

3.2.3.10.5 Related standards. The ANSI/ISO/IEC 9075-1992 standard, Database Languages - SQL, is related to 4GLs.

3.2.3.10.6 Recommendations. No standards are recommended for 4GLs. Implementation-defined features and other nonstandard features of the programming language must be avoided. The 4GL situation is improving. For example, AdaSAGE was developed for the government to provide tools and an environment for Ada programmers to develop major nonproprietary systems completely in Ada.

3.2.4 Bindings. Language bindings are interfaces to operating systems, network software, graphical user interfaces, database management systems, and other system software specific to a programming language. Bindings define conventions for accessing functionality of the specified sub-system. Calling conventions include the name of the functional service called, the arguments to be included in the call, the data type of these arguments, the order of the arguments, error conditions which may result, and returned values. Because of the extensive lists of available bindings for some languages, only a small subset of the available bindings will be listed for each language. References to complete listings of bindings for each language are included.

3.2.4.1 Ada bindings. Few Ada bindings currently are implemented, although many standards exist or are in development for Ada bindings to OSE component sub-systems. Due to the importance of the Ada language, many working groups are active in the development of specifications for many such bindings.

3.2.4.1.1 Standards. Table 3.2-28 presents standards for Ada bindings.

TABLE 3.2-28 Ada bindings standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	POSIX Ada Language Interfaces, Part 1: Binding for System API	1003.5:1992	Adopted (Approved)
IPC	ISO	Database Language SQL (same as ANSI X3.135-1992)	9075:1992	Adopted (Approved)
IPC	ISO/IEC	Ada Bindings of PHIGS (binding for Ada-83)	9593-3:1990	Adopted (Approved)
GPC	NIST	PHIGS language bindings - Part 3: Ada (binding for Ada-83)	FIPS PUB 153:1992	Adopted (Approved)
NPC	ANSI	SQL Ada Module Extensions (SAME) (binding for Ada-83)	X3.168-1989	Adopted (Approved)
NPC/GPC	ANSI/NIST	SQL and Ada Bindings (ANSI X3.135:1992) (binding for Ada-83)	X3.135:1992 FIPS 127-2:1993	Adopted (Approved)
IPC	ISO	Interfacing techniques for dialogues with graphical devices(CGI)--Languages Bindings - Part 3: Ada	9638-3:1994	Adopted (Approved)
IPC	ISO/IEC	SQL Ada Module Description Language (SAMeDL), First Edition	12227:1995	Adopted (Approved)
IPC	ECMA	Portable Common Tool Environment (PCTE) - Ada Programming Language Binding	162 (1991)	Informational (Approved)
IPC	ISO	Graphical Kernel System for Three Dimensions (GKS-3D) language bindings - Part 3: Ada (binding for Ada-83)	8806-3:1988	Informational (Approved)
GPC	DOD	USAF STARS X-Windows binding [actually a binding to Xlib and Xt]	STARS	Informational (Approved)
IPC	ECMA	PCTE - Extensions for Support of Fine-Grain Objects - Ada Programming Language Binding	229 (1995)	Informational (Approved)
NPC	ANSI	GKS Language Bindings for Ada	X3.124.3-1989	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	GKS Language Bindings - Part 3: Ada	8651-3:1988	Informational (Approved)
GPC	NIST	GKS Bindings for Ada	FIPS PUB 120-1:1994	Informational (Approved)
NPC	IFHE	POSIX Ada Language Interfaces - Part 1:Binding for Realtime Extensions	1003.5b:1996 (former 1003.20)	Informational (Approved)
IPC	ISO/IEC	PHIGS PLUS/Ada bindings (binding for Ada-83)	9593-3 PDAM 1	Informational (Draft)
IPC	ISO	Generic Package of Elementary Functions (GPEF) (binding for Ada-83)	TBD-Generic Package of Elementary Functions (GPEF) (binding for Ada-83)	Informational (Draft)
NPC	IEEE	POSIX - Part 1: System API Amendment: Real-Time Distributed Systems Communications	P1003.21	Informational (Draft)
IPC	ISO	Ada Europe Numerics Working Group Primitive Functions (binding for Ada-83)	TBD-Ada Europe Numerics Working Group Primitive Functions (binding for Ada-83)	Informational (Draft)
TBD	TBD	Ada Semantic Interface Specification (ASIS) (binding is planned for approval on the summer of 95)	TBD-Ada Semantic Interface Specification (ASIS) (binding is planned for approval on the summer of 95	Informational (Draft)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Services Interface Amendment 2: Ada bindings (binding for Ada-83)	10728 WDAM 2:1993(E)	Informational (Draft)
GPC	NIST	Initial Graphics Exchange Specification (IGES): v. 5.2 OR 6.0	FIPS PUB 177-1 (future)	Informational (Formative)
NPC	IEEE	Uniform Application Programming Interface - Graphical User Interfaces (binding for Ada-83)	P1201.1	Informational (Formative)
NPC	IEEE	Ada binding to P1003.2 (binding for Ada-83)	TBD-Ada binding to P1003.2 (binding for Ada-83)	Informational (Formative)
NPC	EIA	CASE Data Interchange Format (CDIF) Ada bindings (binding for Ada-83)	TBD	Informational (Formative)
TBD	TBD	Standard Generalized Markup Language (SGML) Ada bindings	TBD-Standard Generalized Markup Language (SGML) Ada bindings	Informational (Formative)
TBD	TBD	Transmission Control Protocol/Internet Protocol (TCP/IP) Ada bindings (binding for Ada-83)	TBD-Transmission Control Protocol/Internet Protocol (TCP/IP) Ada bindings (binding for Ada-83)	Informational (Formative)
IPC	ISO/IEC	X.25 Ada bindings (binding for Ada-83)	X.25 Ada bindings (binding for Ada-83)	Informational (Formative)
TBD	TBD	Generic Package of Primitive Functions (GPPF) (binding for Ada-83)	TBD-Generic Package of Primitive Functions (GPPF) (binding for	Informational (TBD)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
			Ada-83)	
NPC	ANSI/ASME	Digital Representation for Communication of Product Definition Data	Y14.26M:1989	Informational (Superseded)

3.2.4.1.2 Alternative specifications. The following specifications are also available:

a. Rational Systems: X Windows Xlib implementation.

b. U.S. Army HQ Communications-Electronics Command (CECOM), Center for Software Engineering, report on "Thin" Ada Binding to P1003.4 describes a possible Ada-language interface with the proposed IEEE P1003.4 real time standard.

3.2.4.1.3 Standards deficiencies. Most bindings standards are still incomplete and Ada bindings are needed for many standards. No formal standards or specifications for bindings exist between Ada and any graphical user interface. However, the USAF STARS program has developed an Ada binding for Xlib and the Xt Intrinsics.

The IEEE P1003.5 Group has defined an Ada binding to the POSIX operating system kernel which parallels the IEEE 1003.1 C binding. This binding does not include functionality similar to the IEEE 1003.2 POSIX C binding standard for Shell and Utilities. The IEEE P1003.20 Group, which is defining Ada bindings for the POSIX.4 real time extensions, was formed in July 1992. Few or no Ada bindings are defined for other IMS sub-systems.

No open standards or de facto specifications exist for a common, GUI-independent Interactive Design Tools Interchange Format (IDTIF) (e.g., Motif's User Interface Language (UIL) and Sun Microsystems' DEVGUIDE), that would allow different tools for developing interactive, graphical, windowing applications to exchange graphics objects and basic screen information. Work in this area is in progress in the Open Software Foundation's (OSF's) User Interface Management Services (UIMS) working group and as a part of X/Open's GUI research. Presently, few Interactive Design Tool products are available. Those that exist are just maturing and generally do not work with other tools.

Language bindings for character-oriented GUIs (i.e., the display, manipulation, and management of objects in windows on a character-oriented (non-bit-mapped) screen) are needed.

3.2.4.1.4 Portability caveats. It is possible to implement the X Window system in Ada, but this is a substantial amount of work. Some proprietary 4GL GUI builder products claim to have direct Ada bindings to Motif. Ada code can interface with the X libraries, which are written in C, but the Ada and C programming languages have fundamental incompatibilities. A number of COTS products support or supply such bindings.

3.2.4.1.5 Related standards. No other specifications are known.

3.2.4.1.6 Recommendations. The standards identified as adopted should be selected as needed.

3.2.4.2 C language bindings. C has been the language of choice among commercial software developers over the past decade for the development of interface bindings for SQL, communications, windowing systems, and operating systems. This "choice" has been formalized by the explicit generation of C binding standards for the various aspects of POSIX. Other languages which must interface to these support areas often are written with a library layer which binds to an existing C interface library. C++ is emerging as the language of choice among commercial developers for GUI based applications.

3.2.4.2.2 Standards. Table 3.2-29 presents standards for C language bindings.

TABLE 3.2-29 C language bindings standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Graphical Kernel System for 3 Dimensions (GKS-3D) Language Bindings, Part 4: C	8806-4:1991	Informational (Approved)
IPC	ISO/IEC	PHIGS Language Binding, Part 4: C	9593-4:1991	Informational (Approved)
NPC	IEEE	Open Systems Interconnection (OSI) Abstract Data Manipulation C Language Interfaces - Binding for Application Program Interface (API)	1327:1993	Informational (Approved)
NPC	IEEE	X.400-Based Electronic Messaging C Language Interfaces - Binding for API	1327.1:1993	Informational (Approved)
NPC	IEEE	Directory Services C Languages Interfaces - Binding for API	1327.2:1993	Informational (Approved)
IPC	ECMA	Portable Common Tool Environment (PCTE) - C Programming Language Binding	158 (1994)	Informational (Approved)
IPC	ECMA	PCTE - Extensions for Support of Fine-Grain Objects - C Programming Language Binding	228 (1995)	Informational (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Informational (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Services Interface	10728:1993	Informational (Approved)
IPC	ISO	Portable Common Tool Environment (PCTE) - Part 2: C Programming Language Binding	13719-2:1995	Informational (Approved)
IPC	ISO	GKS Language Bindings - Part 3: Ada	8651-3:1988	Informational (Approved)
NPC	IEEE	OSI Application Program Interface (API) - ACE and Presentation Layer API [C Binding]	P1352	Informational (Draft)
IPC	ISO/IEC	Image Processing and Interchange (IPI) API Language Bindings, Part 4: C	CD12087-4:	Informational (Draft)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Services Interface Amendment 1: C Language Binding	10728 AMD 1:1994	Informational (Draft)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C language], (as profiled by FIPS PUB 151-2:1993)	9945-1:1990	Informational (Superseded)

3.2.4.2.4 Alternative specifications. The SAA's SQL bindings to C are also available.

3.2.4.2.5 Standards deficiencies. Many standards lack a C binding, even in draft form, although more standards support C bindings than any other language.

3.2.4.2.6 Portability caveats. Portability problems related to the existing bindings are unknown.

3.2.4.2.7 Related standards. Other related standards are unknown.

3.2.4.2.8 Recommendations. No standards are recommended for C Bindings. C bindings should be used only in the absence of an equivalent Ada binding. A layered Ada-to-C binding approach should be taken to allow rapid migration to the Ada binding when it becomes available.

3.2.4.3 FORTRAN bindings. FORTRAN, because of its historic usefulness and popularity, has been the subject of bindings definition by several standards organizations. These standards and specifications are for standards bindings to the FORTRAN programming language.

3.2.4.3.1 Standards. Table 3.2-30 presents standards for FORTRAN bindings.

TABLE 3.2-30 FORTRAN bindings standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	POSIX FORTRAN 77 Language Interfaces - Part 1: Binding for System API	1003.9:1992	Informational (Approved)
IPC	ISO	GKS-3D FORTRAN binding	8806-1:1988	Informational (Approved)
IPC	ISO	Appendix for COBOL, FORTRAN, Pascal, and PL/1 bindings to SQL2 (Technical content of ISO 9075:1988, SQL, is retained as a level of the 1992 standard)	9075:1992 Appendix	Informational (Approved)
IPC	ISO/IEC	PHIGS FORTRAN binding	9593-1:1990	Informational (Approved)
GPC	NIST	PHIGS FORTRAN binding (Adopts ISO/IEC 9593.1:1990)	FIPS PUB 153:1992	Informational (Approved)
GPC	NIST	FORTRAN binding to GKS	FIPS PUB 120-1:1994	Informational (Approved)
NPC	ANSI	PHIGS FORTRAN binding (X3.144.1)	X3.144.1	Informational (Approved)
NPC	ANSI	FORTRAN binding to GKS	X3.124.1-1985 (R1991)	Informational (Approved)
NPC	IEEE	FORTRAN-90 bindings to POSIX	1003.19	Informational (Draft)

3.2.4.3.2 Standards conformance. Conformance to the ISO/ANSI 1539-1990 standard or FIPS 69-1 is required.

3.2.4.3.3 Alternative specifications. No other specifications are available.

3.2.4.3.4 Standards deficiencies. Many standards lack a FORTRAN binding, even in draft form.

3.2.4.3.5 Portability caveats. Portability problems related to the existing bindings are unknown.

3.2.4.3.6 Related standards. Other related standards are unknown.

3.2.4.3.7 Recommendations. No standards are recommended for FORTRAN. Work on IEEE 1003.19 has been suspended. FORTRAN bindings should be used only in the absence of an equivalent Ada binding. A layered Ada to FORTRAN binding approach should be taken to allow rapid migration to the Ada binding when it becomes available.

3.2.4.4 Bindings to COTS products. These standards and specifications are for bindings for COTS products to a programming language (i.e., Ada).

3.2.4.4.1 Standards. Table 3.2-31 presents standards for bindings to COTS products.

TABLE 3.2-31 Bindings to COTS products standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	OSF/Motif binding to Ada	TBD-OSF/Motif binding to Ada	Informational (Approved)
IPC	ISO/IEC	SQL Ada Module Description Language (SAMoDL), First Edition	12227:1995	Informational (Approved)
TBD	TBD	Transmission Control Protocol/Internet Protocol (TCP/IP) Ada bindings (binding for Ada-83)	TBD-Transmission Control Protocol/Internet Protocol (TCP/IP) Ada bindings (binding for Ada-83)	Informational (Formative)

3.2.4.4.2 Alternative specifications. A number of Ada bindings to Microsoft Windows. These are proprietary, as is Microsoft Windows, and should be used only to support legacy products.

3.2.4.4.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.4.4.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.2.4.4.6 Related standards. No other specifications are known.

3.2.4.4.7 Recommendations. No standards are recommended for COTS Ada bindings.

3.2.5 Software Engineering Security Services. Security engineering activities are critical processes during the software development life-cycle, as well as during system operation and maintenance. Concentration on the analysis and allocation of security requirements is the major goal to be accomplished. Once developed, software systems must take into account operational concerns such as certification and accreditation, risk management, and accountability functions. For users of the ITSG who are not familiar with security terminology, study of the following references is suggested:

a. National Information Systems Security (INFOSEC) Glossary, National Security Telecommunications and Information Systems Security (NTISSI) No. 4009, 5 June 1992.

b. Glossary of Telecommunications Terms, FED-STD-1037B, 3 June 1991.

c. Dictionary of Information Systems, ANSI X3.172, 1990.

d. Security in Open Systems - Data Elements and Service Definitions, ECMA 138:1989 (based on ECMA TR46:1988).

e. Glossary of Computer Security Terms, NCSC-TG-004, version 1, 21 October 1988.

3.2.5.1 Security models and architectures. (This BSA appears in part 2 and part 10.) Security models provide the necessary basis for the development of security-related protocols and security-related protocol elements.

3.2.5.1.1 Standards. Table 3.2-32 presents standards for security models and architectures.

TABLE 3.2-32 Security models and architectures standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
CPC	CEN/CENELEC/ ITAEGV	Taxonomy of Security Standardization	ITAEGV N69 Ver 2 of 4/30/1992	Informational (Approved)
IPC	ECMA	Security in Open Systems - Data Elements and Service Definitions	138 (1989)	Informational (Approved)
IPC	ECMA	Security in Open Systems - A Security Framework	TR/46 (1988)	Informational (Approved)
GPC	NIST	Guidelines for Security of Computer Applications	FIPS PUB 73:1980	Informational (Approved)
IPC	ITU-T	Security Architecture for OSI for CCITT Applications: Security, Structure, and Applications	X.800 (1991)	Informational (Approved)
CPC	X/Open	Security Guide (Second Edition)	G010 (2/91)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ITU-T	Reference Model of OSE for CCITT Applications-Data Communications Networks-OSI Model and Notation, Services Definition	X.200 (1989)	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 3: Naming and Addressing	7498-3:1989	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 4: Management Framework	7498-4:1989	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Abstract Service Definition: (same as ITU-T X.511 (1993))	9594-3:1993 (or 1994)	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Procedures for Distributed Operations:(same as ITU-T X.519(1993))	9594-4:1993 (or 1994)	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Authentication Framework (same as ITU-T X.509 (1993))	9594-8:1993 (or 1994)	Informational (Approved)
IPC	ISO	OSI Upper Layer Security Model	10745:1993	Informational (Approved)
CPC	X/Open	Distributed Security Framework	G410 (12/94)	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
NPC	IEEE	Guide to the POSIX Open Systems Environment - A Security Framework	P1003.22: 1995	Informational (Draft)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems, Part 1: Overview	10181-1	Informational (Draft)
IPC	ISO/IEC	Guide to Open Systems Security	TR by JTC1/SC21/N8380	Informational (Draft)
IPC	ISO/IEC	Management Plan for Security	JTC1/SC21 SD-7	Informational (Draft)

3.2.5.1.2 Alternate specifications. There are no alternate specifications.

3.2.5.1.3 Standards deficiencies. FIPS PUB 73 does not include information on modern security concepts.

3.2.5.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.5.1.5 Related standards. There are no related standards.

3.2.5.1.6 Recommendations. The DGSA, Volume 6 of the TAFIM, is the abstract and generic security architecture of the TAFIM. The DGSA provides security principles and target security capabilities to guide system security architects in creating specific security architectures consistent with the DGSA. The DGSA should be used by system security architects to develop logical and specific security architectures.

3.2.5.2 System development security. (This BSA appears in part 2, part 9, and part 10.) Development of secure systems requires that security engineering be a key discipline in conjunction with other system, software, and hardware engineering activities.

3.2.5.2.1 Standards. Table 3.2-33 presents standards for system development security.

TABLE 3.2-33 System development security standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Network Interpretation	NCSC-TG-005, Version 1: 1987	Mandated (Approved)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
GPC	DOD	FORTEZZA Cryptologic Programmers' Guide	MD4000501-1.52: 1996	Mandated (Approved)
GPC	DOD	FORTEZZA Application Implementon' Guide	MD4002101-1.52: 1996	Mandated (Approved)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Informational (Approved)
IPC	ISO/IEC	Software Life Cycle Processes	12207:1995	Informational (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Guidelines for Security of Computer Applications	FIPS PUB 83:1980	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Abstract Service Definition: (same as ITU-T X.511 (1993))	9594-3:1993 (or 1994)	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Procedures for Distributed Operations:(same as ITU-T X.519(1993))	9594-4:1993 (or 1994)	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Authentication Framework (same as ITU-T X.509 (1993))	9594-8:1993 (or 1994)	Informational (Approved)
CPC	X/Open	Generic Security Service API (GSS-API) Base	C441 (12/95)	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment n: Protection, Audit, and Control Interfaces (C Language), Draft 15	P1003.1e: 1995	Legacy (Draft)
NPC	IEEE	POSIX Part 2: Shell and Utilities - Amendment n: Protection and Control Utilities, Draft 15	P1003.2c: 1995	Emerging (Draft)
CPC	IETF	Generic Security Service - Application Program Interface, Version 2	RFC 2078: 1997	Emerging (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	IETF	Independent Data Unit Protection Generic Security Application Program Interface (IDUP-GSS-API)	draft-ietf-cat-idup-gss-06.txt, 26 November 1996	Emerging (Draft)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

3.2.5.2.2 Alternative specification. There are no alternative specifications.

3.2.5.2.3 Standard deficiencies. Deficiencies in the existing standards are unknown.

3.2.5.2.4 Portability caveats. There are no portability caveats.

3.2.5.2.5 Related standards. DOD Directive 5200.28 "Security Requirements for Automated Information Systems (AISs)," provides the DOD-wide program for AIS security. It provides mandatory, minimum AIS security requirements for systems processing classified, sensitive but unclassified, and unclassified information. For intelligence systems, Director, Central Intelligence Directive (DCID) 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks," and "Security Manual for Uniform Protection of Intelligence Information Processed in Automated Information Systems and Networks," should be used in conjunction with DOD 5200.28-STD. The following guidelines also are for use with DOD 5200.28-STD:

a. NCSC-TG-006, Version 1, 28 March 1988, A Guide to Understanding Configuration Management in Trusted Systems

b. NCSC-TG-007, Version 1, 2 October 1988, A Guide to Understanding Design Documentation in Trusted Systems

c. NCSC-TG-008, Version 1, 15 December 1988, A Guide to Understanding Trusted Distribution in Trusted Systems

d. NCSC-TG-018, Version 1, July 1992, A Guide to Understanding Object Reuse in Trusted Systems

e. NCSC-TG-023, Version 1, July 1993, A Guide to Understanding Security Testing and Test Documentation in Trusted Systems

3.2.5.2.6 Recommendations. The standards listed as mandated are recommended.

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	IETF	Independent Data Unit Protection Generic Security Application Program Interface (IDUP-GSS-API)	draft-ietf-cat-idup-gss-06.txt, 26 November 1996	Emerging (Draft)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

3.2.5.2.2 Alternative specification. There are no alternative specifications.

3.2.5.2.3 Standard deficiencies. Deficiencies in the existing standards are unknown.

3.2.5.2.4 Portability caveats. There are no portability caveats.

3.2.5.2.5 Related standards. DOD Directive 5200.28 "Security Requirements for Automated Information Systems (AISs)," provides the DOD-wide program for AIS security. It provides mandatory, minimum AIS security requirements for systems processing classified, sensitive but unclassified, and unclassified information. For intelligence systems, Director, Central Intelligence Directive (DCID) 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks," and "Security Manual for Uniform Protection of Intelligence Information Processed in Automated Information Systems and Networks," should be used in conjunction with DOD 5200.28-STD. The following guidelines also are for use with DOD 5200.28-STD:

a. NCSC-TG-006, Version 1, 28 March 1988, A Guide to Understanding Configuration Management in Trusted Systems

b. NCSC-TG-007, Version 1, 2 October 1988, A Guide to Understanding Design Documentation in Trusted Systems

c. NCSC-TG-008, Version 1, 15 December 1988, A Guide to Understanding Trusted Distribution in Trusted Systems

d. NCSC-TG-018, Version 1, July 1992, A Guide to Understanding Object Reuse in Trusted Systems

e. NCSC-TG-023, Version 1, July 1993, A Guide to Understanding Security Testing and Test Documentation in Trusted Systems

3.2.5.2.6 Recommendations. The standards listed as mandated are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. MIL-STD-498 contains requirements for security and privacy for software development and documentation. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service approval, until organizational processes for IEEE/EIA 12207US are in place.

If FORTEZZA services are used, the following two guidelines should be consulted:

a. MD4002101-1.52, 3/5/96, FORTEZZA Application Implementors' Guide

b. MD4000502-1.52, 1/30/96, FORTEZZA Cryptologic Programmers' Guide, Revision 1.52

3.2.5.3 Personal authentication. (This BSA appears in part 2, part 3, part 9, and part 10.) Personal authentication supports the accountability objective of being able to trace all security relevant events to individual users. In addition to supporting unique identification, standards are provided to authenticate the claimed identity.

3.2.5.3.1 Standards. Table 3.2-34 presents standards for personal authentication.

TABLE 3.2-34 Personal authentication standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
GPC	NIST	Password Usage	FIPS PUB [illegible] 1985	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
GPC	NIST	Guidelines on Evaluation of Techniques for Automated Personal Identification	FIPS PUB 48:1977	Informational (Approved)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - The Directory: Authentication Framework edition 2 (Same as ITU-T X.509:1993)	9594-8.2:1993	Informational (Approved)
GPC	NIST	Guideline for Use of Advanced Authentication Technology Alternatives	FIPS PUB 190:1994	Informational (Approved)
CPC	IETF	A One-Time Password System	RFC 1938: 1996	Emerging (Draft)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
CPC	IETF	The Kerberos Network Authentication Service (V5)	RFC 1510:1993	Informational (Draft)

3.2.5.3.2 Alternate specifications. There are no alternative specifications.

3.2.5.3.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.5.3.4 Portability caveats. OSF DCE Version 1.1's authentication service is based on Kerberos Version 5 (RFC 1510), but is not totally compatible with RFC 1510. DCE 1.2.2 adds testing and official support for Kerberos Version 5.

3.2.5.3.5 Related standards. The following standards are related to personal authentication standards (particularly TCSEC):

a. DOD 5200.28-STD, DOD Trusted Computer Systems Evaluation Criteria

b. NCSC-TG-017, Version 1, "A Guide to Understanding Identification and Authentication in Trusted Systems

c. CSC-STD-002-85, "Password Management Guideline"

d. NCSC-WA-002-85, "Personal Computer Security Considerations"

e. ITU-T X.509 (1993) (same as ISO 9594-8), The Directory: Authentication Framework

3.2.5.3.6 Recommendations. The mandated standards are recommended.

3.2.5.4 Certification and accreditation. (This BSA appears in part 2, part 9, and part 10.) Certification and accreditation constitute a set of procedures and judgments leading to a determination of the suitability of the system to operate in the targeted operational environment.

Accreditation is the official management authorization to operate a system. The accreditation normally grants approval for the system to operate (a) in a particular security mode, (b) with a prescribed set of countermeasures (administrative, physical, personnel, communications security, emissions, and computer security controls), (c) against a defined threat and with stated vulnerabilities and countermeasures, (d) within a given operational concept and environment, (e) with stated interconnections to other systems, (f) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility, and (g) for a specified period of time. The Designated Approving Authority(s) (DAA) formally accepts security responsibility for the operation of the system and officially declares that the specified system will adequately protect against compromise, destruction, or unauthorized modification under stated parameters of the accreditation. The accreditation decision affixes security responsibility with the DAA and shows that due care has been taken for security in accordance with the applicable policies.

An accreditation decision is in effect after the issuance of a formal, dated statement of accreditation signed by the DAA, and remains in effect for the specified period of time (varies according to applicable policies). A system processing classified or sensitive unclassified information should be accredited prior to operation or testing with live data unless a written waiver is granted by the DAA. In some cases (e.g., when dealing with new technology, during a transition phase, or when additional time is needed for more rigorous testing), the DAA may grant an interim approval to operate for a specified period of time. At the end of the specified time period, the DAA must make the final accreditation decision.

Certification is conducted in support of the accreditation process. It is the comprehensive analysis of both the technical and nontechnical security features and other safeguards of a system to establish the extent to which a particular system meets the security requirements for its mission and operational environment. A complete system certification must consider factors dealing with the system in its unique environment, such as its proposed security mode of operation, specific users, applications, data sensitivity, system configuration, site/facility location, and interconnections with other systems. Certification should be done by personnel who are technically competent to assess the systems ability to meet the security requirements according to an acceptable methodology. The resulting documentation of the certification activities is provided to the DAA to support the accreditation decision. Many security activities support certification, such as risk analysis, security test and evaluation, and various types of evaluations.

Ideally, certification and accreditation procedures encompass the entire life cycle of the system. Ideally, the DAA is involved from the inception of the system to ensure that the accreditation goals are clearly defined. A successful certification effort implies that system security attributes were measured and tested against the threats of the intended operational scenarios. Additionally, certification and accreditation are seen as continuing and dynamic processes; the security state of the system needs to be tracked and assessed through changes to the system and its operational

environment. Likewise, the management decision to accept the changing system for continued operation is an ongoing decision process.

Standards for certification and accreditation services provide definitions and procedures for the testing and accreditation of computer systems in so far as their conformance with security standards is concerned.

3.2.5.4.1 Standards. Table 3.2-35 presents standards for certification and accreditation.

TABLE 3.2-35 Certification and accreditation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	NIST	Guideline for Computer Security Certification and Accreditation	FIPS PUB 102:1983	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
GPC	DOD	DOD Information Technology Certification and Accreditation Process	DITSCAP: 1996	Informational (Draft)

3.2.5.4.2 Alternate specifications. No other consortia or de facto specifications are available.

3.2.5.4.3 Standards deficiencies. Because of its age, FIPS PUB 102 does not include services for the certification and accreditation of all modern security concepts. No known up-to-date standards exist for certification and accreditation.

Certification and accreditation evaluation criteria that address current information technology, such as distributed computing and networking, are needed. As new criteria such as the Common Criteria emerge, revision of existing certification and accreditation guidelines may be required.

3.2.5.4.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.2.5.4.5 Related standards. NCSC-TG-029, "Introduction to Certification and Accreditation," January 1994, discusses basic concepts related to certification and accreditation and is the first of a series of guidelines in the "Rainbow Series" supporting the Trusted Computer System Evaluation Criteria (TCSEC) standard.

3.2.5.4.6 Recommendations. The mandated standard is recommended.

Procurements that require that an AIS be certified and/or accredited must reference DOD Directive 5200.28 and applicable designated approving authority guidance. DOD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," requires

certification and accreditation of AIS. FIPS PUB 102, Guidelines for Computer Security and Accreditation provides Federal guidelines for certification and accreditation. Because of its age, this FIPS PUB does not include services for the certification and accreditation of all modern security concepts. DOD 5200.28-STD provides criteria to assess security assurances of trusted systems to specific classes. DCID 1/16 provides security requirements for systems processing intelligence information.

The DISA CISS and NSA are each developing documents that will standardize the certification and accreditation process within DOD. Each document is in draft form; final documents are expected to be issued in 1997. The NSA document, "Certification and Accreditation Process Handbook for Certifiers," will be published as a "Rainbow" series document supporting the TCSEC standard. This NSA handbook focuses on certification and accreditation of standalone systems. The DISA CISS document, "DOD Information Technology Certification and Accreditation Process" (DITSCAP), will be published as a DOD publication. The DITSCAP focuses on certification and accreditation in conjunction with the programmatic aspects of the DII.

3.2.5.5 Security risk management. (This BSA appears in part 2, part 7, part 9, and part 10.) Security risk management supports accreditation through a risk analysis of an information system and its operational environment, and the steps taken to manage the risk requirements.

3.2.5.5.1 Standards. Table 3.2-36 presents standards for security risk management.

TABLE 3.2-36 Security risk management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	NIST	Guideline for the Analysis of Local Area Network Security	FIPS PUB 191:1994	Informational (Approved)
GPC	NIST	Guideline for Automated Data Processing Risk Analysis	FIPS PUB 65:1979	Informational (Approved)
GPC	NIST	Guideline for Automatic Data Processing Physical Security and Risk Management	FIPS PUB 31:1974	Informational (Approved)

3.2.5.5.2 Alternate specifications. No alternative specifications are known.

3.2.5.5.3 Standards deficiencies. Because of its age, FIPS PUB 31 does not include information of all modern security concepts.

3.2.5.5.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.5.5.5 Related standards. The following standards are related to the TCSEC standard:

a. CSC-STD-003-85 25 June 1985, Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer Security Evaluation Criteria in Specific Environments

b. CSC-STD-004-85, 25 June 1985, Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer Security Evaluation Criteria in Specific Environments

3.2.5.5.6 Recommendations. The mandated standard is recommended. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," provides guidance on effective security risk management of federal information systems. NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook" provides additional guidance on risk management. DOD Directive 5200.28 requires a risk analysis of an information system be conducted in its operational environment to support accreditation of the information system. System implementors should perform the risk analysis in accordance with CSC-STD-003-85 and CSC-STD-004-85 to determine the appropriate DOD-5200.28-STD class.

3.2.5.6 Detection and notification. (This BSA appears in part 2, part 9, and part 10.) Detection and notification objectives ensure that a secure system has the capability to recognize that it is: under attack; may potentially enter a non-available state; has been compromised; or has failed in a potentially compromising manner. Guidance in this area focuses on reporting detected security critical conditions to proper authorities, and implementing predetermined corrective actions.

3.2.5.6.1 Standards. Table 3.2-37 presents standards for detection and notification.

TABLE 3.2-37 Detection and notification standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)

3.2.5.6.2 Alternate specifications. No alternate specifications are known.
There are no alternative specifications.

3.2.5.6.3 Standards deficiencies. No standards deficiencies are known.

3.2.5.6.4 Portability caveats. No portability caveats are known.

3.2.5.6.5 Related standards. NSA's C-Technical Report-001, Computer Viruses: Prevention, Detection, and Treatment, and NIST SP 800-5, A Guide to the Selection of Anti-Virus Tools and Techniques, provide guidance on computer viruses. The following specifications support the TCSEC standard:

a. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation

b. NCSC-TG-015, Version 1, October 1989, A Guide to Understanding Trusted Facility Management

c. NCSC-TG-016, Version 1, October 1992, Guidelines for Writing Trusted Facility Manuals

3.2.5.6.6 Recommendations. The mandated standard is recommended.

3.2.5.7 Security recovery. (This BSA appears in part 2, part 9, and part 10.) Recovery guidance defines provisions to allow system personnel or processes with the proper authorizations to repair or eliminate the cause of security relevant failures, isolate compromised portions of the system, and revalidate proper operations prior to returning the system to a fully operational secure state.

3.2.5.7.1 Standards. Table 3.2-38 presents standards for security recovery.

TABLE 3.2-38 Security recovery standard

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)

3.2.5.7.2 Alternate specifications. No alternative specifications are known.
There are no alternative specifications.

3.2.5.7.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.2.5.7.4 Portability caveats. Portability problems with the existing standards are unknown.

3.2.5.7.5 Related standards. The following specifications are related to the TCSEC standard:

a. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation

b. NCSC-TG-022, Version 1, December 1991, A Guide to Understanding Trusted Recovery in Trusted Systems

c. NCSC-TG-015, Version 1, October 1989, A Guide to Understanding Trusted Facility Management

d. NCSC-TG-016, Version 1, October 1992, Guidelines for Writing Trusted Facility Manuals

3.2.5.7.6 Recommendations. The mandated standard is recommended.

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 3 of 14 parts)

USER INTERFACE SERVICES

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

TABLE OF CONTENTS

LIST OF TABLES

3.3 User interface services. User interface services define how users may interact with an application. Depending on the capabilities required by users and the applications, these interfaces may include window management, dialog support, and user interface security.

NOTE: throughout Part 3, all tables shall have abbreviations listed under the column (Standard Type) as follows:

a. National Public Consensus = NPC
b. International Public Consensus = IPC
c. Government Public Consensus = GPC
d. Consortia Public Consensus = CPC
e. Corporate Private Non-Consensus = CPN-C

3.3.1 Introduction. The user interface is a combination of menus, screen design, keyboard commands, command language, and help screens, which create the way a user interacts with a computer. The use of mice, touch screens, and other input hardware are included as part of the user interface. A well-designed user interface is vital to the success of an application.

A graphical user interface (GUI) lets users initiate, enter, and exit applications and manipulate the commands in those applications primarily by the use of a pointing device (often a mouse). A GUI uses a visual metaphor (icons) representing actual desktop objects. The user can access and manipulate these icons with a pointing device on the display.

User Interface Services (UIS) provide a consistent way for the people who develop, administer, and use a system to gain access to applications programs, operating systems, and various system utilities. UIS standards define the multi-tier environment which exists between applications and the operating system and hardware of the computer platform.

Historically, software applications interfaced directly to the operating system and even to the platform hardware. The advent of the GUI and the desire for easy to use, platform-independent, uniform interfaces for user applications have led to a layered approach to interfacing well behaved, user friendly applications to operating systems and platforms. Modern GUI based applications predominately interface through a high level Windowing Application Programming Interface (API) which provides a common look and feel to users across applications via a supplied toolkit of functions and data structures. This interface is explicitly designed to be platform independent. The Windowing API interfaces to a Basic Windowing Toolkit which provides middle level windowing functionality. At this level, the emphasis is also on platform independence, but look and feel is not as tightly controlled as at the higher level. This basic toolkit interfaces to a set of toolkit primitives which supplies an operating system and platform specific interface. Thus, it should be possible to write cross-platform applications using Windowing API calls and require implementation of platform and operating system specific tailoring at the primitives level. These three intervening layers between the platform and the operating system are the areas of concern for UIS.

The Adopted Information Technology Standards (AITS) and ITSG recognize Institute of Electrical and Electronics Engineers (IEEE) POSIX operating systems and hardware as the open system of choice for the Department of Defense (DOD). Graphical user interface oriented applications and environments are emphasized over character-based interfaces. This emphasis arises from the realization that, for modern computer systems, GUIs can provide consistent, easy-to-use software to users and thereby lower training time and expense and enhance individual productivity. An information system architecture must address not only the technical features of the user interface but also the human engineering considerations. Thus, many of the UIS standards discussed in this part of the ITSG address the specification of aspects of a GUI environment layering on a POSIX operating system.

The major UIS standards issues facing DOD is the widespread use within DOD of Microsoft Windows (MS Windows) GUI platforms. This usage mirrors the 85% commercial market dominance of MS Windows. While POSIX systems are the adopted DOD standard, the vast majority of DOD systems are based upon MS Windows. Commercial users may accept the proprietary MS Windows as a de facto standard, but the DOD OSE mandate does not allow the adoption of this single vendor product as a standard [illegible] total reliance of the US defense establishment on the caprice of a single company. [illegible] due to economic and office automation compatibility reasons, these platforms are commonly [illegible] for DOD agencies and services in circumvention of the OSE standards.

A solution to this issue is being sought in the current consortium development activity by a working group within the European Computer Manufacturer's Association (ECMA) to produce an ISO standard for an Applications Programming Interface for Windows (APIW). The APIW will be an open specification based upon key MS Windows 3.1 functionality. This ECMA/ISO standard will allow eventual adoption of the APIW by DOD as a GUI windowing API, thus legitimizing existing Windows platforms and encouraging other vendors to develop alternate, compliant UIS windowing products.

There are several standards defining organizations which are significant contributors to UIS IT standards. To aid the reader in following the standards discussions in this chapter, these organizations are briefing described in the following paragraphs.

The National Institute of Standards and Technology (NIST), part of the Department of Commerce, is the primary standards defining agency for the US government. NIST, formerly the National Bureau of Standards, produces the Applications Portability Profile (APP) and Federal Information Processing Standard (FIPS). NIST Standards in this chapter are labeled as GPC.

The Institute of Electrical and Electronic Engineers (IEEE) is an open, non-profit standards making body composed of over 10,000 engineers, scientists, and students in electronics and related fields. IEEE produces telecommunications and computing standards include those for and relating to the POSIX operating system. Adopted IEEE standards for UIS are noted as NPC.

The Open Software Foundation (OSF) is a non-profit organization which emphasizes the development of open computing environment standard products. Motif and the Distributed

Computing Environment (DCE) are their primary UIS standard specifications. ITSG adopted OSF standards are CPC.

X/OPEN is a consortium of computer manufacturers which promotes the development of information technology specific ns based on UNIX and provides a program for product branding. X/OPEN standards are denoted as CPC.

The Common Open Software Environment (COSE) was a consortium of six UNIX vendors. COSE is now defunct and its primary standard specification, the Common Desktop Environment (CDE) is now being developed by X/OPEN.

The Organization for International Standards (ISO) sets a broad range of international standards. For information technology, ISO has established the Joint Technical Committee for Information Technology (JTC1). ISO UIS standards are labeled as IPC.

Several standards, particularly those which relate to GUIs, are referenced by a number of base service areas discussed in the following sections. Additionally, while each set of standards associated with a base service area are summarized in a table in each section, there is significant overlap between these common standards. A summary of these key standards, the various base service areas addressed by each, and the overlap of the standards is presented in the following discussion.

FIPS 158-1, The User Interface Component of the Applications Portability Profile, October 8, 1993, adapts the X Protocol, Xlib Interface, Xt Intrinsics, and Bitmap Distribution Format (BDF) specifications of the X Window System, Version 11, Release 5 (X11R5). (See following paragraph.) This current version supersedes the original FIPS 158, X-Windows User Interface, May 1990, which was based upon X Windows System, Version 11, Release 3 (X11R3) and compatible with X11R4. (The name of the older standard differs from the current standard as it predated the existence of the NIST APP.) A new version, FIPS 158-2, is being developed to adopt the new X11R6 windowing standard. Whenever FIPS 158-1 is referenced in a base service area, it is the adopted standard in the AITS. Components of this standard are referenced in the following base service areas (BSAs):

3.3.3.1	Data stream encoding
3.3.3.2	Data stream interface
3.3.3.3	Subroutine foundation library
3.3.3.4	Raster data interchange
3.3.3.6	User Interface Management System
3.3.3.7	Data interchange format for GUI-based applications
3.3.4.4	Three-dimensional appearance

The original FIPS 158 is noted in these base service areas as a superseded standard which supports legacy systems based upon X11R3 and X11R4. FIPS 158-2 is noted as a formative standard in the base service area called Communications between GUI client applications.

X11R6 is the current release (May 1994) of the X-Windows standard developed by the MIT X Consortium. It is a GUI standard which provides portability of information across hardware and operating systems and allows applications and resources to be distributed across a network, based upon a client-server architecture. X11R6 implements advanced windowing concepts and support "thread safe" multi-threading. As no significant products are as yet available for the newly released X11R6, the previous version, X11R5, as adopted by FIPS 158-1, remains as the accepted secondary reference standard for many UIS BSAs, including all BSAs noted above, except Raster data interchange and User Interface Management System. Additionally, X11R5 and X11R6 are referenced independently in the following base service areas:

3.3.4.6 Customization to local norms
3.3.5.1 Independent window management services

X11R6 is listed as the primary standard in base service area called X windows over Open Systems Interconnection (OSI) at 3.3.3.11. X11R5 does not address this BSA.

OSF/Motif Version 2.0 is the current version (June 1994) of the Open Systems Foundation specification for GUI behavior and screen appearance for applications running on systems that support X11R5. It includes an API consisting of a toolkit (adopted by IEEE MTE, 1295), a User Interface Language, the Application Environment Specification (AES), and a style guide. It is somewhat incompatible with the multi-threading implementation in the new X11R6 standard. As no significant products are as yet available for the newly released Motif 2.0, the previous version Motif 1.2 remains as the reference standard for many UIS BSAs. Adoption of Motif 2.0 as an ITSG standard will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved. Components of the Consortia Public Consensus Motif 2.0 and 1.2 standards are referenced in the following base service areas:

3.3.3.1 Data stream encoding
3.3.3.2 Data stream interface
3.3.3.3 Subroutine foundation library
3.3.3.6 User Interface Management System
3.3.3.7 Data interchange format for GUI-based applications
3.3.3.8 X Logical Font Description
3.3.3.9 Compound text encoding
3.3.4.1 Application programming interfaces
3.3.4.2 User Interface Definition Language
3.3.4.3 GUI style guides
3.3.4.5 Interchange format for design tools
3.3.4.6 Customization to local norms
3.3.4.7 Language bindings for GUIs
3.3.5.1 Independent window management services
3.3.5.2 Multiple displays
3.3.5.4 On-line help
3.3.5.5 Drivability

3.3.5.6 Commands, menus, and dialog services

The IEEE Modular Toolkit Environment (IEEE MTE, 1295) is a standard for GUI applications and user interfaces to open systems and defines the application interface to display objects (widgets) built upon the X Window System X Toolkit Intrinsics. It adopts the software interface toolkit associated with OSF/Motif Version 1.2. As with Motif, the MTE defines a C language binding. It is referenced as an approved standard in base service areas Application programming interfaces, 3.3.4.1, and Language bindings for GUIs, 3.3.4.7.

The Human-Computer Interface (HCI) Style Guide, Version 3.0, is a DOD publication that provides a common framework for HCI design and implementation with particular emphasis on standard look and feel for GUI based applications. It is currently published as volume 8 of the Technical Architecture Framework for Information Management (TAFIM). This DOD style guide is adopted as the AITS standard in the following base service areas:

3.3.2.2 Human factors for video display terminals
3.3.2.3 Human factors for keyboards
3.3.2.4 Human factors for non-keyboard input devices
3.3.2.5 Human factors for the physical environment
3.3.4.3 GUI style guides
3.3.4.6 Customization to local norms
3.3.4.9 Color use
3.3.5.4 On-line help
3.3.5.5 Drivability
3.3.5.6 Commands, menus, and dialog services
3.3.8.1 User interface security labeling

UIS standards must be consistent with other ITSG service areas. It has already been noted that UIS standards are consistent with the DOD mandate of the POSIX operating system standard. Three other base service areas discussed in this part of ITSG have a direct overlap with other service areas. These areas and the overlapping service areas are listed below:

3.3.8 Security base service areas, cloned from the equivalent base service areas in Security Services.
3.3.3.4 Raster data interchange, cloned from the BSA in Data Interchange Services and coincident with the BSA in Graphics Services.
3.3.6.3 Electronic forms, cloned from the BSA in Data Management Services and coincident with the BSA in Data Interchange Services.

Modern systems and applications are and will be based upon graphical user interfaces and the associated standards for such systems. However, many legacy systems still include a large number of character-based terminals. Base service areas for character-based display terminals discuss standards which can be applied to such systems. No recommendations are made as to the use of these standards on legacy systems, since such recommendations may be inappropriately or

uneconomically applied to such systems. Should a new system be developed employing such technology, the appropriate character-based standards should be used.

3.3.2 User interface hardware. User interface hardware deals with all forms of hardware used to provide an interface between humans and computers. These devices include, for example, keyboards.

3.3.2.1 Keyboard device layout. (This BSA appears in both part 3, User Interface, and part 14, Internationalization.) Keyboard device layout standards specify the arrangement of keys on a keyboard.

3.3.2.1.1 Standards. Table 3.3-1 presents standards for keyboard device layout.

TABLE 3.3-1 Keyboard device layout standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Keyboard Layouts for Text and Office Systems	9995-1..8:1994	Mandated (Approved)
GPC	DOD	Military Standard Keyboard Arrangements	MIL-STD-1280, Notice 1, 1969	Informational (Approved)
NPC	ANSI	Allocation of Letters to the Keys of Numeric Keypads	T1.703 (1995)	Informational (Approved)
NPC	ANSI	Coded Character Sets for Keyboard Arrangement in ANSI X4.23-1982 and X4.22-1983	X3.114-1984 (R1991)	Informational (Approved)
NPC	ANSI	Keyboard Arrangement	X3.154-1988	Informational (Approved)
NPC	ANSI	Alternate Keyboard Arrangement	X3.207-1991	Informational (Approved)
CPC	X/Open	Key Values (in Window Management, Issue 3)	XPG3 Vol. 6 C216	Informational (Approved)
IPC	ISO	Keyboard Layouts for Numeric Applications	3791:1976	Informational (Approved)
IPC	ISO/IEC	Numeric Keyboard for Home Electronic Systems (HES)	946:1988	Informational (Approved)
IPC	ECMA	Common Secondary Keyboard Layout for Languages Using a Latin Alphabet	115 (1986)	Informational (Canceled)
IPC	ISO	Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) part 4: Keyboard requirements	9241-4	Informational (Draft)
IPC	ISO	Keyboard for International Information Processing Interchange Using the ISO 7-Bit Coded Character Set - Alphanumeric Area	2530:1975	Informational (Superseded)
IPC	ISO	Keyboard Layouts for Text/Office Systems	3243:1975	Informational (Superseded)
IPC	ISO	Keyboard Layouts for Text/Office Systems	3244:1984	Informational (Superseded)
IPC	ISO	Keyboard Layouts for Text/Office Systems	8884:1987	Informational (Superseded)
NPC	ANSI	Keyboard Arrangement	X4.23-1982	Informational (Superseded)

3.3.2.1.2 Alternative specifications. The only other available specifications are proprietary.

3.3.2.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.3.2.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.3.2.1.5 Related standards. No standards are related to keyboard device layout standards.

3.3.2.1.6 Recommendations. Conformance to all ISO and ISO/IEC keyboard specifications conforming to DIS or IS levels is recommended. This is especially important for equipment that will interoperate with that of U.S. allies (e.g., NATO).

3.3.2.2 Human factors for video display terminals. (This BSA appears in both part 3, User Interface, and part 13, Human Factors.) This base service area addresses the human factors requirements for all types of video displays, and includes safety concerns.

3.3.2.2.1 Standards. Table 3.3-2 presents human factors standards for video display terminals.

TABLE 3.3-2 Human factors for video display terminals standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) Part 1: Introduction	9241-1:1992	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) Part 2: Task Requirements	9241-2: 1992	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) Part 3: Visual Display Requirements	9241-3:1992	Informational (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
GPC	DOD	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	MIL-STD-1472D Notice 2, 30 June 1992	Informational (Approved)
IPC	ECMA	Ergonomics - Requirements for Non-CRT (Cathode Ray Tube) Visual Display Units	136 (1989)	Informational (Approved)
IPC	ISO	Ergonomic Principles in the Design of Work Systems	6385:1981	Informational (Approved)
NPC	ANSI/AIIM	Electronic Imaging Output Displays	TR19-1993	Informational (Approved)
CPC	NSC	Guide to Working Safely with Computers - Manual (relates to VDTs)	13068-0000	Informational (Approved)
IPC	ECMA	Procedure for Measurement of Emissions of Electric and Magnetic Fields from VDUs from 5 Hz to 400 kHz	172 (1992)	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 8: Requirements for displayed colors	9241-8	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 7: Display requirements with reflections	9241-7	Informational (Draft)
IPC	ISO	Flat Panel Display Ergonomic Requirements	13406	Informational (Draft)
NPC	ANSI/HFS	Human Factors Engineering of Visual Display Terminal Workstations (Rev. 1)	100-1988 (Revision 1)	Informational (Draft (WD))
IPC	ECMA	Ergonomics - Requirements for Colour Visual Display Devices	126 (1987)	Informational (Canceled)
IPC	ECMA	Ergonomics - Requirements for Monochromatic Visual Display Devices	110 (1985)	Informational (Canceled)

3.3.2.2.2 Alternative specifications. There are no alternative specifications available.

3.3.2.2.3 Standards deficiencies. The performance-based test described in ISO 9241-3 adequately discriminates between a display that meets the physical requirements of the standard and one that does not. However, timing scores may be badly affected by the effects of testing practice. Changes to the test method and metrics are under consideration. ISO 9241-3 does not adequately address flat panel displays. ISO 13406 is intended to remedy this situation.

3.3.2.2.4 Portability caveats. No portability problems are known with the above specifications.

3.3.2.2.5 Related standards. The following standards are related to human factors standards for video display terminals:

a. ISO CD 10075-2, Ergonomic principles related to mental work load, Part 2: Design Principles, gives guidance on the design of work systems in general, with the intention of providing optimal working conditions with respect to health and safety, well-being, performance, and effectiveness.

b. MIL-STD-1908 (1992) Definition of Human Factors Terms.

c. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

d. MIL-STD-1800A (1990) Human Engineering Performance Requirements for Systems (Air Force published, but rarely used, duplicates MIL-STD-1472).

e. MIL-HDBK-759B(2) (1993) Human Factors Engineering Design for Army Materiel. (Draft 759C is complete.)

f. MIL-HDBK-761A(1989) Human Engineering Guidelines for Management Information Systems.

g. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

h. DOD-HDBK-743A (1991) Anthropometry of U.S. Military Personnel.

i. ITU-T E.134 Human Factors Aspects of Public Terminals: Generic Operating Procedures.

j. An ISO work item for a standard on "Human-Centered design" has been approved, but no working draft has yet been released for comment.

3.3.2.2.6 Recommendations. Procurements that require hardware components to be addressed by ergonomic standards can require conformance with standards for computer displays. Display characteristics include brightness and contrast, character legibility, image stability, glare, and the use of color.

Note, however, that ISO human factors/ergonomics standards are either normative or informative. An informative standard contains no mandatory requirements. A normative standard contains one or more requirements that must be met in order to achieve conformance with the standard.

ISO 9241-1 presents an overview of the content and usage of the multipart ISO 9241 standard. A revised version of ISO 9241-1 is currently at the Committee Draft (CD) level and will soon be released for Draft International Standard (DIS) ballot. ISO 9241-2 presents an overview of factors that should be considered when designing tasks to be performed in a specific computing environment.

Parts 1 and 2 of the ISO 9241 standard are informative. Part 3 of the ISO 9241 standard is normative; parts 2-9 are expected to be normative on completion. Conformance requirements for each normative part are embedded within that part. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product.

Procurements must recognize the difference between informative and normative parts of the standard in question. Where possible, both the informative and normative parts should be required for the best implementation of modern human factors/ergonomic thinking. In general, conformance tests for informative parts will not be available.

The ISO and ISO/IEC standards cited in the gray area of the table are being balloted and revised at a rapid rate. Interested parties should monitor the progress of these standards at six month intervals to ensure they have the latest information. Offerers of products meeting existing or emerging standards should be required to provide a migration plan to ensure compliance of the products with the final standards documents.

The DOD HCI Style Guide is recommended, in particular section 3, which deals with hardware.

3.3.2.3 Human factors for keyboards. (This BSA appears in both part 3, User Interface, and part 13, Human Factors.) This BSA covers keyboard layout, including specific directions for layout of regions of the keyboard, and keyboard design. Ease of use and correct ergonomic design also are a part of this BSA.

3.3.2.3.1 Standards. Table 3.3-3 presents human factors standards for keyboards.

TABLE 3.3-3 Human factors for keyboards standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 1: General principles governing keyboard layout	9995-1:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 2: Alphanumeric section	9995-2:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 3: Common secondary layout of the alphanumeric section	9995-3:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 4: Numeric section	9995-4:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 5: Editing section	9995-5:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 6: Function section	9995-6:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 7: Symbols used to represent functions	9995-7:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 8: Allocation of Letters to the Keys of a Numeric Keyboard	9995-8:1994	Informational (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
NPC	ANSI	Coded Character Sets for Keyboard Arrangement in ANSI X4.23-1982 and X4.22-1983	X3.114-1984 (R1991)	Informational (Approved)
NPC	ANSI	Keyboard Arrangement	X3.154-1988	Informational (Approved)
NPC	ANSI	Alternate Keyboard Arrangement	X3.207-1991	Informational (Approved)
GPC	DOD	Military Standard Keyboard Arrangements	MIL-STD-1280, Notice 1, 1969	Informational (Approved)
GPC	DOD	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	MIL-STD-1472D Notice 2, 30 June 1992	Informational (Approved)
IPC	IEC	Man-Machine Interface (MMI) - Actuating Principles	447:1993	Informational (Approved)
CPC	NSC	Cumulative Trauma Disorders: a Manual for Musculoskeletal Diseases of the Upper Limbs	12221-0000	Informational (Approved)
IPC	ISO	Ergonomic Principles in the Design of Work Systems	6385:1981	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ACGIH	Ergonomic Interventions to Prevent Musculoskeletal Injuries in Industry	9000:1987	Informational (Approved)
CPC	NSC	Evaluating Your Workplace: Hands & Arms - Ergonomic Changes Manual	12587-0004	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) part 4: Keyboard requirements	9241-4	Informational (Draft)
NPC	ANSI/HFS	Human Factors Engineering of Visual Display Terminal Workstations (Rev. 1)	100-1988 (Revision 1)	Informational (Draft (WD))

3.3.2.3.2 Alternative specifications. There are no alternative specifications available.

3.3.2.3.3 Standards deficiencies. MIL-STD-1472D is in need of a comprehensive revision to update technical material so that it is reasonably consistent with the state of the art and to ensure that the two commands not currently using the standard can do so.

3.3.2.3.4 Portability caveats. No portability problems are known with the above specifications.

3.3.2.3.5 Related standards. The following standards are related to human factors standards for keyboards:

a. ISO 9241-1:1992, Ergonomic requirements for office work with visual display terminals (VDTs), part 1: Introduction, presents an overview of the content and usage of the multipart ISO 9241 standard. A revised version of ISO 9241-1 is currently at the CD level and will soon be released for DIS ballot.

b. ISO 9241-2:1992, Ergonomic requirements for office work with VDTs, part 2: Task Requirements, presents an overview of factors that should be considered when designing tasks to be performed in a specific computing environment.

c. ISO CD 10075-2, Ergonomic principles related to mental work load -- Part 2: Design Principles, gives guidance on the design of work systems in general, with the intention of providing optimal working conditions with respect to health and safety, well-being, performance, and effectiveness.

d. MIL-STD-1908 (1992), Definition of Human Factors Terms.

e. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

f. MIL-STD-1800A (1990) Human Engineering Performance Requirements for Systems.

g. MIL-HDBK-759B(2) (1993) Human Factors Engineering Design for Army Materiel. (Draft 759C is complete.)

h. MIL-HDBK-761A(1989) Human Engineering Guidelines for Management Information Systems.

i. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

j. DOD-HDBK-743A (1991) Anthropometry of U.S. Military Personnel.

k. ITU-T E.134 Human Factors Aspects of Public Terminals: Generic Operating Procedures.

l. An ISO work item for a standard on "Human-Centered design" has been approved, but no working draft has yet been released for comment.

3.3.2.3.6 Recommendations. Procurements that require hardware components to be addressed by ergonomic standards can require conformance with standards for keyboards. Keyboard characteristics include keyboard height, slope, profile, surface properties, adjustability, bounce and character repeat, key positioning, key displacement and force, keytop shape, and keytop legends.

Parts 1 and 2 of the ISO 9241 standard (see related standards) are informative. Parts 2-9 are expected to be normative on completion. Conformance requirements for each normative part are embedded within that part. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product.

Parts 1-8 of the ISO/IEC 9995 standard are normative. Conformance requirements for each normative part are embedded within that part. Conformance with the overall ISO 9995 standard is based on conformance with all normative parts that apply to a particular product.

The DOD HCI Style Guide is recommended, particularly for section 3, which covers hardware.

3.3.2.4 Human factors for non-keyboard input devices. (This BSA appears in both part 3, User Interface, and part 13, Human Factors.) This section presents human factors standards for input devices other than keyboards. These devices include trackballs, pens, and tablets among others.

3.3.2.4.1 Standards. Table 3.3-4 presents human factors standards for non-keyboard input devices.

TABLE 3.3-4 Human factors for non-keyboard input devices standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 7: Symbols used to represent functions	9995-7:1994	Informational (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
IPC	IEC	Man-Machine Interface (MMI) - Actuating Principles	447:1993	Informational (Approved)
IPC	ISO	Ergonomic Principles in the Design of Work Systems	6385:1981	Informational (Approved)
CPC	NSC	Cumulative Trauma Disorders: a Manual for Musculoskeletal Diseases of the Upper Limbs	12221-0000	Informational (Approved)
CPC	NSC	Evaluating Your Workplace: Hands & Arms - Ergonomic Changes Manual	12587-0004	Informational (Approved)
CPC	NSC	Cumulative Trauma	15229-0000	Informational (Approved)
NPC	ACGIH	Ergonomic Interventions to Prevent Musculoskeletal Injuries in Industry	9000:1987	Informational (Approved)
IPC	ISO/IEC	Text and Office Systems, Dialog Interaction Part 1: Cursor Control	10741-1:1992	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 9: Requirements for non-keyboard input devices	9241-9	Informational (Draft)
NPC	ANSI/HFS	Human Factors Engineering of Visual Display Terminal Workstations (Rev. 1)	100-1988 (Revision 1)	Informational (Draft (WD))

3.3.2.4.2 Alternative specifications. There are no alternative specifications available. Research in this area includes a foot operated control for the cursor when the hands are occupied (nicknamed a "mole" in obvious derivation from "mouse").

3.3.2.4.3 Standards deficiencies. Deficiencies in the cited standards are not known.

3.3.2.4.4 Portability caveats. No portability problems are known with the above specifications.

3.3.2.4.5 Related standards. The following standards are related to human factors standards for non-keyboard input devices:

a. ISO 9241-1:1992, Ergonomic requirements for office work with VDTs, part 1: Introduction, presents an overview of the content and usage of the multipart ISO 9241 standard. A revised version of ISO 9241-1 is currently at the CD level and will soon be released for DIS ballot.

b. ISO 9241-2:1992, Ergonomic requirements for office work with VDTs, part 2: Task Requirements, presents an overview of factors that should be considered when designing tasks to be performed in a specific computing environment.

c. ISO CD 10075-2, Ergonomic principles related to mental work load -- Part 2: Design Principles, gives guidance on the design of work systems in general, with the intention of providing optimal working conditions with respect to health and safety, well-being, performance, and effectiveness.

d. MIL-STD-1908 (1992), Definition of Human Factors Terms.

e. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

f. MIL-STD-1800A (1990) Human Engineering Performance Requirements for Systems.

g. MIL-HDBK-759B(2) (1993) Human Factors Engineering Design for Army Materiel. (Draft 759C is complete.)

h. MIL-HDBK-761A (1989) Human Engineering Guidelines for Management Information Systems.

i. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

j. DOD-HDBK-743A (1991) Anthropometry of U.S. Military Personnel.

k. ITU-T E.134 Human Factors Aspects of Public Terminals: Generic Operating Procedures.

l. An ISO work item for a standard on "Human-Centered design" has been approved, but no working draft has yet been released for comment.

3.3.2.4.6 Recommendations. Procurements that require hardware components to be addressed by ergonomic standards can require conformance with standards for non-keyboard input devices. Ergonomic issues for non-keyboard input devices include keyclick, tracking speed, and on-screen ghosting of the pointer.

Parts 1 and 2 of ISO 9241 are informative. Parts 2-9 are expected to be normative on completion. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product. Parts 1-8 of ISO/IEC 9995 are normative. Conformance

with the overall ISO 9995 standard is based on conformance with all normative parts that apply to a particular product. Part 1 of the ISO/IEC 10741 standard is expected to be normative on completion.

Procurements must recognize the difference between informative and normative parts of the standard in question. Where possible, both the informative and normative parts should be required for the best implementation of modern human factors/ergonomic thinking. In general, conformance tests for informative parts will not be available.

The DOD HCI Style Guide is recommended particularly for section 3, which covers hardware.

3.3.2.5 Human factors for the physical environment. (This BSA appears in both part 3, User Interface, and part 13, Human Factors.) Procurements that require computing environments to be addressed by ergonomic standards can require conformance with standards for illuminance, glare, acoustic noise, the thermal environment, electromagnetic emissions, computer workspace design and furniture design.

The effects of low-level non-ionized radiation, particularly from CRTs, on humans have been a controversial topic. Over the years there have been articles advising pregnant women who have a prior history of miscarriage to stay away from working in computer areas. During the cold war, the Soviets were suspected of secretly bombarding foreigners with non-ionized radiation to study long term effects. People who live near high voltage power lines and have developed cancer are suspected victims of electromagnetic radiation. While there are no hard theories to describe the relationship between health problems and this kind of radiation, let alone a standard established. Some VDT vendors have made claims regarding the emissions of their products and there are aftermarket shields available that may provide some protection against this form of radiation.

Laser printers are said to emit ozone during the printing process. In an enclosed area, high levels of ozone can be unhealthy or even toxic. This issue is still unclear. It remains to be seen how much ozone is emitted and what concentrations are hazardous.

3.3.2.5.1 Standards. Table 3.3-5 presents human factors standards for the physical environment.

TABLE 3.3-5 Human factors for the physical environment standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
CPC	OSF	Motif Style Guide	Motif SG Rev. 1.2:1992	Mandated (Approved)
CPN-C	Microsoft	The Windows Interface: An Application Design Guide, Microsoft Press, 1992	API Design Guide	Mandated (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
GPC	DOD	Noise Limits for Military Material	MIL-STD-1474C of 8 March 1991	Informational (Approved)
GPC	DOD	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	MIL-STD-1472D Notice 2, 30 June 1992	Informational (Approved)
GPC	DOD	Physical Ear Noise Attenuation Testing	MIL-STD-912 of 11 December 1990	Informational (Approved)
IPC	ISO	Ergonomic Principles Related to Mental Work Load - General Terms and Definitions	10075:1991	Informational (Approved)
IPC	ISO	Principles of Visual Ergonomics - Lighting of Indoor Work Systems	8995:1989	Informational (Approved)
IPC	ISO	Expression of Users' Requirements Part 1: Thermal Requirements	6242-1:1992	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Expression of Users' Requirements Part 2: Air Purity Requirements	6242-2:1992	Informational (Approved)
IPC	ISO	Expression of Users' Requirements Part 3: Acoustical Requirements	6242-3:1992	Informational (Approved)
NPC	EIA	Considerations Used in Establishing the X-Radiation Ratings of Monochrome and Color Direct-View Television Picture and Data Display Tubes	TEP 194, Amd 1 1987, Amd 2 1988	Informational (Approved)
CPC	NSC	Ergonomics in Computerized Offices	12223-0000	Informational (Approved)
CPC	NSC	Guide to Working Safely with Computers - Manual (relates to VDTs)	13008-0000	Informational (Approved)
CPC	NSC	Guide to Working Safely with Computers	13608-0000	Informational (Approved)
CPC	NSC	Working Safely with Your Computer	15223-0000	Informational (Approved)
IPC	ECMA	Ergonomics - Recommendations for VDU (Visual Display Units) Work Places	TR/22 (1984)	Informational (Approved)
IPC	ECMA	Application of Human Engineering to Advanced Aircrew Systems	3994 (1984)	Informational (Approved)
IPC	ECMA	Measurement of Airborne Noise Emitted by Computer and Business Equipment	74 (1992)	Informational (Approved)
IPC	ECMA	Measurement of High Frequency Noise Emitted by Computer and Business Equipment	108 (1989)	Informational (Approved)
IPC	ECMA	Declared Noise Emission Values of Computer and Business Equipment	109 (1992)	Informational (Approved)
IPC	ECMA	Determination of Sound Power Levels of Computer and Business Equipment Using Sound Intensity Measurements; anning Method in Controlled Rooms	160 (1992)	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) Part 5: Workplace requirements	9241-5	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 6: Environmental requirements	9241-6	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 7: Display requirements with reflections	9241-7	Informational (Draft)
NPC	ANSI/HFS	Human Factors Engineering of Visual Display Terminal Workstations (Rev. 1)	100-1988 (Revision 1)	Informational (Draft (WD))

3.3.2.5.2 Alternative specifications. MPR II 1990:8 (Test Methods for Visual Display Units, Section 2.0.1) is a Swedish document containing recommended values for electronic emissions from visual display units. While not an ISO standard, it serves as a de facto electromagnetic emissions standard for displays in most other countries. Many vendors of monitors claim compliance with this or a similar specification. After-market radiation and glare shields are also available.

3.3.2.5.3 Standards deficiencies. Deficiencies in the existing standards are not known.

3.3.2.5.4 Portability caveats. MIL-STD-1474C's criteria are more stringent than those of the Occupational Safety and Health Administration and also covers additional topics such as nondetectability. This standard may be incorporated into the next revision of MIL-STD-1472, eliminating the need to retain MIL-STD-1474C.

3.3.2.5.5 Related standards. The following standards are related to human factors standards for computer environments:

a. ISO 9241-1:1992, Ergonomic Requirements for Office Work with VDTs, part 1: Introduction, presents an overview of the content and usage of the multipart ISO 9241 standard. A revised version of ISO 9241-1 is at the CD level and will soon be released for DIS ballot.

b. ANSI/ASHRAE 55, Thermal Environmental Conditions for Human Occupancy, 1992.

c. ANSI S12.10-1985, Method for Measurement and Designation of Noise Emitted by Computer and Business Equipment.

d. ANSI S1.13-1971, Methods for the Measurement of Sound Pressure Levels.

e. ANSI X5.1-1985, Tests for General Office Chairs.

f. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

g. MIL-STD-1800A (1990) Human Engineering Performance Requirements for Systems.

h. MIL-HDBK-759B(2) (1993) Human Factors Engineering Design for Army Materiel. (Draft 759C is complete.)

i. MIL-HDBK-761A (1989) Human Engineering Guidelines for Management Information Systems.

j. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

k. DOD-HDBK-743A (1991) Anthropometry of U.S. Military Personnel.

l. MIL-STD-740-1 (1986) Airborne Sound Measurements and Acceptance Criteria of Shipboard Equipment.

m. MIL-STD-740-2 (1986) Structureborne Vibratory Acceleration Measurements Acceptance Criteria of Shipboard Equipment.

n. MIL-STD-1294A (1985) Acoustical Noise Limits in Helicopters.

o. An ISO work item for a standard on "Human-Centered design" has been approved, but no working draft has yet been released for comment.

3.3.2.5.6 Recommendations. The approved standards in this section are recommended where they are applicable. Parts 2-9 and 12-17 are expected to be normative on completion. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product.

The DOD HCI Style Guide is recommended particularly for section 3, which covers hardware.

3.3.3 GUI client-server operations. Graphical client-server operations define the relationships between client and server processes operating within a network; in particular, graphical user interface display processes. The program that controls each display unit is a server process, while independent user programs are client processes that request display services from the server.

3.3.3.1 Data stream encoding. Data stream encoding provides a client-server protocol to interface between the local windowing system and the outside world.

3.3.3.1.1 Standards. Table 3.3-6 presents standards for data stream encoding.

TABLE 3.3-6 Data stream encoding standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	User Interface Component of the Applications Portability Profile (Adopts the X Protocol, Xlib Interface, Xt Intrinsics, and Bitmap Distribution Format of X11R5)	FIPS PUB 158-1:1993	Mandated (Approved)
CPC	X/Open	X Window System Protocol (X Protocol)	C150 (7/91)	Informational (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	MIT X Consortium	Data Stream Encoding (X Protocol)	X11R6 (1994)	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
GPC	NIST	X-Windows User Interface (same as in X11R3)	FIPS PUB 158	Informational (Superseded)

3.3.3.1.2 Alternative specifications. The Sun Microsystems X11/NeWS specification is also available for appropriate legacy systems. Users of X11/NeWS need Sun's proprietary "libcps" library instead of Xlib. (See Data stream interface.)

3.3.3.1.3 Standards deficiencies. A formal standards effort is no longer in progress for the X Protocol because the American National Standards Institute (ANSI X3H3.6) X Protocol effort has been disbanded. Efforts to resume its work have failed and there will be no ANSI X Protocol standard. If the X Protocol is required for a procurement, reference Federal Information Processing Standard (FIPS) 158-1 (which references the MIT X Consortium).

As no significant products are as yet available for the newly released X11R6, the previous version, X11R5, as adopted by FIPS 158-1, remains as the accepted secondary reference standard.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate

threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.3.1.4 Portability caveats. System V Interface Definition (SVID) users with Sun's X11/NeWS (instead of the X Protocol) need Sun's proprietary "libcps" library instead of Xlib (see Data stream interface).

3.3.3.1.5 Related standards. The following standards are related to data stream encoding or data stream encoding standards:

a. ISO/IEC JTC 1/SC18/WG9: Working on a Voice Messaging User Interface Forum (VMUIF). (This effort moves the ANSI work of X3V1.9 to International Standard (IS) status.)

b. ANSI X3V1.9 User-System Interfaces and Symbols committee: Working on a Voice Messaging User Interface Forum (VMUIF).

c. X Consortium: Data Stream Interface (Xlib).

d. X Consortium: Inter-Client Communications Conventions Manual (ICCCM).

3.3.3.1.6 Recommendations. The MIT X Consortium X11R5 Data Stream Encoding (X Protocol) is recommended in all procurements using a client-server computing architecture in a networked environment. It is specified in FIPS 158-1 and the NIST APP (NIST Special Publication 500-187). FIPS 158-1 is the current release of the government standard which adopts the MIT X Consortium X11R5 specification. If the X Protocol is required for a procurement, provision should be made for hard copy output systems to be delivered in a portable manner or for such systems to be developed in-house.

FIPS 158 is the original version of this standard and adopts the X11R3 specification. It is included in the table for support of legacy systems. Motif 1.2 is the reference version of the OSF specification for GUI behavior and appearance and programming and data interfaces.

3.3.3.2 Data stream interface. The data stream interface is a library of interfaces to the data stream and the graphical object library. It is not to be confused with a library of subroutines which implements graphical objects (e.g., Xt Intrinsics).

3.3.3.2.1 Standards. Table 3.3-7 presents standards for the data stream interface.

TABLE 3.3-7 Data stream interface standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	User Interface Component of the Applications Portability Profile (Adopts the X Protocol, Xlib Interface, Xt Intrinsics, and Bitmap Distribution Format of X11R5)	FIPS PUB 158-1:1993	Mandated (Approved)
CPC	OSF	Motif 1.2	Motif 1.2	Informational (Approved)
CPC	X/Open	XLIB - C Language Binding	C140 (8/91)	Informational (Approved)
CPC	MIT X Consortium	Data Stream Interface (Xlib)	X11R6 (1994)	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
GPC	NIST	X-Windows User Interface (same as in X11R3)	FIPS PUB 158	Informational (Superseded)

3.3.3.2.2 Alternative specifications. The following specifications are available only to support legacy systems:

a. Sun's X11/NeWS, which uses Sun's proprietary "libcps" library. This library is not compatible with the X Consortium's Xlib.

b. Application Programming Interface for Windows (APIW).

c. Systems Application Architecture (SAA)'s Presentation Manager.

These specifications are referenced here for completeness and are not recommended for use in systems which do not require support of legacy components.

3.3.3.2.3 Standards deficiencies. As no significant products are as yet available for the newly released X11R6, the previous version, X11R5, as adopted by FIPS 158-1, remains as the accepted secondary reference standard.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.3.2.4 Portability caveats. Sun Microsystems "libcps" library, included in X11/NeWS, is not compatible with the X Consortium's Xlib.

3.3.3.2.5 Related standards. The following standards are related to data stream interface or data stream interface standards:

a. X Consortium: X Protocol.
b. X Consortium: Xt Intrinsics.

3.3.3.2.6 Recommendations. The MIT X Consortium X11R5 Data Stream Interface (Xlib) is required in all procurements using a client-server computing architecture with a graphical user interface in a networked environment. It is specified in FIPS 158-1 and NIST Special Publication 500-187, Application Portability Profile (NIST APP). FIPS 158-1 is the current release of the government standard which adopts the MIT X Consortium X11R5 specification.

FIPS 158 is the original version of this standard and adopts the X11R3 specification. It is included in the table for support of legacy systems. Motif 1.2 is the current version of the OSF specification for GUI behavior and appearance and programming and data interfaces.

3.3.3.3 Subroutine foundation library. The subroutine foundation library is a library of basic objects to use in implementing or customizing a graphical user interface.

3.3.3.3.1 Standards. Table 3.3-8 presents standards for the subroutine foundation library.

TABLE 3.3-8 Subroutine foundation library standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	User Interface Component of the Applications Portability Profile (Adopts the X Protocol, Xlib Interface, Xt Intrinsics, and Bitmap Distribution Format of X11R5)	FIPS PUB 158-1:1993	Mandated (Approved)
CPC	X/Open	X Toolkit Intrinsics (Xt Intrinsics)	C160 (7/91)	Informational (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	MIT X Consortium	Subroutine Foundation Library (Xt Intrinsics)	X11R6 (1994)	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
GPC	NIST	X-Windows User Interface (same as in X11R3)	FIPS PUB 158	Informational (Superseded)

3.3.3.3.2 Alternative specifications. The following proprietary specifications are available for support of legacy systems:

a. X11/NeWS, which uses Sun Microsystems Xview Intrinsics, instead of the X Consortium's Xt Intrinsics.

b. Applications Programming Interface for Windows (APIW) Intrinsics.

c. IBM Presentation Manager.

3.3.3.3.3 Standards deficiencies. As no significant products are as yet available for the newly released X11R6, the previous version, X11R5, as adopted by FIPS 158-1, remains as the accepted secondary reference standard.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.3.3.4 Portability caveats. Sun's Xview Intrinsics included in X11/NeWs, is not compatible with the X Consortium's Xt Intrinsics.

Intrinsics from proprietary but widely-used offerings from Microsoft Windows' Presentation Manager, IBM's SAA Presentation Manager, and Apple Computer's Macintosh interface are not compatible with one another or with Xt Intrinsics.

3.3.3.3.5 Related standards. The following specifications are related to the subroutine foundation library or subroutine foundation library standards:

a. Open Software Foundation (OSF): Motif High-Level Toolkit.
b. X Consortium. Xlib.
c. Xview.
d. The News Toolkit (TNT).

3.3.3.3.6 Recommendations. The MIT X Consortium X11R5 Xt Intrinsics Subroutine Foundation Library is recommended in all procurements using a client-server computing architecture with a graphical user interface in a networked environment. It is specified in FIPS 158-1 and the NIST APP. FIPS 158-1 is the current release of the government standard which adopts the MIT X Consortium X11R5 specification.

FIPS 158 is the original version of this standard and adopts the X11R3 specification. It is included in the table for support of legacy systems. Motif 1.2 is the reference version of the OSF specification for GUI behavior and appearance and programming and data interfaces.

3.3.3.4 Raster data interchange. (This BSA appears in part 3, part 5, and part 6.) Raster data interchange MIL SPEC identifies the requirements to be met when raster graphics data represented in digital, binary format are delivered to the government. Raster graphics standards are standards for pixel-by-pixel representation of images. (See still image compression, section 3.5.8.2, for more facsimile standards suitable for raster data interchange.)

3.3.3.4.1 Standards. Table 3.3-9 presents standards for raster data interchange.

TABLE 3.3-9 Raster data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	User Interface Component of the Applications Portability Profile (Adopts the X Protocol, Xlib Interface, Xt Intrinsics, and Bitmap Distribution Format of X11R5)	FIPS PUB 158-1:1993	Mandated (Approved)
NPC/IPC	ANSI/ISO/IEC	Interfacing Techniques for Dialogues with Graphical Devices (CGI) - Functional Specification - Part 6: Raster	9636-6:1991	Mandated (Approved)
GPC	DOD (NIMA)	Raster Product Format (RPF)	MIL-STD-2411:1994	Mandated (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 1: Overview and Fundamental Principles (formerly Product Data Exchange Specification (PDES))	10303-1:1994	Informational (Approved)
CPC	X/Open	X Window System File Formats and Application Conventions (Bitmap Distribution Format (BDF))	C170 (7/91)	Informational (Approved)
GPC	NIST	General Aspects of Group 4 Facsimile Apparatus (Adopts EIA-536-1988)	FIPS PUB 149:1988	Informational (Approved)
GPC	NIST	Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus (Adopts EIA 538-1988)	FIPS PUB 150:1988	Informational (Approved)
GPC	NIST	Initial Graphics Exchange Specification (IGES) (adopts ASME/ANSI Y14.26M-1989) (IGES ver. 4)	FIPS PUB 177:1992	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-PRF-28000	Informational (Approved)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-PRF-28002	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Illustration Data : CGM Application Profile (based on FIPS 128)	MIL-PRF-28003	Informational (Approved)
NPC	ANSI/AIIM	Recommended Practice: File Format for Storage and Exchange of Images; Bi-Level Image File Format: Part 1	MS53-1993	Informational (Approved)
GPC	NIST	Standard for the Interchange of Large Format Tiled Documents	NISTIR 88-4017	Informational (Approved)
IPC	NATO	Analogue Video Standard for Aircraft System Applications	STANAG 3350	Informational (Approved)
IPC	NATO	Exchange Specifications for ARC Standardized Raster Graphics (ASRG)	STANAG 4387:1996	Informational (Approved)
IPC	NATO	Specifications for UTM/UPS Standardized Raster Products (USRP)	STANAG 7077	Informational (Approved)
IPC	ITU-T	Document Application Profile for the Interchange of Formatted Mixed Mode Document - Terminal Equipment and Protocols for Telematic Services	T.501 (1989)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ITU-T	Document Application Profile for the Interchange of Group 4 Facsimile Documents	T.503 (1991)	Informational (Approved)
NPC	AIIM	Interchange of Tiled Raster Documents	TR14:1988	Informational (Approved)
IPC	NATO	Exchange Specifications for ARC Digitized Raster Graphics (ADRG)	STANAG 7108	Informational (Draft)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-D-28000A(1) of 12/14/92	Informational (Superseded)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-R-28002B(1) of 9/20/1993	Informational (Superseded)

3.3.3.4.2 Alternative specifications. Currently IGES is the most mature and widely implemented standard for conveying product data information. Other bitmap formats include proprietary formats such as GIF, PCX, TIFF, RLE, and TGA. Except for support of legacy products, these formats are not recommended.

3.3.3.4.3 Standards deficiencies. Raster graphics files require enormous amounts of storage and must be supplemented by compression standards.

3.3.3.4.4 Portability caveats. A standard technique for raster data interchange should be selected for use throughout the DOD and applied wherever possible.

3.3.3.4.5 Related standards. The following standards are related to raster data interchange or raster data interchange standards:

a. ASME/ANSI Y14.28M-1989, which describes product design and manufacturing information.

b. ITU-T, facsimile transmission standards.

c. Raster compression standards.

3.3.3.4.6 Recommendations. The mandated standards are recommended for raster data interchange.

MIL PRF-28002 (Raster) can be used in a Computer-Aided Acquisition and Logistic Support (CALS) environment, and, when needed, supplemented by National Institute of Standards and Technology Interim Report (NISTIR) 88-4017 (tiling). FIPS Pub 150 can also be used. With only the CALS Raster standard available, no real tailoring guidance is possible. This version (MIL-PRF-28002) supports engineering drawings and technical manual illustrations. The previous CALS Raster standard (MIL-R-28002B) can be used for in-place and unrevised legacy data. Tiling (as in NISTIR 88-4017) and compression are desirable for very large raster graphics files. (See the Still image compression BSA, part 3.5.8.2 of the ITSG.) MIL-PRF-28003 (CGM)

offers the capability for having raster and vector graphics in the same file. The approved BDF provides conventions for font conversion/interchange between external and internal X Windows fonts and can be used in procurements using a client-server computing architecture with a graphical user interface in a networked environment. BDF can be compiled in Server Normal Format to be optimized for a particular server.

3.3.3.5 Communication between GUI client applications. Communications between GUI client applications is a functionality of a windowing system which includes the dynamic exchange of data and manual exchange via cut-and-paste operations between windows.

3.3.3.5.1 Standards. Table 3.3-10 presents standards for communication between GUI client applications.

TABLE 3.3-10 Communication between GUI client applications standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Inter-Client Communications Conventions Manual (ICCCM)	ICCCM Version 1.0	Mandated (Approved)
CPC	MIT X Consortium	Inter-Client Communications Conventions Manual (ICCCM)	ICCCM Version 1.0	Informational (Approved)
CPC	X/Open	Inter-Client Communications Conventions Manual (ICCCM)	ICCM	Informational (Approved)
GPC	NIST	User Interface Component of the APP Inter-Client Communications Conventions Manual (ICCCM)	FIPS PUB 158-2	Informational (Formative)

3.3.3.5.2 Alternative specifications. The only other available specifications are proprietary (e.g., Dynamic Data Exchange (DDE), Object Linking and Embedding(OLE)), and should be used only to support legacy products.

3.3.3.5.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.3.3.5.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.3.3.5.5 Related standards. The X Consortium's X Protocol is a standard which is related to interclient communications and interclient communications.

3.3.3.5.6 Recommendations. The OSF ICCCM is recommended in all procurements using a client-server computing architecture with a graphical user interface in a networked environment. It will be specified in FIPS 158-2. Note that this area is not covered in FIPS 158-1. FIPS 158-2 is a formative release of the government standard which adopts the MIT X Consortium X11R6 specification.

3.3.3.6 User Interface Management System. The User Interface Management System (UIMS) is a CASE-like GUI building tool, which can be used to develop GUI-based applications that are portable across platforms with different appearance and functionality.

3.3.3.6.1 Standards. Table 3.3-11 presents standards for the user interface management system.

TABLE 3.3-11 User Interface Management System standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	User Interface Component of the Applications Portability Profile (Adopts the X Protocol, Xlib Interface, Xt Intrinsics, and Bitmap Distribution Format of X11R5)	FIPS PUB 158-1:1993	Mandated (Approved)
CPC	OSF	Motif User Interface Management System (UIMS)	Motif 1.2	Informational (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)

3.3.3.6.2 Alternative specifications. The following specifications are also available to support legacy systems:

a. Carnegie Mellon University (CMU) Software Engineering Institute's (SEI) Serpent UIMS (unsupported).

b. NASA/Goddard Space Flight Center's (NASA) Transportable Application Environment (TAE+) (for Motif, based on X11R5).

3.3.3.6.3 Standards deficiencies. Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.3.6.4 Portability caveats. OSF's Motif User Interface Management System (UIMS) and USL's Xt+ user interface management systems are not compatible with one another.

3.3.3.6.5 Related standards. There are no related standards.

3.3.3.6.6 Recommendations. If a CASE-like GUI applications prototyping tool (set) is required for a procurement, a UIMS should be acquired that works with the proprietary product to which it is matched. No formal standards efforts are in progress.

FIPS 158-1 is recommended. It is the current release of the government standard that adopts the MIT X Consortium X11R5 specification. Motif 1.2 is the reference version of the OSF specification for GUI behavior and appearance and programming and data interfaces.

3.3.3.7 Data interchange format for GUI-based applications. A data interchange format for GUI-based applications allows data to be exchanged via a standard format between applications using different GUIs.

3.3.3.7.1 Standards. Table 3.3-12 presents standards for a data interchange format for GUI-based applications.

TABLE 3.3-12 Data interchange format for GUI-based applications standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Inter-Client Communications Conventions Manual (ICCCM)	ICCCM Version 1.0	Mandated (Approved)
CPC	MIT X Consortium	Inter-Client Communications Conventions Manual (ICCCM)	ICCCM Version 1.0	Informational (Approved)
CPC	MIT X Consortium	Inter-Client Communications Conventions Manual (ICCCM)	ICCCM (X11R6)	Informational (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
GPC	NIST	User Interface Component of the APP Inter-Client Communications Convntions Manual (ICCCM)	FIPS PUB 158-2	Informational (Formative)

3.3.3.7.2 Alternative specifications. The legacy supporting specification available is the Application Programming Interface for Windows (APIW): Dynamic Data Exchange (DDE).

3.3.3.7.3 Standards deficiencies. The MIT X Consortium's ICCCM provides incomplete coverage, but now defines interapplication drag and drop.

As no significant products are as yet available for the newly released X11R6, the previous version, X11R5, as adopted by FIPS 158-1, remains as the accepted secondary reference standard.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.3.7.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.3.3.7.5 Related standards. The X Consortium's X Protocol is related to data interchange formats for GUI-based applications.

3.3.3.7.6 Recommendations. The OSF ICCCM is recommended in all procurements using a client-server computing architecture with a graphical user interface in a networked environment. It will be specified in FIPS 158-2. Note that this area is not covered in FIPS 158-1. FIPS 158-2 is a formative release of the government standard which adopts the MIT X Consortium X11R6 specification.

If a standard data interchange format for data to be exchanged between applications using different GUIs is needed, no complete specification is available. Some capability is provided in MIT's ICCCM for X Windows-based systems, while APIW-based applications can exchange data between conforming applications using MS's DDE software.

3.3.3.8 X Logical Font Description. The X logical font description is a format for fonts in use in the X Windows System.

3.3.3.8.1 Standards. Table 3.3-13 presents standards for X logical font description.

TABLE 3.3-13 X Logical Font Description standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	X Logical Font Description (XLFD)	XLFD Version 1.3	Adopted (Approved)
CPC	MIT X Consortium	X Logical Font Description (XLFD)	XLFD Version 1.3	Informational (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)

3.3.3.8.2 Alternative specifications. The only other available specifications are proprietary.

3.3.3.8.3 Standards deficiencies. Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.3.8.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.3.3.8.5 Related standards. The X Consortium's X Window System is related to X Logical Font Description.

3.3.3.8.6 Recommendations. The X Logical Font Description (XLFD) is recommended to provide standardized conventions for client applications to query and access fonts across all X servers in a procurement. Motif 1.2 is the reference version of the OSF specification for GUI behavior and appearance and programming and data interfaces. This standard equivalently includes the X Logical Font Description.

3.3.3.9 Compound text encoding. A compound document is composed of a variety of data types and formats. Each data type is linked to the application used to create it. A compound document might include audio, video, images, text, and graphics.

3.3.3.9.1 Standards. Table 3.3-14 presents standards for compound text encoding.

TABLE 3.3-14 Compound text encoding standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Compound Text Encoding (CTE)	CTE Version 1.1	Adopted (Approved)
CPC	MIT X Consortium	Compound Text Encoding (CTE)	CTE Version 1.1	Informational (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)

3.3.3.9.2 Alternative specifications. No other specifications are available.

3.3.3.9.3 Standards deficiencies. Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.3.9.4 Portability caveats. OSF's Motif support of two CTEs can result in portability problems.

3.3.3.9.5 Related standards. The X Consortium's X Window System is related to compound text encoding.

3.3.3.9.6 Recommendations. The CTE for a standards-based X Windows interchange format for multiple character sets in a procurement is recommended. Motif 1.2 is the current version of the OSF specification for GUI behavior and appearance and programming and data interfaces. This standard equivalently specifies a Compound Text Encoding standard.

3.3.3.10 Uniform API. A uniform GUI API toolkit is a software library defining a layer between application specific code and a system specific GUI code, as defined by a platform or system specific toolkit (API). It does not directly provide window or graphics support, but it should allow software developers to write their applications to one common interface regardless of the underlying (native) GUI of a particular system or platform.

3.3.3.10.1 Standards. Table 3.3-15 presents standards for a uniform API.

TABLE 3.3-15 Uniform API standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.3.3.10.2 Alternative specifications. The following specifications are available:

a. Planning Research Corporation's (PRC) THINGS (The Higher-Level Interface-Non-GUI Specific): A public domain specification developed under a U. S. Air Force Contract.

b. TAE Plus (Transportable Applications Environment Plus): A public domain window programming tools specification developed by the NASA/Goddard Space Flight Center and Century Computing, Inc.

3.3.3.10.3 Standards deficiencies. No standards exist for UAPIs.

3.3.3.10.4 Portability caveats. All existing UAPIs are proprietary products. There are no standards for their implementation.

3.3.3.10.5 Related standards. The following standards are related to GUI uniform toolkit APIs:

a. IEEE P1201.2: Drivability (recommended practice, in ballot).
b. OSF: Motif.

3.3.3.10.6 Recommendations. The IEEE P1201.1 working group, which was attempting to produce a standard in this area, has disbanded. There is a lack of interest in this area by the commercial software community. A number of proprietary products are available for the development of cross-platform applications based upon a uniform API. All existing UAPIs are proprietary products. There are no standards for their implementation. If a proprietary UAPI toolkit must be selected, one supporting Ada should be chosen.

3.3.3.11 X Windows over OSI. (This BSA appears in part 3 and part 11.) These are standards for implementing the X Window System in an application running on the Open Systems Interconnection (OSI) protocol stack.

3.3.3.11.1 Standards. Table 3.3-16 presents standards for X Windows over OSI.

TABLE 3.3-16 X Windows over OSI standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	MIT X Consortium	X Windows Over OSI	X11R6	Informational (Formative)

3.3.3.11.2 Alternative specifications. The only other available specifications are proprietary.

3.3.3.11.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.3.3.11.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.3.3.11.5 Related standards. The following standards are related to implementing X Windows over the OSI stack:

a. X Consortium: X Window System.
b. ISO: OSI Stack.

3.3.3.11.6 Recommendations. No formal standard is available to support a procurement for X Windows running on the OSI stack and none is in progress. The MIT X Consortium intends to incorporate a version of the European Workshop for Open Systems (EWOS) X Windows over OSI specification in a future X11 release (X11R6), which probably will be adopted by X/Open and appear in a future version of FIPS 146, the Government Open Systems Interconnection Profile. The manner in which X11R6 handles "safe threading" to support multi-threaded applications is inconsistent with the Motif 2.0 standard, which is based upon X11R5. Motif 2.0 will execute on X11R6, but thread-safe operation is not assured. X11R6 is the current version of the X Windows Version 11 GUI standard.

3.3.4 Object definition and management. GUI object definitions are display objects specifications that define characteristics of display elements such as color, shape, size, movement, graphics context, user preferences, interactions among display elements.

3.3.4.1 Application programming interfaces. An application programming interface (API) is a library of predefined higher-level objects which defines a programming "layer" to facilitate development of applications. A GUI API usually is designed to implement a GUI for a particular environment and, therefore, may not produce portable applications. A uniform GUI API supports common functionality across operating systems and platforms specifically to promote portability.

3.3.4.1.1 Standards. Table 3.3-17 presents standards for application programming interfaces.

TABLE 3.3-17 Application programming interfaces standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Services and Applications	C323 (4/95)	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Definitions and Infrastructure	C324 (4/95)	Mandated (Approved)
NPC	IEEE	Modular Toolkit Environment (MTE)	1295:1993	Informational (Approved)
IPC	ECMA	Application Programming Interface for Windows (APIW)	234 (1995)	Informational (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
CPC	OSF	CDEnext/Motif (CDE/Motif under OSF Prestructured Technology (PST))	CDE/Motif PST	Emerging (Formative)

3.3.4.1.2 Alternative specifications. The only other available specifications are proprietary and should only be used to support legacy software.

3.3.4.1.3 Standards deficiencies. Formal and government standards will not be available in the near-to-medium term.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 is resolved.

3.3.4.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.3.4.1.5 Related standards. The following standards are related to APIs or API standards:

a. ISO/IEC JTC 1/SC18/WG9: Working on a VMUIF. (This effort moves the ANSI work of X3V1.9 to ISO status.) The group also is developing standards for user interfaces and symbols associated with text and office systems.)

b. ISO DIS 11730 FIMS.

c. ANSI X3V1.9 User-System Interfaces and Symbols committee: Working on a VMUIF.

3.3.4.1.6 Recommendations. The Common Desktop Environment (CDE) is recommended. CDE is a unified UNIX interface based on a highly customized Motif toolkit. Initially developed by the Common Open Software Environment (COSE), it is now part of a unified, vendor-neutral development of CDE, Motif, and the X Window System under the X Consortium. CDE provides a more modern and robust GUI interface than Motif for POSIX platforms as well as a more robust development environment. CDE is found in two companion documents, C323 and C324.

The IEEE 1295 standard is based upon a C language binding to Motif. A number of products are available which support the development of applications using an IEEE 1295 like Ada API interface. An IEEE study group is currently beginning the process of specifying an Ada-95 binding to MTE (IEEE 1295) and Motif. IEEE 1295 adopts the C language toolkit defined by the OSF/Motif 1.2 specification. Motif 1.2 is the current version of the OSF specification for GUI behavior and appearance and programming and data interfaces.

An ECMA working group has developed an API specification for Windows based upon MS Windows 3.1 functionality. This specification will provide an ISO open standard for interfacing to MS Windows and similar alternate GUIs.

3.3.4.2 User Interface Definition Language. A User Interface Language (UIL) is a rapid prototyping tool that simplifies programming of GUI-based applications. It allows application developers to create a file containing a high-level description of an interface's graphical objects and resources.

3.3.4.2.1 Standards. Table 3.3-18 presents standards for user interface definition language.

TABLE 3.3-18 User Interface Definition Language standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Motif User Interface Language (UIL)	Motif AES 1.2	Mandated (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)

3.3.4.2.2 Alternative specifications. The only other available specifications are proprietary and are not recommended except in support of legacy systems.

3.3.4.2.3 Standards deficiencies. Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.4.2.4 Portability caveats. The OSF Motif User Interface Language (UIL)/User Interface Management Services (UIMS) and the USL Xt+ user interface definition languages are not compatible with one another.

3.3.4.2.5 Related standards. The only other available specifications are proprietary.

3.3.4.2.6 Recommendations. Motif UIL is recommended. A UIL usually is contained within a UIMS. A UIMS may contain a UIL with additional tools. Motif 1.2 is the current version of the OSF specification for GUI behavior and appearance and programming and data interfaces. It includes the specification of the UIL.

3.3.4.3 Graphical user interface style guides. A GUI's style guide, which is part of the presentation management layer in the NIST's User Interface Reference Model, specifies a standard "look" for the GUI of an application to the user.

3.3.4.3.1 Standards. Table 3.3-19 presents graphical user interface style guides.

TABLE 3.3-19 Graphical user interface style guides standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
CPC	OSF	Motif Style Guide	Motif SG Rev. 1.2:1992	Mandated (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
IPC	NATO	Principles of Presentation of Information in Aircrew Stations	STANAG 3705	Informational (Approved)
GPC	DOD	User/Computer Interface	MIL-STD-1801 29 May 1987	Informational (Approved)
GPC	DOD	Human Engineering Performance Requirements for Systems	MIL-STD-1800A 10 Oct. 1990	Informational (Approved)
GPC	DOD	DOD Handbook, Human Engineering Guidelines for Management Information Systems	MIL-HDBK-761A 30 Sep. 1989	Informational (Approved)
GPC	DOD	Guidelines for Designing User Interface Software	ESD-TR-86-278	Informational (Approved)
GPC	DOD	Air Force Intelligence Data Handling System (IDHS) Style Guide	IDHS Style Guide 1990	Informational (Approved)
GPC	DOD	Human Factors Guidelines for the Army Tactical Command and Control System (ATCCS) Soldier-Machine Interface	ATCCS Guidelines v.1.0 and v.2.0, 1990 and 1992	Informational (Approved)
GPC	DOD	The User Interface Specifications for Navy Command and Control Systems	Navy CCS, Version 1.1, 1992	Informational (Approved)
GPC	DOD	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	MIL-STD-1472D Notice 2, 30 June 1992	Informational (Approved)
GPC	DOD	Human Engineering Guidelines for Management Information Systems	DOD-HDBK-71A (DOD 1989c)	Informational (Approved)
GPC	DOD	Human Engineering Requirements for Military Systems, Equipment, and Facilities	MIL-STD-46855B 26 May 1994	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
GPC	DOD	Department of Defense Intelligence Information Systems Style Guide	DODIIS Style Guide, 10/91	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 10: Dialogue principles	9241-10:1996	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 11: Guidance on usability specifications and measures	9241-11	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 12: Presentation of information	9241-12	Informational (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 13: User guidance	9241-13	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 14: Menu dialogs	9241-14	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 15: Command language dialogs	9241-15	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Officer Work with VDTs Part 16: Direct manipulation dialogs	9241-16	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 17: Form-filling dialogs	9241-17	Informational (Draft)
IPC	ISO/IEC	Graphical Symbols Used on Screens: Interactive Icons	11581	Informational (Draft (CD))
NPC	IEEE	Recommended Practice for Graphical User Interface Drivability	P1201.2	Informational (Draft (Project being canceled, lack of progress))
GPC	DOD	Joint Satellite Control (JSC) Human Computer Interface Standard, Version 1.0	JSC HCI Std., 1.0	Informational (Draft)

3.3.4.3.2 Alternative specifications. Several applicable consortia or de facto style guides are available for software user interfaces. These style guides promote consistency in user interface design across applications. However, conformance with one or more the style guides listed below does not guarantee conformance with ergonomic standards (e.g., ISO 9241). These style guides include:

a. The Windows Interface: An Application Design Guide (Microsoft)

b. Object-Oriented Interface design: IBM Common User Access Guidelines (IBM)

c. Macintosh Human Interface Guidelines (Apple Computer)

d. SAA Presentation Manager Style Guide/ Common User Access (CUA) (IBM)

e. Standard User Interface Style Guide for Compartmented Mode Workstations (Defense Intelligence Agency (DIA))

f. Compartmented Mode Workstation Labeling: Source Code and User Interface Guidelines (DIA)

g. Air Force Standard Systems Center GUI Style Guide, SSCR 700-10, Vol I

h. User Interface Specifications for the Global Command and Control System (GCCS), Version 1.0, draft, October 1994

i. Theater Battle Management Style Guide (U.S. Navy)

j. Army Theater Battle Management HCI Specification

k. Navy JMCIS.

3.3.4.3.3 Standards deficiencies. Currently, conformance to parts 12-17 of the ISO 9241 standard is on a part-by-part basis. There is concern that the overall standard may thus fail to address potential ergonomic problems arising from interactions between the user interface elements covered by the individual parts.

There is concern that ISO/IEC 11581 may contain overly rigid specifications for the set of icon shapes that can be used to represent different user interface parts.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.4.3.4 Portability caveats. NIST FIPS 158-1 (User Interface Component of the Applications Portability Profile) mandates the use of the X Window protocol, X library, and X toolkit intrinsics. IEEE P1201.2, when completed, is intended to increase the level of user interface consistency (and thus user interface portability) across X Windows-based environments. There are potential conflicts here.

DOD HCI Style Guide is based on (and intended to supersede) the Army, Navy, Air Force, and DODIIS style guides cited in the table above. The goal of this effort is to minimize unnecessary user interface diversity across DOD systems. There are potential problems with systems designed to accommodate different style guides.

MIL-STD-1800 is an Air Force-only standard that duplicates MIL-STD-1472D and is largely ignored in Air Force acquisitions. It has been recommended that MIL-STD-1800 be canceled and any value added material be added to MIL-STD-1472D.

3.3.4.3.5 Related standards. The following standards are related to user interface style guides:

a. ISO 9241-1:1992, Ergonomic requirements for office work with VDTs, part 1: Introduction, presents an overview of the content and usage of the multipart ISO 9241 standard. A revised version of ISO 9241-1 is currently at the CD level and will soon be released for DIS ballot.

b. ISO 9241-2:1992, Ergonomic requirements for office work with VDTs, part 2: Task Requirements, present an overview of factors that should be considered when designing tasks to be performed in a specific computing environment.

c. ISO CD 10075-2, Ergonomic principles related to mental work load -- Part 2: Design Principles, gives guidance on the design of work systems in general, with the intention of providing optimal working conditions with respect to health and safety, well- being, performance, and effectiveness.

d. MIL-STD-1908 (1992), Definition of Human Factors Terms.

e. NIST FIPS 158-1, User Interface Component of the Applications Portability Profile.

f. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

g. MIL-HDBK-759B(2) (1993) Human Factors Engineering Design for Army Materiel. (Draft 759C is complete.)

h. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

i. DOD-HDBK-743A (1991) Anthropometry of U.S. Military Personnel.

j. ITU-T E.134 Human Factors Aspects of Public Terminals: Generic Operating Procedures.

k. An ISO work item for a standard on "Human-Centered design" has been approved, but no working draft has yet been released for comment.

3.3.4.3.6 Recommendations. A style guide is necessary for development of all GUIs. There are no formal standards efforts in this area. A style guide is part of the Presentation Layer in NIST FIPS 158-1. Procurements that require software user interfaces to be addressed by ergonomic standards can require conformance with standards for menu structures, command languages, direct manipulation dialogs, forms-based dialogs, windowing, icons, screen formatting, information coding, and user guidance.

It is recommended that the practices of the DOD HCI Style Guide, TAFIM, Volume 8 be followed. It provides a common framework for HCI design and implementation with emphasis on standard look and feel for GUI based applications. As many aspects of standard GUI style are application specific, application area style guides should also be used when available. Motif 1.2 is the current version of the OSF specification for GUI behavior and appearance and programming and data interfaces. It includes a style guide for GUI interfaces and is also recommended.

Parts 1 and 2 of the ISO 9241 standard are informative; parts 10 and 11 are expected to be informative on completion. Parts 12-17 are expected to be normative on completion. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product. The ISO/IEC 11581 standard is expected to be normative on completion.

3.3.4.4 Three-dimensional appearance. Modern, color GUI applications make use of a three-dimensional appearance which is more pleasing to the user than the older two-dimensional appearance of monochrome GUIs.

3.3.4.4.1 Standards. Table 3.3-20 presents standards for three-dimensional appearance.

TABLE 3.3-20 Three-dimensional appearance standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	User Interface Component of the Applications Portability Profile (Adopts the X Protocol, Xlib Interface, Xt Intrinsics, and Bitmap Distribution Format of X11R5)	FIPS PUB 1[illegible]-1:1993	Mandated (Approved)
CPC	MIT X Consortium	X Consortium's PHIGS-based 3-D Extension to the X Window System (PEX)	X11R5	Informational (Approved)
CPC	MIT X Consortium	X Consortium's PHIGS-based 3-D Extension to X Window System (PEX)	X11R6	Informational (Approved)

3.3.4.4.2 Alternative specifications. The only other available specifications are proprietary.

3.3.4.4.3 Standards deficiencies. As no significant products are as yet available for the newly released X11R6, the previous version, X11R5, as adopted by FIPS 158-1, remains as the accepted secondary reference standard.

3.3.4.4.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.3.4.4.5 Related standards. The standard related to integration of 3-D graphics with GUIs is ISO 9592-1, -2, -3: PHIGS (Programmers Hierarchical Interactive Graphics System).

3.3.4.4.6 Recommendations. Conformance to FIPS 158-1, which subsumes PHIGS Extension to X (PEX), is required. 3-D extensions to X Windows based on the PHIGS graphics standard (ISO 9592) are needed. FIPS 158-1 is the current release of the government standard which adopts the MIT X Consortium X11R5 specification. These standards specify the PHIGS Extension to X Windows (PEX).

3.3.4.5 Interchange format for design tools. A common, GUI-independent Interchange Format for Interactive Design Tools (IDTIF) would allow different tools for developing interactive graphical windowing applications to exchange graphic objects and basic screen information.

3.3.4.5.1 Standards. Table 3.3-21 presents standards for interchange formats for design tools.

TABLE 3.3-21 Interchange format for design tools standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Services and Applications	C323 (4/95)	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Definitions and Infrastructure	C324 (4/95)	Mandated (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
CPC	OSF	OSF User Interface Management System (UIMS) Working Group	UIMS WG	Informational (Formative)
CPC	OSF	CDE/Motif (CDE/Motif under OSF Prestructured Technology (PST))	CDE/Motif PST	Emerging (Formative)

3.3.4.5.2 Alternative specifications. No other consortia or de facto specifications are available.

3.3.4.5.3 Standards deficiencies. Interactive Design Tools (IDT) that want to interchange graphic objects and screen information need a common GUI-independent Interchange Format (IF). There are few of these tools (IDTs), and they do not have a common IDTIF. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.4.5.4 Portability caveats. Portability problems with the existing specification are unknown.

3.3.4.5.5 Related standards. No standards are related to design tool interchange format standards.

3.3.4.5.6 Recommendations. Consortia work on IDTIF specifications is in the early stages. Tools must be procured for specific GUIs, and these cannot work with tools for other GUIs.

The Common Desktop Environment (CDE) is recommended. CDE is a unified UNIX interface based on a highly customized Motif toolkit. Initially developed by the Common Open Software Environment (COSE), it is now part of a unified, vendor-neutral development of CDE, Motif, and the X Window System under the X Consortium. CDE provides a more modern and robust GUI interface than Motif for POSIX platforms as well as a more robust development environment. CDE is found in two companion documents, C323 and C324.

3.3.4.6 Customization to local norms. (This BSA appears in part 3, User Interface, part 13, Human Factors, and part 14, Internationalization.) Customization to local norms involves modification of the key mapping to accommodate the local language and display of data in the commonly-used format (e.g., numbers, dates, time).

3.3.4.6.1 Standards. Table 3.3-22 presents standards for customization to local norms.

TABLE 3.3-22 Customization to local norms standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
CPC	X/Open	Internationalisation Guide, version 2	G304 (7/93)	Informational (Approved)
CPC	X/Open	Locale Registry Procedures	G303 (1993)	Informational (Approved)
CPC	OSF	Motif 1.2 (consistent with X/Open's NLS specifications & also double-byte character sets)	Motif 1.2	Informational (Approved)
CPC	MIT X Consortium	X Window System (X font manager- includes double-byte character sets)	X11R5	Informational (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
GPC	DOD	Military Standard Keyboard Arrangements	MIL-STD-1280, Notice 1, 1969	Informational (Approved)
GPC	DOD	User/Computer Interface	MIL-STD-1801 29 May 1987	Informational (Approved)
GPC	DOD	Human Engineering Performance Requirements for Systems	MIL-STD-1800A 10 Oct. 1990	Informational (Approved)
GPC	DOD	DOD Handbook, Human Engineering Guidelines for Management Information Systems	MIL-HDBK-761A 30 Sep. 1989	Informational (Approved)
GPC	DOD	Guidelines for Designing User Interface Software	ESD-TR-86-278	Informational (Approved)
GPC	DOD	Department of Defense Intelligence Information Systems Style Guide	DODIIS Style Guide, 10/91	Informational (Approved)
GPC	DOD	Air Force Intelligence Data Handling System (IDHS) Style Guide	IDHS Style Guide 1990	Informational (Approved)
GPC	DOD	Human Factors Guidelines for the Army Tactical Command and Control System (ATCCS) Soldier-Machine Interface	ATCCS Guidelines v.1.0 and v.2.0, 1990 and 1992	Informational (Approved)
GPC	DOD	The User Interface Specifications for Navy Command and Control Systems	Navy CCS, Version 1.1, 1992	Informational (Approved)
GPC	DOD	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	MIL-STD-1472D Notice 2, 30 June 1992	Informational (Approved)
GPC	DOD	Human Engineering Guidelines for Management Information Systems	DOD-HDBK-71A (DOD 1989c)	Informational (Approved)
CPC	X/Open	Distributed Internationalisation Services	S213 (11/92)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Internationalisation of Internetworking Specifications	S302 (4/93)	Informational (Approved)
CPC	X/Open	File System Safe UCS Transformation Format (FSS-UTF)	P316 (1993)	Informational (Approved)
CPC	X/Open	System Interface and Headers, Issue 3	C212 (3/92)	Informational (Approved)
CPC	X/Open	Supplementary Definitions, Issue 3	C213 (3/92)	Informational (Approved)
CPC	X/Open	Universal Multiple-Octet Coded Character Set Coexistence and Migration	E401 (3/94)	Informational (Approved)
NPC	ANSI/SAE	Human Interface Design Methodology for Integrated Display Symbology	ARP 4155 (1990)	Informational (Approved)
GPC	DOD	Human Engineering Requirements for Military Systems, Equipment, and Facilities	MIL-STD-46855B 26 May 1994	Informational (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Informational (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Informational (Approved)
CPC	X/Open	Locale Registry Procedures, Version 2	G502 (5/95)	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
CPC	X/Open	Internationalisation Guide, Version 3	G503 (11/95)	Informational (TBD)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 11: Guidance on usability specifications and measures	9241-11	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 12: Presentation of information	9241-12	Informational (Draft)
NPC	IEEE	Recommended Practice for Graphical User Interface Drivability	P1201.2	Informational (Draft (Project being canceled, lack of progress))
GPC	DOD	Joint Satellite Control (JSC) Human Computer Interface Standard, Version 1.0	JSC HCI Std., 1.0	Informational (Draft)

3.3.4.6.2 Alternative specifications. Several applicable consortia or de facto style guides are available for internationalization. However, conformance with one or more the style guides listed below does not guarantee conformance with ergonomic standards:

a. The Windows Interface: An Application Design Guide (Microsoft)
b. Object-Oriented Interface design: IBM Common User Access Guidelines (IBM)
c. Macintosh Human Interface Guidelines (Apple Computer).

3.3.4.6.3 Standards deficiencies. Currently, conformance to parts 12-17 of the ISO 9241 standard is on a part-by-part basis. There is concern that the overall standard may thus fail to

address potential ergonomic problems arising from interactions between the user interface elements covered by the individual parts.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.4.6.4 Portability caveats. Although Motif supports the X/Open Native Language System, it also supports a number of its own internationalization extensions which makes it incompatible with some legacy specifications.

NIST FIPS 158-1 (User Interface Component of the Applications Portability Profile) mandates the use of the X Window protocol, X library, and X toolkit intrinsics. IEEE P1201.2, when completed, is intended to increase the level of user interface consistency (and thus user interface portability) across X Windows-based environments. There are potential conflicts here.

The DOD HCI Style Guide is based on (and intended to supersede) the Army, Navy, Air Force, and DODIIS style guides cited in the table above. The goal of this effort is to minimize unnecessary user interface diversity across DOD systems. There are potential problems with systems designed to accommodate different style guides.

3.3.4.6.5 Related standards. The following standards are related to cultural convention services:

a. X/Open Internationalisation Locale: L001 (1994): ja_JP - Japanese for Japan.

b. X/Open Internationalisation Locale: L002 (1994): da_DK - Danish for Denmark.

c. X/Open Internationalisation Locale: L003 (1994): de_AT - German for Austria.

d. X/Open Internationalisation Locale: L004 (1994): en_DK - English for Denmark.

e. X/Open Internationalisation Locale: L005 (1994): fo_FO - Faroese for the Faroes.

f. X/Open Internationalisation Locale: L006 (1994) is_IS - Icelandic for Iceland.

g. X/Open Internationalisation Locale: L007 (1994) kl_GL - Greenlandic for Greenland.

h. X/Open Internationalisation Locale: L008 (1994) lt_LT - Lithuanian for Lithuania.

i. X/Open Internationalisation Locale: L009 (1994): lv_LV - Latvian for Latvia.

j. X/Open Internationalisation Locale: L010 (1994): de_CH - German for Switzerland.

k. X/Open Internationalisation Locale: L011 (1994): de_DE - German for Germany.

l. X/Open Internationalisation Locale: L012 (1994): en_GB - English for Great Britain.

m. X/Open Internationalisation Locale: L013 (1994): en_IE - English for Ireland.

n. X/Open Internationalisation Locale: L014 (1994): en_US - English for the U.S.A.

o. X/Open Internationalisation Locale: L015 (1994): hu_HU - Hungarian for Hungary.

p. X/Open Internationalisation Locale: L016 (1994): it_IT - Italian for Italy.

q. X/Open Internationalisation Locale: L017 (1994): nl_NL - Dutch for the Netherlands.

r. X/Open Internationalisation Locale: L018 (1994): pl_PL - Polish for Poland.

s. X/Open Internationalisation Locale: L019 (1994): pt_PT - Portuguese for Portugal.

t. X/Open Internationalisation Locale: L020 (1994): ro_RO - Romanian for Romania.

u. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

v. MIL-STD-1908 (1992) Definitions of Human Factors Terms.

w. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

3.3.4.6.6 Recommendations. Procurements that require software user interfaces to be addressed by ergonomic standards can require conformance with standards for menu structures, command languages, direct manipulation dialogs, forms-based dialogs, windowing, icons, screen formatting, information coding, and user guidance.

Parts 1 and 2 of the ISO 9241 standard are informative; parts 10 and 11 are expected to be informative on completion. Part 3 of the ISO 9241 standard is normative; parts 2-9 and 12-17 are expected to be normative on completion. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product.

Procurements must recognize the difference between informative and normative parts of the standard in question. Where possible, both the informative and normative parts should be required for the best implementation of modern human factors/ergonomic thinking. In general, conformance tests for informative parts will not be available.

The DOD HCI Style Guide is recommended for customization to local norms.

3.3.4.7 Language bindings for GUIs. These are specifications for language bindings for the display, manipulation, and management of objects in windows on a raster graphics screen.

3.3.4.7.1 Standards. Table 3.3-23 presents standards for language bindings for GUIs.

TABLE 3.3-23 Language bindings for GUIs standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	Modular Toolkit Environment (MTE)	1295:1993	Informational (Approved)
CPC	OSF	Motif binding to C	Motif 1.2	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)

3.3.4.7.2 Alternative specifications. The following specifications are also available for support of legacy systems:

a. Rational Systems implements Xlib with an Ada binding.
b. The Software Technology for Adaptable, Reliable Systems (STARS) program has an Ada binding for Xlib and Xt Intrinsics.
c. APIW.
d. Ada bindings for Motif.

3.3.4.7.3 Standards deficiencies. The X Window system was designed with the C language in mind. Ada code can interface with the X libraries, which are written in C, but fundamental semantic incompatibilities exist between the Ada and C programming languages.

No open-standard bindings are present from Ada to any GUI or GUI toolkit, so an Ada application will have to be written to a GUI/toolkit using a nonstandard binding with portability severely compromised.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.4.7.4 Portability caveats. Although Ada compiler vendors are required by the Ada Language Reference Manual to provide the capability for Ada to call routines written in other languages, they are not required to provide a capability that allows routines written in other languages to call Ada programs. The result is reduced portability, interoperability, and integratability between the X Window system and Ada systems.

3.3.4.7.5 Related standards. GUI standards and language standards are related.

3.3.4.7.6 Recommendations. An IEEE study group has begun work on the specification of an Ada-95 binding to IEEE 1295/Motif. Several proprietary products are available which supply an Ada-83 binding to Motif. Most of these interface to C function libraries (Xlib, Xt Intrinsics), although at least one such product has directly reprogrammed these libraries into Ada-83. If an Ada application must be interfaced via an IEEE 1295 C binding, a layered approach should be taken which limits the direct calls of C functions by the application. This will allow a smoother transition to a future standard Ada binding to Motif. Program managers for procurements specifying graphical windowing interfaces should take a practical and realistic approach in view of the current lack of a standard for Ada bindings to GUIs. Choice of an existing library which takes this layering approach is desirable.

IEEE 1295 adopts the C language toolkit defined by the OSF/Motif 1.2 specification. Motif 1.2 is the current version of the OSF specification for GUI behavior and appearance and programming and data interfaces.

3.3.4.8 Visualization. (This BSA appears in part 3, User Interface, and part 13, Human Factors.) Visualization is the method of displaying data in a graphical manner to aid in recognition of patterns and trends in data and to give the viewer a depiction of a physical system that has been modeled by data points (e.g., finite element analysis (FEA) and computational fluid dynamics (CFD)). Another technique is the visualization user interface (VUI), a GUI that interprets text and numbers as pictures to show their relative scales and other relationships. A VUI remodels data so that text and numbers are hidden behind a picture expressing their complex relationships. Engineering visualization is a term freely applied to almost any intersection where the engineering process meets image creation technologies.

3.3.4.8.1 Standards. Table 3.3-24 presents standards for visualization.

TABLE 3.3-24 Visualization standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI/SAE	Aerodynamic Flow Visualization Techniques and Procedures	HS J1566 - 1986	Informational (Approved)

3.3.4.8.2 Alternative specifications. There are no alternative specifications available, but extensive academic research on this topic is taking place, particularly in the University of Maryland's Human-Computer Interaction Laboratory and the Software Psychology Society. Topics include using treemaps for visualizing hierarchical information, using statistical distortion to promote the detection of outlying data, and use of color coding as a visualization aid.

3.3.4.8.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.3.4.8.4 Portability caveats. Portability problems with the existing standards are unknown.

3.3.4.8.5 Related standards. The following standards are related to visualization standards:

a. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems

b. MIL-STD-1800A (1990) Human Engineering Performance Requirements for Systems

c. MIL-STD-1908 (1992) Definitions of Human Factors Terms

d. MIL-HDBK-761A (1989) Human Engineering Guidelines for Management Information Systems

e. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

3.3.4.8.6 Recommendations. There are no recommendations for visualization itself, but it does require the use of power graphics generation if a dynamic system will be shown, rather than a

series of static views. Other requirements can include a high degree of mathematical precision and single-pixel accuracy in rendering.

3.3.4.9 Color use. (This BSA appears in part 3, User Interface, and part 13, Human Factors.) The use of color is a vital part of communication with the user of computer applications. Computer representation of color is done through the use of the Red, Green, Blue (RGB) color separation method which must be used to approximate color definitions used in graphic technologies.

3.3.4.9.1 Standards. Table 3.3-25 presents standards for color use.

TABLE 3.3-25 Color use standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
IPC	CIE	Recommendations on Uniform Color Spaces, Color-Difference Equations, and Psychrometric Color Terms	CIE Pub. 15, Suppl. 2 (1986)	Informational (Approved)
IPC	NATO	Aircraft Electronic Colour Display Systems	STANAG 3940 (1991)	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 8: Requirements for displayed colors	9241-8	Informational (Draft)

3.3.4.9.2 Alternative specifications. Alternative specifications include any user interface style guide that addresses the use and meaning of color.

3.3.4.9.3 Standards deficiencies. Comparison of color defined by the existing standards assumes identical viewing conditions. There are no standards directly addressing comparisons across viewing environments, although developers are working on models.

3.3.4.9.4 Portability caveats. Translation of color from one color definition system to another can be difficult and is only an approximation at best. There are three different color definitions from the CIE. They are CIEXYZ, CIELAB, and CIELUV. These standards have existed for a long time and are seen as the common basis for any future unifying definitions.

One problem with the use of color is color blindness. To accommodate the color blind, if color is used to convey important information, then a second method should also be used (such as brightness of the color).

3.3.4.9.5 Related standards. The following standards are related to human factors standards for the use of color:

a. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems

b. MIL-STD-1800A (1990) Human Engineering Performance Requirements for Systems

c. MIL-STD-1908 (1992) Definitions of Human Factors Terms

d. MIL-HDBK-761A (1989) Human Engineering Guidelines for Management Info. Systems

e. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

3.3.4.9.6 Recommendations. The approved standards in this section are recommended where they are applicable. The DOD HCI Style Guide is recommended, particularly section 4.3 which addresses the use and meaning of color.

3.3.5 Window management. Window management specifications define how windows are created, moved, stored, retrieved, removed, and related to each other.

3.3.5.1 Independent window management services. (This BSA appears both in part 3 and part 9.) Window management services are a necessary part of any windows system to perform functions such as resizing or moving windows. These services are not to be confused with services managing individual windows as though they were separate terminals.

3.3.5.1.1 Standards. Table 3.3-26 presents standards for independent window management services.

TABLE 3.3-26 Independent window management services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	Modular Toolkit Environment (MTE)	1295:1993	Informational (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	MIT X Consortium	X Window System (Tab Window Manager)	X11R5	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)

3.3.5.1.2 Alternative specifications. The following specifications are also available for legacy support:

a. APIW
b. USL/Sun Open Look Windows Manager (olwm)
c. IBM SAA Presentation Manager Window Manager.

3.3.5.1.3 Standards deficiencies. Although all window managers perform functions such as window resizing and moving (window manipulation), some do not manage their windows independently, as if each window were a separate system. Failure to manage windows independently may create situations in an application seizing in one window may propagate the errors to other windows causing the to seize (lock up). In addition, without an independent window manager, usually it is not possible to invoke programs that run in graphical mode at the same time (but in different windows on the same screen) as programs running in character mode. Certain windows systems running under single-tasking DOS also do not support independent window managers.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate

threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.5.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.3.5.1.5 Related standards. No standards are related to independent window management standards.

3.3.5.1.6 Recommendations. A procurement should specify a Windows Manager that accommodates window manipulation and application seizure protection. Windows systems using X Windows operating on protected operating systems like UNIX are more robust (i.e., the failure of one application will not cause other applications to fail automatically) than some running on the unprotected DOS operating system.

3.3.5.2 Multiple displays. Multiple display services allow the use of multiple, possibly heterogeneous, displays as separate windows within an application.

3.3.5.2.1 Standards. Table 3.3-27 presents standards for multiple displays.

TABLE 3.3-27 Multiple displays standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Motif	Motif 1.2	Adopted (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)

3.3.5.2.2 Alternative specifications. The only other available specifications are proprietary and should only be used to support legacy systems.

3.3.5.2.3 Standards deficiencies. Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is avaiable and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.5.2.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.3.5.2.5 Related standards. No standards are related to multiple display standards.

3.3.5.2.6 Recommendations. Motif 1.2 is the current version of the OSF specification for GUI behavior and appearance and programming and data interfaces. Motif 1.2 includes specifications for multiple physical displays used in the same logical display without downgrading the performance of the most advanced display to that of the least advanced.

3.3.5.3 Shared screens. Shared screen capabilities enable two or more workstations to display the same screen simultaneously. Changes made by one user can be seen by others as they are made. Shared screens can be implemented in two ways. One way enables people to view each other's screen, while one person makes changes. The other way enables people to run the same application on both screens so both users can make changes simultaneously.

3.3.5.3.1 Standards. Table 3.3-28 presents standards for shared screens.

TABLE 3.3-28 Shared screens standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.3.5.3.2 Alternative specifications. The only other available specifications are proprietary.

3.3.5.3.3 Standards deficiencies. There are no standards to have deficiencies.

3.3.5.3.4 Portability caveats. This is a high portability risk area because no standards exist.

3.3.5.3.5 Related standards. Currently, no standard specifies sharing and updating by two or more users on the same screen(s), and none are anticipated.

3.3.5.3.6 Recommendations. No standards-based way to require that screens be sharable and updatable by two or more communicating users working on the same screen(s) is available for a procurement, and no standards are anticipated.

3.3.5.4 On-line help. On-line help allows the user to access application reference material directly from the application or system through the computer.

3.3.5.4.1 Standards. Table 3.3-29 presents standards for on-line help.

TABLE 3.3-29 On-line help standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
NPC	IEEE	Recommended Practice for Graphical User Interface Drivability	P1201.2	Informational (Draft (Project being canceled, lack of progress))

3.3.5.4.2 Alternative specifications. The only other available specifications are proprietary.

3.3.5.4.3 Standards deficiencies. On-line help is included in the P1201.2 Drivability specification. However, this document is a "Recommended Practice" rather than an IEEE standard.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 are resolved.

3.3.5.4.4 Portability caveats. There are no known portability problems with the existing standards.

3.3.5.4.5 Related standards. No standards are related to on-line help standards.

3.3.5.4.6 Recommendations. The only specification for on-line help available for a procurement is the specification provided by the proprietary GUIs. The P1201.2 effort is not yet available. The DOD HCI Style Guide, TAFIM, Volume 8, is recommended for its partial specification.

3.3.5.5 Drivability. Drivability refers to the ease with which users may transfer from one GUI "look and feel" or application to another with minimal interference, errors, confusion, relearning, or retraining. The intent is to eliminate error provoking inconsistencies, misleading expectations about the results of user actions, gross inconsistencies in the high-level user model or metaphor, and incompatible motor control tendencies. This only relates to those aspects for which consistency is necessary to promote easy transfer among conforming environments.

3.3.5.5.1 Standards. Table 3.3-30 presents standards for drivability.

TABLE 3.3-30 Drivability standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
CPC	OSF	Motif Style Guide	Motif SG Rev. 1.2:1992	Mandated (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
NPC	IEEE	Recommended Practice for Graphical User Interface Drivability	P1201.2	Informational (Draft (Project being canceled, lack of progress))

3.3.5.5.2 Alternative specifications. The following specifications are also available:

a. APIW drivability
b. IBM: SAA's Common User Access (CUA).

3.3.5.5.3 Standards deficiencies. Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 is resolved.

3.3.5.5.4 Portability caveats. The IEEE P1201.2 Working Group, is producing a "Recommended Practice" rather than a mandatory standard. This specification uses the best features from commercial products, as well as features from various ISO standards and hur in-computer interface research. Its hybridization prevents it from being completely compatible with any particular commercial product. Portability problems can result if vendors selectively implement parts of P1201.2.

3.3.5.5.5 Related standards. The following standards are related to drivability or drivability standards:

a. ISO DIS 9995 Parts 1-7: Keyboard Layouts.

b. ISO TC159/SC4/WG5: This software Ergonomics and Man-Machine Dialog committee is developing parts of ISO 9241 ("Ergonomics of Visual Display Terminals").

c. ANSI X3V1.9 User-System Interfaces and Symbols committee: Working on a VMUIF.

d. ISO/IEC JTC 1/SC18/WG9: Working on a VMUIF. (This effort moves the ANSI work of X3V1.9 to ISO status.) The group also is developing standards for user interfaces and symbols associated with text and office systems.

e. ANSI HFS-HCI: This ANSI committee is working on drafts on the design process, information presentation, forms-based dialog, and window-based interaction.

3.3.5.5.6 Recommendations. The mandated standards are recommended. IEEE P1201.2 specifies recommended practice for drivability of GUI based applications. IEEE P1201.2 will be recommended for use once completed.

3.3.5.6 Commands, menus, and dialog services. In any software system it is necessary for users to command it to perform functions. In a GUI commands are entered either by pointing and clicking on a menu item, or by entering commands interactively in data entry windows known as dialogs. Dialog support services translate the data entered for display to that which is actually displayed on the screen (e.g., cursor movements, keyboard data entry, external data entry devices).

3.3.5.6.1 Standards. Table 3.3-31 presents standards for command, menu, and dialog services.

TABLE 3.3-31 Commands, menus, and dialog services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
IPC	ISO	Software Ergonomics and Man-Machine Dialogue	TC159/SC4/WG5	Informational (Draft)

3.3.5.6.2 Alternative specifications. The following proprietary specifications are available for support of legacy systems:

a. IBM: SAA Presentation Manager
b. Microsoft: MS Windows.

3.3.5.6.3 Standards deficiencies. The emerging ISO standard on Software Ergonomics and Man-Machine Dialogue (under development in ISO TC159/SC4/WG5) contains only text-based style information rather than implementable specifications.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products is available and until potential conflicts between Motif 2.0 and X11R6 is resolved.

3.3.5.6.4 Portability caveats. Because the ISO effort only addresses style, products written to the ISO standard may not be portable.

3.3.5.6.5 Related standards. The following standards are related to dialog, command, and menu service standards:

a. ISO TC159/SC4/WG5: This software Ergonomics and Man-Machine Dialog committee is developing parts of ISO 9241 ("Ergonomics of Visual Display Terminals").

b. ISO 11730 Forms Interface Management System (FIMS).

c. ANSI HFS-HCI: This ANSI committee is working on the design process, information presentation, forms-based dialogs, and window-based interaction.

3.3.5.6.6 Recommendations. No strong recommendation can be made. For specifying how to enter commands in graphical menus through dialogs, only proprietary offerings are available for procurement. The ISO effort is in its early stages and, even when it is complete, it will not offer implementable specifications but, rather, style information.

The Human-Computer Interface (HCI) Style Guide is recomomended. This style guide provides a common framework for HCI design and implementation with emphasis on standard look and feel for GUI based applications.

3.3.5.7 Input device management and control. Input device management covers the keyboard, pointing devices, tablets, and touch screens which allow the user to control the application.

3.3.5.7.1 Standards. Table 3.3-32 presents standards for input device management and control.

TABLE 3.3-32 Input device management and control standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.3.5.7.2 Alternative specifications. The only other available specifications are proprietary.

3.3.5.7.3 Standards deficiencies. Such input devices as pointing devices, tablets, and touch screens have no input device service standards, and none are known to be developing.

3.3.5.7.4 Portability caveats. This is a high portability risk area because no standards exist.

3.3.5.7.5 Related standards. The following standards are related to input device management and control:

a. ISO DIS 9995 Parts 1-7: Keyboard Layouts.

b. ANSI X3V1.9 User-System Interfaces and Symbols committee: Working on a VMUIF.

c. ISO/IEC JTC 1/SC18/WG9: Working on a VMUIF. (This effort moves the ANSI work of X3V1.9 to ISO status.)

3.3.5.7.6 Recommendations. There are no recommendations.

3.3.5.8 Multimedia input APIs to windows-based systems. Multimedia input refers to the integration of windows systems with non-traditional computer input, such as audio (digital and voice) and video (photographic and full motion).

3.3.5.8.1 Standards. Table 3.3-33 presents standards for multimedia input APIs to windows-based systems.

TABLE 3.3-33 Multimedia input APIs to windows-based systems standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.3.5.8.2 Alternative specifications. The only other available specifications are proprietary.

3.3.5.8.3 Standards deficiencies. There are no multimedia API standards for windows-based systems, and none are known to be under development.

3.3.5.8.4 Portability caveats. This is a high portability risk area because no standards exist.

3.3.5.8.5 Related standards. The following standards are related to multimedia input APIs or their standards:

a. ANSI X3V1.9 User-System Interfaces and Symbols committee: Working on a VMUIF.

b. ISO/IEC JTC 1/SC18/WG9: Working on a VMUIF. (This effort moves the ANSI work of X3V1.9 to ISO status.)

3.3.5.8.6 Recommendations. There are no standards to recommend.

3.3.6 Character-based user interface. Character-based user interface can be either a command-line interface or a menu-driven interface similar to a graphical user interface, but it does not use graphics and may depend solely on the keyboard for user input, i.e., not make use of an explicit pointing device. Modern systems and applications are and will be based upon graphical user interfaces and the associated standards for such systems. However, many legacy systems still include a large number of character-based terminals. The following sections discuss standards which can be applied to such systems. No recommendations will be made as to the use of these standards on legacy systems, since such recommendations may be inappropriately or uneconomically applied to such systems.

3.3.6.1 Style guide. A style guide, which is part of the Presentation Management layer in the NIST User Interface Reference Model, determines the "look" of an interface. Many style guides for GUIs have application to character-based interfaces.

3.3.6.1.1 Standards. Table 3.3-34 presents style guides.

TABLE 3.3-34 Style guide standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
IPC	NATO	Principles of Presentation of Information in Aircrew Stations	STANAG 3705	Informational (Approved)
GPC	DOD	User/Computer Interface	MIL-STD-1801 29 May 1987	Informational (Approved)
GPC	DOD	Human Engineering Performance Requirements for Systems	MIL-STD-1800A 10 Oct. 1990	Informational (Approved)
GPC	DOD	DOD Handbook, Human Engineering Guidelines for Management Information Systems	MIL-HDBK-761A 30 Sep. 1989	Informational (Approved)
GPC	DOD	Guidelines for Designing User Interface Software	ESD-TR-86-278	Informational (Approved)
GPC	DOD	Department of Defense Intelligence Information Systems Style Guide	DODIIS Style Guide, 10/91	Informational (Approved)
GPC	DOD	Air Force Intelligence Data Handling System (IDHS) Style Guide	IDHS Style Guide 1990	Informational (Approved)
GPC	DOD	Human Factors Guidelines for the Army Tactical Command and Control System (ATCCS) Soldier-Machine Interface	ATCCS Guidelines v.1.0 and v.2.0, 1990 and 1992	Informational (Approved)
GPC	DOD	The User Interface Specifications for Navy Command and Control Systems	Navy CCS, Version 1.1, 1992	Informational (Approved)
GPC	DOD	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	MIL-STD-1472D Notice 2, 30 June 1992	Informational (Approved)
GPC	DOD	Human Engineering Guidelines for Management Information Systems	DOD-HDBK-71A (DOD 1989c)	Informational (Approved)
GPC	DOD	Human Engineering Requirements for Military Systems, Equipment, and Facilities	MIL-STD-46855B 26 May 1994	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 10: Dialogue principles	9241-10:1996	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 11: Guidance on usability specifications and measures	9241-11	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 12: Presentation of information	9241-12	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 13: User guidance	9241-13	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 14: Menu dialogs	9241-14	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 15: Command language dialogs	9241-15	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Officer Work with VDTs Part 16: Direct manipulation dialogs	9241-16	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 17: Form-filling dialogs	9241-17	Informational (Draft)
IPC	ISO/IEC	Graphical Symbols Used on Screens: Interactive Icons	11581	Informational (Draft (CD))
NPC	IEEE	Recommended Practice for Graphical User Interface Drivability	P1201.2	Informational (Draft (Project being canceled, lack of progress))
GPC	DOD	Joint Satellite Control (JSC) Human Computer Interface Standard, Version 1.0	JSC HCI Std., 1.0	Informational (Draft)

3.3.6.1.2 Alternative specifications. Several applicable consort or de facto style guides are available for software user interfaces. These style guides promote consistency in user interface design across applications. However, conformance with one or more of the style guides listed below does not guarantee conformance with ergonomic standards (e.g., ISO 9241). These style guides include the following:

a. Defense Intelligence Agency (DIA) Standard User Interface Style Guide for Compartmented Mode Workstations.

b. DDS-2600-6215-91: Compartmented Mode Workstation Labeling: Source Code and User Interface Guidelines.

d. The Windows Interface: An Application Design Guide (Microsoft).

e. Object-Oriented Interface Design: IBM common user Access Guidelines (IBM).

f. Macintosh Human Interface Guidelines (Apple Computer).

g. SAA Presentation Manager Style Guide/Common User Access (CUA) (IBM).

h. Air Force Standard Systems Center GUI Style Guide, SSCR 700-010, Vol. I.

i. User Interface Specifications for the Global command and Control System (GCCS), version 1.0, draft, October 1994.

j. Theater Battle Management Style Guide (U.S. Navy).

k. Army Theater Battle Management HCI Specification.

l. Navy JMCIS.

3.3.6.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.3.6.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.3.6.1.5 Related standards. The following standards are related to user interface style guides:

a. DOD Human-Computer Interface (HCI)Style Guide, TAFIM Volume 8, Version 2.0, 30 September 1994. The Human-Computer Interface (HCI) Style Guide provides a common framework for HCI design and implementation with emphasis on standard look and feel for GUI based applications.

b. OSF Motif Style Guide, Motif SG Rev. 1.2:1992.

c. ISO 9241-1:1992, Ergonomic requirements for office content and usage of the multipart ISO 9241 standard. A revised version of ISO 9241-1 is currently at the CD level and will soon be released for DIS ballot. (Parts 1 and 2 of the ISO 9241 standard are informative; parts 10 and 11 are expected to be informative on completion. Parts 12-17 are expected to be normative on completion. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product.)

d. ISO 9241-2:1992, Ergonomic requirements for office work with VDTs, part 2: Task Requirements, presents an overview of factors that should be considered when designing tasks to be performed in a specific computing environment.

e. ISO CD 10075-2, Ergonomic principles related to mental work load -- Part 2: Design Principles, gives guidance on the design of work systems in general, with the intention of providing optimal working conditions with respect to health and safety, well-being, performance, and effectiveness.

f. MIL-STD-1908 (1992), Definition of Human Factors Terms.

g. NIST FIPS 158-1, User Interface Component of the Applications Portability Profile.

h. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

i. MIL-HDBK-759B(2)(1993) Human Factors Engineering Design for Army Materiel. (Draft 759C is complete.)

j. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

k. DOD-HDBK-743A (1991) Anthropometry of U.S. Military Personnel.

l. ITU-T E.134 Human Factors Aspects of Public Terminals: Generic Opening Procedures.

m. An ISO work item for a standard on "Human-Centered design" has been approved, but no working draft has yet been released for comment.

3.3.6.1.6 Recommendations. No recommendation is made for legacy systems which are based upon a character-based interface. Modifications of software running on such systems should be consistent with the existing look and feel of the system. New systems should be based on equipment which supports GUI applications.

3.3.6.2 Character-based terminal support. These specifications provide the ability to mimic a GUI interface on a character-based terminal.

3.3.6.2.1 Standards. Table 3.3-35 presents standards for character-based terminal support.

TABLE 3.3-35 Character-based terminal support standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	DIA	AlphaWindows	AlphaWindows	Informational (Approved)

3.3.6.2.2 Alternative specifications. The following specifications are also available to support legacy systems:

a. USL's SVID, which provides screen/menu enhancements to Curses, which will be compatible with Open Look.

b. Some proprietary implementations of Motif and MS Windows on character-based terminals.

3.3.6.2.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.3.6.2.4 Portability caveats. This is a high portability risk area because no standards exist.

3.3.6.2.5 Related standards. Some virtual APIs can provide character terminal support.

3.3.6.2.6 Recommendations. No recommendation is made for legacy system which are based upon a character-based interface.

AlphaWindows specifies a standard developed by the Display Industry Association for displaying applications software on low-cost terminals which do not support graphics.

3.3.6.3 Electronic forms. (This BSA appears in part 3, User Interface, part 4, Data Management, and part 5, Data Interchange.) These standards specify the functional interface requirements, transfer of various fields and the interface between programming languages and form filling applications for use on a terminal display.

3.3.6.3.1 Standards. Table 3.3-36 presents standards for electronic forms.

TABLE 3.3-36 Electronic forms standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	DOD Standardized Electronic Forms Requirements	JIEO-E-2300	Adopted (Approved)
IPC	ISO/IEC	Forms Interface Management System (FIMS)	11730:1994	Informational (Approved)
GPC	NIST	Government Open System Interconnection Profile (GOSIP 2): Virtual Terminal Forms Class Profile	FIPS PUB 146-1:1991	Informational (Approved)
CPC	X/Open	Single UNIX Specification (Spec. 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C436 (9/94)	Emerging (Approved)
CPC	X/Open	Single Unix Specification: X/Open Curses, Issue 4 (part of XPG4)	C437 (2/95)	Emerging (Approved)
GPC	DOD	DOD Forms Management Program Procedures Manual	DOD 7750.7-M	Informational (Approved)
CPN-C	Numerous vendors	Query by Forms	Query by Forms	Informational (Approved)
IPC	ISO/IEC	OSI Virtual Terminal Basic Class Service, Amendment 2: Additional Functional Units (forms capability)	9040:1990 DAM 2	Informational (Draft)
IPC	ISO/IEC	OSI Virtual Terminal (VT) Basic Class Protocol, Part 1, Amendment 2: Additional Functional Units (Forms Capability)	9041-1:1990 DAM 2	Informational (Draft)
CPC	X/Open	Internationalized Terminal Interfaces (XCURSES), Issue 4	S422 (4/94)	Informational (Superseded)

3.3.6.3.2 Alternative specifications. The Berkeley Software Distribution (BSD) 4.2/4.3 UUNIX Curses are also available.

3.3.6.3.3 Standards deficiencies. The X/Open Portability Guide 4 (XPG4) Curses is based on the System V Interface Definition (SVID) Issue 2 Curses version, which does not include the SVID's forms and menu libraries.

Forms Class Virtual Terminal has bindings in C only.

DOD has developed a specification for electronic forms (JIEO-E-2300). It defines the minimum operational requirements for electronic forms software and mandates an interchange file format based on Forms Interface Management System (FIMS).

3.3.6.3.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.3.6.3.5 Related standards. The Forms Class Virtual Terminal requires the Synchronous mode (S-mode) of operation and specifies simple delivery control. The following standards are related to forms query and management:

a. ISO 9075: SQL
b. ANSI X3.135-1992: SQL2
c. NIST FIPS 127-2: SQL
d. NIST FIPS 193: SQL Environments

3.3.6.3.6 Recommendations. The recommended standard is JIEO-E-2300. For User Interface, FIMS should be considered. For Data Management, make sure the forms management systems are compatible with FIPS 127-2 SQL. Database forms management systems should be integrated with the SQL database language and formats set forth in FIPS PUB 127-2.

3.3.7 Audio user interface. An audio user interface allows voice commands as input or voice or digital sound output.

3.3.7.1 Voice recognition. Voice recognition is the conversion of spoken words into computer text. Speech is digitized first then matched against a dictionary of coded wave forms. The matches are converted into text as if the words were typed on the keyboard. Speaker-dependent systems must be trained before using by taking samples of actual words from the person who will use it. Speaker-independent systems can recognize limited vocabularies such as numeric digits and a handful of words.

3.3.7.1.1 Standards. Table 3.3-37 presents standards for voice recognition.

TABLE 3.3-37 Voice recognition standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.3.7.1.2 Alternative specifications. The only other available specifications are proprietary.

3.3.7.1.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.3.7.1.4 Portability caveats. This is a high portability risk area because no standards exist.

3.3.7.1.5 Related standards. The following standards are related to voice recognition or voice recognition standards:

a. ANSI X3V1.9 User-System Interfaces and Symbols committee: Working on a VMUIF.

b. ISO/IEC JTC 1/SC18/WG9: Working on a VMUIF. (This effort moves the ANSI work of X3V1.9 to ISO status.)

3.3.7.1.6 Recommendations. There are no standards to recommend.

3.3.7.2 Speech synthesis. Speech synthesis is the generation of machine voice by arranging phonemes (e.g., k, ch, and sh) into words. Speech synthesis performs real time conversion without a predefined vocabulary but does not create human-sounding speech.

3.3.7.2.1 Standards. Table 3.3-38 presents standards for speech synthesis.

TABLE 3.3-38 Speech synthesis standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.3.7.2.2 Alternative specifications. The only other available specifications are proprietary.

3.3.7.2.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.3.7.2.4 Portability caveats. This is a high portability risk area because no standards exist.

3.3.7.2.5 Related standards. The following standards are related to speech synthesis or speech synthesis standards:

a. X3V1.9 User-System Interfaces and Symbols committee: Working on a VMUIF.

b. ISO/IEC JTC 1/SC18/WG9: Working on a VMUIF. (This effort moves the ANSI work of X3V1.9 to ISO status.)

3.3.7.2.6 Recommendations. There are no standards to recommend.

3.3.7.3 Voice messaging. Voice messaging is the use of voice mail as an alternative to electronic mail, in which voice messages are recorded intentionally, not because the recipient was not available. Voice mail is a computerized telephone answering system that digitizes incoming voice messages and stores them on disks. It usually provides auto attendant capability, which uses prerecorded messages to route the caller to the appropriate person, department, or mail box.

3.3.7.3.1 Standards. Table 3.3-39 presents standards for voice messaging.

TABLE 3.3-39 Voice messaging standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	User Interface to Telephone-Based Services - Voice Messaging Applications	13714:1995	Informational (Approved)
IPC	ISO/IEC	Voice Messaging User Interface Forum (VMUIF) (related to ANSI X3V1.9)	JTC1/SC18/WG9	Informational (Formative)

3.3.7.3.2 Alternative specifications. The only other available specifications are proprietary.

3.3.7.3.3 Standards deficiencies. Deficiencies in the standards are unknown.

3.3.7.3.4 Portability caveats. Portability problems related to the existing specification are unknown.

3.3.7.3.5 Related standards. No standards are related to voice messaging standards.

3.3.7.3.6 Recommendations. There are no recommendations.

3.3.8 Security. Security concerns for user interface services concentrate on identifying and authenticating the access control restrictions placed on system users, as well as the labeling of data by which those access control decisions can be made.

3.3.8.1 User interface security labeling. (This BSA appears in part 3 and part 10.) User interface security labeling provides a human readable representation of the internal security labels associated with data management, data interchange, graphics, data communications, system, and distributed computing services.

3.3.8.1.1 Standards. Table 3.3-40 presents standards for user interface security labeling.

TABLE 3.3-40 User interface security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Adopted (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	Defense Intelligence Agency Standard User Interface Style Guide for Compartmented Mode Workstations	DIA Style Guide: 1983	Informational (Approved)

3.3.8.1.2 Alternative specifications. There are no alternative specifications.

3.3.8.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.3.8.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.3.8.1.5 Related standards. DOD 5200.28-STD is a related standard. DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

Security-related interface requirements for workstations operating in System High or Compartmented Mode are discussed in DDS-2600-6243-91 and the DIA Style Guide, which provide the basis for the security portion of the HCI Style Guide (TAFIM Volume 8).

3.3.8.1.6 Recommendations. Appendix A of the TAFIM, Volume 8, DOD HCI Style Guide, outlines security presentation guidelines for workstations and is recommended.

3.3.8.2 Personal authentication. (This BSA appears in part 2, part 3, part 9, and part 10.) Personal authentication supports the accountability objective of being able to trace all security relevant events to individual users. In addition to supporting unique identification, standards are provided to authenticate the claimed identity.

3.3.8.2.1 Standards. Table 3.3-41 presents standards for personal authentication.

TABLE 3.3-41 Personal authentication standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
GPC	NIST	Password Usage	FIPS PUB 112: 1985	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
GPC	NIST	Guidelines on Evaluation of Techniques for Automated Personal Identification	FIPS PUB 48:1977	Informational (Approved)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - The Directory: Authentication Framework edition 2 (Same as ITU-T X.509:1993)	9594-8.2:1993	Informational (Approved)
GPC	NIST	Guideline for Use of Advanced Authentication Technology Alternatives	FIPS PUB 190:1994	Informational (Approved)
CPC	IETF	A One-Time Password System	RFC 1938: 1996	Emerging (Draft)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
CPC	IETF	The Kerberos Network Authentication Service (V5)	RFC 1510:1993	Informational (Draft)

3.3.8.2.2 Alternative specifications. There are no alternative specifications.

3.3.8.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.3.8.2.4 Portability caveats. OSF DCE Version 1.1's authentication service is based on Kerberos Version 5 (RFC 1510), but is not totally compatible with RFC 1510. DCE 1.2.2 adds testing and official support for Kerberos Version 5.

3.3.8.2.5 Related standards. The following standards are related to personal authentication standards (particularly TCSEC):

a. DOD 5200.28-STD, DOD Trusted Computer Systems Evaluation Criteria

b. NCSC-TG-017, Version 1, "A Guide to Understanding Identification and Authentication in Trusted Systems

c. CSC-STD-002-85, "Password Management Guideline"

d. NCSC-WA-002-85, "Personal Computer Security Considerations"

e. ITU-T X.509 (1993) (same as ISO 9594-8), The Directory: Authentication Framework

3.3.8.2.6 Recommendations. The mandated standards are recommended.

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 4 of 14 parts)

DATA MANAGEMENT SERVICES

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

TABLE OF CONTENTS

LIST OF TABLES

3.4 Data management services. Data management service standards provide (1) data dictionary/directory services for accessing and modifying data about data (i.e., metadata), (2) the database management services for accessing and modifying structured data, and (3) the distributed data service for accessing and modifying data from a remote database.

NOTE: Throughout Part 4, all tables shall have abbreviations listed under the column (Standard Type) as follows:

a. National Public Consensus = NPC
b. International Public Consensus = IPC
c. Government Public Consensus = GPC
d. Consortia Public Consensus = CPC
e. Consortia Private Non-Consensus = CPN-C
f. National Public Non-Consensus = NPN-C

3.4.1 Data management system. These standards provide the basic database services needed by an application using a database. A Database Management System (DBMS) is an application used to create, store, retrieve, change, manipulate, sort, format, and print the information in a database.

3.4.1.1 Basic database services. Basic database services include data definition, manipulation, query, and integrity, embedded Structured Query Language (SQL), and dynamic facilities. Data definition includes create, alter, and delete tables, views, records, fields, classes, objects, instances, attributes, and data. Data manipulation includes insert, select, update, and delete tables, views, records, fields, classes, objects, instances, attributes, and data. Data query includes the ability to specify search conditions consisting of a combination of select lists, predicates, and comparison operators. Data integrity includes data locking (to some degree of granularity), consistency, transaction control (to specify commit and rollback commands and guarantee the ability to serialize database transactions), referential constraints (to help ensure data consistency), and synchronous writing of data. Embedded SQL consists of SQL statements embedded in a high-level language source program. In a separate compiling phase, the SQL may be optimized and converted into special function calls. Dynamic SQL is SQL interpreted by the SQL database at runtime. Dynamic SQL may be generated by programs or entered interactively by the user. Facilities embedded in application programs generate executable SQL statements during program execution so control of a database can be turned over temporarily to the end user for interactive access and manipulation of data.

3.4.1.1.1 Standards. Table 3.4-1 presents standards for basic database services.

TABLE 3.4-1 Basic database services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Database Language SQL (Adopts ANSI X3.135-1992 (same as ISO 9075:1992))	FIPS PUB 127-2:1993	Mandated (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	SQL Environments	FIPS PUB 193:1995	Informational (Approved)
GPC	NIST	Guidelines for Functional Specifications for Database Management Systems	FIPS PUB 124:1986	Informational (Approved)
CPC	X/Open	Embedded SQL (Cobol and C)	SQL Developers Specification	Informational (Approved)
IPC	ISO	Database Language - Network (NDL)	8907:1987	Informational (Approved)
GPC	NIST	Database Language - NDL (adopts ANSI X3.133-1986)	FIPS PUB 126:1987	Informational (Approved)
NPC	ANSI	Database Language - (NDL)	X3.133-1986	Informational (Approved)
CPC	X/Open	Data Management: Reference Model	G505 (10/95)	Informational (Approved)
IPC	ISO/IEC	Database Language SQL3 (will replace SQL2)	9075	Emerging (Draft)
GPC	NIST	SQL3-Based FIPS	FIPS PUB 127-3	Emerging (Formative)
NPC	ANSI	Database Language SQL3 (will replace SQL2)	X3H2 Project 0525-R	Informational (Draft)
CPC	X/Open	Structured Query Language (SQL)	C201 (9/92)	Informational (Superseded)

3.4.1.1.2 Alternative specifications. The following alternative specifications are available:

a. For data definition, manipulation, query, data integrity, embedded SQL, and dynamic facilities standards: Integrated Database Application Programming Interface (IDAPI), a specification, published by Borland, IBM, Novell, and Word Perfect Corporation, will allow DOS, OS/2, and Windows applications to access a variety of SQL and non-SQL databases transparently.

b. No applicable consortia or de facto SQL integrity constraint specifications are available.

c. For X/Open SQL and the IBM Systems Application Architecture (SAA) SQL support Embedded C.

d. For dynamic facilities the only other available specifications are proprietary.

3.4.1.1.3 Standards deficiencies. The following deficiencies in the standards have been identified:

a. or data definition, manipulation, query, data integrity, embedded SQL, and dynamic facilities standards:

(1) No standardized way exists to specify logical database access control, which is important to database security.

(2) Hashing methods to access data are neither standardized nor in progress.

(3) SQL1 is inadequate and has failed to be transportable or standardized to be very useful. The upcoming SQL-3 provides an opportunity for DOD requirements to be incorporated.

b. For data integrity standards, SQL Integrity Enhancement is a simple capability with no constructs to help programmers maintain data consistency.

c. For Embedded SQL standards, SQL2 supports Embedded SQL in C and Ada. However, products will not be available for some time. International Organization for Standardization (ISO)/American National Standards Institute (ANSI) Embedded SQL does not support the C programming language. The use of embedded SQL requires a precompiler for each language in which SQL is embedded.

d. For dynamic facilities standards, deficiencies in the existing formal standards are unknown.

e. For SQL environments, the emphasis in this first FIPS for SQL Environments is on profiles for limited SQL interfaces to non-SQL data repositories. Subsequent versions of this FIPS may specify more complete profiles for other products in an SQL environment. The profiles defined by this standard are not complete in and of themselves. The user is required to add information before this standard can be successfully used in a procurement.

3.4.1.1.4 Portability caveats. The following portability caveats apply:

a. For data definition, manipulation, query, data integrity, embedded SQL, and dynamic facilities standards,

(1) SQL 2's segmentation into multiple levels increases the likelihood of incompatibility between different vendors' SQLs, because different vendors will implement entry level SQL 2, then choose options from other levels.

(2) The ISO, ANSI, and Federal Information Processing Standard (FIPS) versions of SQL specify state exception code values (called SQLCODE parameters) such as 0 for successful execution, 100 for nonexistent data, and implementation defined code values for particular exception conditions. Different products that conform with SQL have different SQLCODE values for exception conditions. The set of SQL character

values for the character data type and collating sequence of characters is defined by the implementor, and therefore, nonstandard in products.

b. For data integrity the following portability caveats apply:

(1) Most vendors' products contain extensions. To maximize portability, reduce the use of extensions as much as possible.

(2) Different vendors provide locking to different degrees of granularity. Portability and/or interoperability of applications result in locking to the largest degree of granularity.

c. For dynamic facilities the following portability caveat applies: Although the X/Open and SAA SQLs support dynamic SQL, X/Open SQL is an X/Open-enhanced specification of the 1986 version of Level 1 SQL, while SAA SQL is not fully ISO/ANSI SQL compatible, although it will be. Also, X/Open and SAA dynamic SQL facilities are not fully compatible with each other.

d. For SQL environments, conformance testing for products claiming conformance to one of the profiles specified by FIPS 193 will be achieved by a suitable modification of the existing NIST SQL test suite. This FIPS requires the customer to choose from among the different binding styles already defined by the SQL standards. Two of these styles (CLI and RDA) are expected to be more popular than the others. If a programming language binding style is chosen, then FIPS SQL specifies the parameter passing requirements for each of seven different programming languages.

3.4.1.1.5 Related standards. The following standards are related to basic database services or basic database service standards:

(1) ISO 9579-1: Remote Database Access (RDA) (Generic Model, Service and Protocol)(supports remote database access in client-server environments)

(2) ISO 9579-2: RDA: (SQL Specialization)

(3) SQL Access Group's (SAG's) SQL Access Formats and Protocols (FAP) (1991)

(4) SAG's Call Level Interface (CLI)

(5) X/Open RDA Preliminary Specification (Identical to the SAG's RDA Specification

(6) X/Open's CLI Snapshot Specification (Identical to the SAG's CLI Specification)

(7) Open Systems Interconnection (OSI) CCR (Commitment, Concurrency, and Recovery): ISO/International Electrotechnical Commission (IEC) 9804-3/9805-3

(8) OSI Distributed Transaction Processing (DTP) Protocol: ISO/IEC 10026 Parts 1, 2, and 3.

(9) ISO 1989:1985: COBOL

(10) ANSI X3.9-1978: FORTRAN-77

(11) ANSI X3.159-1989: C

(12) National Institute for Standards and Technology (NIST) FIPS 021-3: COBOL

(13) NIST FIPS 069-1: FORTRAN

(14) NIST FIPS 119, DOD MIL-STD 1815A:1983, ISO 8652: Ada

(15) NIST FIPS 160: C

(16) ISO/IEC Draft International Standard (DIS) 10032: Reference Model of Data Management

(17) ISO 12227 SQL/Ada Models Description Language, 1994

(18) X3 SQLIB-1 SQL Information Bulletin Number 1 Interpretation of ANSI X.3.135 - 1989

3.4.1.1.6 Recommendations. The following are related to data definition, manipulation, query, data integrity, embedded SQL, and dynamic facilities standards:

(1) Consult the wording suggested in the October 1991 General Services Agency (GSA) publication for proposed language for requiring that a database conform to SQL, and consult FIPS 127-2 for guidance on how to structure a Request for Proposal (RFP). The FIPS "flagger" (to flag nonconforming extensions) is optional and must be specified explicitly.

(2) If interactive SQL is required, a procurement must indicate explicitly whether or not "direct invocation of SQL statements" is required and, if required, which SQL statements are to be directly invocable. If not specified, the default is "CREATE TABLE," "CREATE VIEW," "GRANT privilege," "SELECT" with "ORDER BY" option, "INSERT," "UPDATE:searched," "DELETE:searched," "COMMIT WORK," and "ROLLBACK WORK."

(3) Explicitly specify sizing constraints for database constructs. The FIPS 127-2 sizing specifications are reasonable to expect vendors to deliver, but are fairly minimal. Since database construct sizing specifications depend on the procurement, a procurement can override them.

(4) Require the use of NIST conformance tests and/or services to validate conformance to the SQL-based FIPS for required and optional FIPS 127-2 features. Testing applies only to a specific platform, so call for conformance tests for each platform bid. Use the quarterly list of processors validated against FIPS 127-2 by NIST to help evaluate bids.

(5) Specify the NIST's Transition Level SQL 2 and the SAG's CLI and RDA interfaces and protocols for the following reasons. Most DBMS vendors have no intention of conforming to the Full Level SQL 2:1992 because it is very large and complex. As a result, the time it will take to add the necessary features will probably exceed the time before the SQL 3 standard is completed. To ensure portability as well as functionality, users are encouraged to include the following two specifications in their procurement:

(a) NIST's Transition Level SQL 2 (specified in FIPS 127-2), which is a hybrid of Entry Level and higher levels of SQL 2:1992.

(b) SAG's and X/Open's CLI and RDA standards. The SAG specifications are not segmented like SQL '92 and offer a nice balance between the Full Level SQL '92 feature set and what users need now. The SAG specifications include connection management capabilities (which are part of the SQL '93 Full Level), schema manipulation and the CHARACTER VARYING data type (both of which are part of SQL '93 Intermediate Level), and features not included in any level of SQL '92 conformance, including the CREATE INDEX and DROP INDEX statements. SAG's specifications are published jointly with X/Open as X/Open specifications.

(6) Specify SQL2 (and later SQL3) as soon as possible because SQL2/3 contains greater standardized functionality than SQL1. This will reduce the use of nonstandard extensions. SQL2 also standardizes more than 60 SQLCODE exception code values.

(7) Carefully specify and check all sizing constraints for a procurement to meet functionality requirements and avoid portability problems.

(8) Avoid the Network Data Language (NDL), if possible, because it is little used and will not be upgraded.

(9) Specify the ISO RDA standard, and also the X/Open or SAG's RDA and CLI specifications in conjunction with SQL/SQL2 to obtain remote data access capabilities in a distributed environment.

The Integrity Constraint feature is optional in SQL and must be specified explicitly for a procurement. Failure to do so means the Integrity Constraint feature is not required. Specify FIPS 127-2, especially if any of the services unique to FIPS 127-2 are needed.

In SQL2, the integrity enhancement feature is mandatory, not optional. Also, SQL2 has better integrity constraints, such as "cascade delete on referential integrity" (in the intermediate SQL Level) and "deferrable integrity constraints" (in full SQL2).

For embedded SQL:

(1) Specify embedded SQL in an RFP, although it is optional in the standard. Indicate which programming language is to be supported in references to embedded SQL in a procurement. Failure to do so means that support for any one FIPS language satisfies the FIPS SQL requirement. Indicate whether the language interface is to support the Module Language interface style, the embedded language interface style, or both. Failure to do so means that vendors supporting any one interface style satisfy the FIPS SQL requirement.

(2) Require the use of NIST conformance tests and/or services to validate conformance to every one of the embedded interfaces and module interfaces, and to validate the compilers that will be used with the embedded SQL because SQL testing is independent of the host programming language testing. Testing applies only to a specific platform, so call for conformance tests for each platform bid. Specify FIPS 127-2 if any of the services unique to FIPS 127-2 are needed. Specify that the character data values and collating sequences coincide with the character values and collating sequence of the specific programming languages to be used. Failure to indicate specific character set requirements means that support for representation of the 95-character graphic subset of American Standard Code for Information Interchange (ASCII) (FIPS 1-2) in an implementor specified collating sequence defaults to the minimum requirement, and may not be portable across other procured systems.

For dynamic facilities, SQL2 is preferred. Dynamic SQL is an intermediate level SQL2 capability. Either SQL2's dynamic SQL facilities or the SQL2 intermediate level must be specified explicitly in a procurement.

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

3.4.1.2 Indexed sequential access. The Indexed Sequential Access Method (ISAM) is a procedure for storing and retrieving data from a disk file. When the programmer designs the file format, a set of indices is created describing where the records of the file are located on the disk. This provides a quick method of retrieving the data and eliminates the need to read all data from the beginning to find the desired information. The indexes can be stored as part of the data file or in a separate index file. The sequential order will be the one most commonly used for batch processing and printing (e.g., account number, name).

3.4.1.2.1 Standards. Table 3.4-2 presents standards for indexed sequential access.

TABLE 3.4-2 Indexed sequential access standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Data Management, Issue 3	C215 (3/92)	Adopted (Approved)
CPC	X/Open	Indexed Sequential Access Method (ISAM): Developers' Specification	D010 (8/90)	Adopted (Approved)

3.4.1.2.2 Alternative specifications. Another specification option is Informix Software Inc.'s C-ISAM, on which X/Open's ISAM is based.

3.4.1.2.3 Standards deficiencies. The greatest deficiency in ISAM standards is the lack of any formal ISAM specifications or functionality.

3.4.1.2.4 Portability caveats. Consider the use of ISAM carefully as risks are involved in using an informal standard.

3.4.1.2.5 Related standards. The following standards are related to ISAM or ISAM standards:

a. ISO 9075: SQL
b. ISO 9579-1: RDA (Generic Model, Service and Protocol
c. ISO 9579-2: RDA (SQL Specialization)
d. ANSI X3.135-1992: SQL
e. NIST FIPS 127-2: SQL
f. NIST FIPS 193: SQL Environments

3.4.1.2.6 Recommendations. When specifying ISAM services, all ISAM systems offered as a result of a procurement's requirements should be integrated with the SQL database language set forth in FIPS PUB 127-2, and should implement all of the features specified elsewhere in this document. All ISAM systems offered as a result of a procurement's requirements should be integrated with ISO 9579-1: RDA (Generic Model, Service and Protocol). If SQL is used, it also should be integrated with ISO 9579-2: RDA (SQL Specialization). Carefully weigh the portability risks in specifying ISAM, because only consortia ISAM standards exist.

3.4.1.3 Electronic forms. (This BSA appears in part 3, User Interface, part 4, Data Management, and part 5, Data Interchange.) These standards specify the functional interface requirements, transfer of various fields and the interface between programming languages and form filling applications for use on a terminal display.

3.4.1.3.1 Standards. Table 3.4-3 presents standards for electronic forms.

TABLE 3.4-3 Electronic forms standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	DOD Standardized Electronic Forms Requirements	JIEO-E-2300	Adopted (Approved)
IPC	ISO/IEC	Forms Interface Management System (FIMS)	11730:1994	Informational (Approved)
GPC	NIST	Government Open System Interconnection Profile (GOSIP 2): Virtual Terminal Forms Class Profile	FIPS PUB 146-1:1991	Informational (Approved)
CPC	X/Open	Single UNIX Specification (Spec. 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C436 (9/94)	Emerging (Approved)
CPC	X/Open	Single Unix Specification: X/Open Curses, Issue 4 (part of XPG4)	C437 (2/95)	Emerging (Approved)
GPC	DOD	DOD Forms Management Program Procedures Manual	DOD 7750.7-M	Informational (Approved)
CPN-C	Numerous vendors	Query by Forms	Query by Forms	Informational (Approved)
IPC	ISO/IEC	OSI Virtual Terminal Basic Class Service, Amendment 2: Additional Functional Units (forms capability)	9040:1990 DAM 2	Informational (Draft)
IPC	ISO/IEC	OSI Virtual Terminal (VT) Basic Class Protocol, Part 1, Amendment 2: Additional Functional Units (Forms Capability)	9041-1:1990 DAM 2	Informational (Draft)
CPC	X/Open	Internationalized Terminal Interfaces (XCURSES), Issue 4	S422 (4/94)	Informational (Superseded)

3.4.1.3.2 Alternative specifications. The Berkeley Software Distribution (BSD) 4.2/4.3 UUNIX Curses are also available.

3.4.1.3.3 Standards deficiencies. The X/Open Portability Guide 4 (XPG4) Curses is based on the System V Interface Definition (SVID) Issue 2 Curses version, which does not include the SVID's forms and menu libraries.

Forms Class Virtual Terminal has bindings in C only.

DOD has developed a specification for electronic forms (Joint Interoperability and Engineering Organization (JIEO)-E-2300). It defines the minimum operational requirements for electronic forms software and mandates an interchange file format based on Forms Interface Management System (FIMS).

3.4.1.3.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.4.1.3.5 Related standards. The Forms Class Virtual Terminal requires the Synchronous mode (S-mode) of operation and specifies simple delivery control. The following standards are related to forms query and management:

a. ISO 9075: SQL
b. ANSI X3.135-1992: SQL2
c. NIST FIPS 127-2: SQL
d. NIST FIPS 193: SQL Environments

3.4.1.3.6 Recommendations. The recommended standard is JIEO-E-2300. For User Interface, FIMS should be considered. For Data Management, make sure the forms management systems are compatible with FIPS 127-2 SQL. Database forms management systems should be integrated with the SQL database language and formats set forth in FIPS PUB 127-2.

3.4.1.4 Report writer. A report writer is an application that prints a report based on a description of the layout. As a stand-alone program or part of a DBMS, it retrieves selected records from a file and may sort them into a new sequence before printing. Once created, it is stored in a report file for future use.

Nonprocedural forms management includes forms creation, modification, and management, including screen painting. Procedural forms management includes forms creation, modification, and management, using procedural methods. A nonprocedural report writer includes nonprocedural formatted database report definition, modification, and management. A procedural report writer includes formatted database report definition, modification, and management using procedural techniques.

3.4.1.4.1 Standards. Table 3.4-4 presents report writer standards.

TABLE 3.4-4 Report writer standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.4.1.4.2 Alternative specifications. The only available specifications are proprietary, such as IBM's SAA RPG: Common Programming Interface: Database Reference (SC09-1286-01).

3.4.1.4.3 Standards deficiencies. The lack of procedural or nonprocedural capabilities for database report writing is the deficiency in open standards for report writers.

3.4.1.4.4 Portability caveats. This is a high portability risk area because no standards exist.

3.4.1.4.5 Related standards. The following standards are related to report writers or report writer standards:

a. ISO 9075: 1992 - Database Languages - SQL, Third Edition
b. ANSI X3.135-1992: SQL
c. NIST FIPS 127-2: SQL
d. NIST FIPS 193: SQL Environments
e. (see also Fourth Generation Language under Software Engineering Services)

3.4.1.4.6 Recommendations. All database report writing systems should be integrated with the SQL database language set forth in FIPS PUB 127-2 and the SQL Environments of FIPS 193. The lack of procedural or nonprocedural capabilities for database report writing is a deficiency in open database standards.

3.4.1.5 Database administration. (This BSA appears in part 4 and part 9.) Data administration is the process of the analysis, classification, and maintenance of an organization's data and data relationships. It includes the development of data models, data warehousing, and data dictionaries, which combined with transaction processing, are the raw materials for database design.

3.4.1.5.1 Standards. Table 3.4-5 presents standards for database administration.

TABLE 3.4-5 Database administration standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Data Element Standardization Procedures, January 1993	Manual 8320.1-M-1	Mandated (Approved)
GPC	NIST	Guide to Data Entity Naming Conventions	NBS SP 500-149 of Oct. 1987	Informational (Approved)
GPC	DOD	Defense Data Repository System	End User Manual ver. 2.0 of 10 August 1993	Informational (Approved)
IPC	ISO/IEC	Specification and Standardization of Data Elements, Part 3: Basic Attributes of Data Elements	11179-3:1994	Informational (Approved)
IPC	ISO/IEC	Specification and Standardization of Data Elements, Part 4: Rules and Guidelines for the Formulation of Data Definitions	11179-4:1995	Informational (Approved)
IPC	ISO/IEC	Specification and Standardization of Data Elements, Part 5: Naming and Identification Principles for Data Elements	11179-5:1995	Informational (Approved)
IPC	ISO/IEC	Specification and Standardization of Data Elements, Part 6: Registration of Data Elements	11179-6	Informational (Draft)
GPC	DOD	DOD Data Administration	DODD 8320.1 of 9/26/1991	Informational (Superseded)

3.4.1.5.2 Alternative specifications. The only other available specifications are proprietary database utilities.

3.4.1.5.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.4.1.5.4 Portability caveats. This is a high portability risk area because no standards exist.

3.4.1.5.5 Related standards. The following standards are related to database administration or database administration standards:

a. ISO 7498-4:1989: Management Framework
b. ISO 9075: SQL
c. ISO 9579-1: RDA (Generic Model, Service and Protocols)
d. ISO 9579-2: RDA (SQL Specialization)
e. ISO 9595:1991: CMIS.
f. ISO 9596-1:1991: CMIP.
g. ISO/IEC 9945-1: (IEEE P1003.1)

h. ISO 10164-1:1993: Object Management Function
i. ISO 10165-1:1991: SMI - Part 1 Management Information Model
j. ISO 10165-2:1991: SSMI - Part 2 DMI
k. ISO 10165-4:1992: Guidelines for the Definition of Managed Objects (GDMO)
l. ANSI X3.135-1992: SQL
m. ANSI X3.168-1989: Embedded SQL
n. NIST FIPS 127-2: Database Language SQL
o. NIST FIPS 146-1: Government Open Systems Interconnection Profile (GOSIP)
p. NIST FIPS 156: IIRDS
q. NIST FIPS 193: SQL Environments

3.4.1.5.6 Recommendations. DODD 8320.1 is recommended for data administration. Database administration systems should be compatible with and integrated with the SQL database language set forth in FIPS PUB 127-2. Furthermore, all database administration systems offered as a result of this procurement's requirements shall be integrated with ISO 9579-1 RDA (Generic Model, Service and Protocol), ISO 9579-2 Remote Database Access (SQL Specialization) of December 1993, and NIST FIPS PUB 193, SQL Environments.

3.4.1.6 Menu-driven database access. These standards provide access to a database through a menu-driven or form-filling interface.

3.4.1.6.1 Standards. Table 3.4-6 presents standards for menu-driven database access.

TABLE 3.4-6 Menu-driven database access standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	DOD Standardized Electronic Forms Requirements	JIEO-E-2300	Informational (Approved)
IPC	ISO/IEC	Forms Interface Management System (FIMS)	11730:1994	Informational (Approved)

3.4.1.6.2 Alternative specifications. The only other available specifications are proprietary.

3.4.1.6.3 Standards deficiencies. The FIMS is not specific to database management systems. Instead, it is a generic programming language for building generic forms. No menu-driven database access standard either exists or is emerging.

3.4.1.6.4 Portability caveats. When completed, FIMS will apply to many types of applications, and is related only generically to database forms and menus. Consequently, programs built using FIMS have a high probability of not being compatible with a particular database, or with interconnected databases.

3.4.1.6.5 Related standards. The only standard related to menu-driven database access or menu-driven database access standards is Open Software Foundation (OSF): Motif.

3.4.1.6.6 Recommendations. JIEO-E-2300 is recommended.

3.4.1.7 Data storage and archiving. Data storage and archiving services provide a database application with the facilities for temporary storage and long-term data archiving. Archiving files is a process in which the information contained in an active computer file is made ready for storing in a nonactive file, perhaps in off-line or near-line storage. Typically when files are archived, they are compressed to reduce their size. To restore the file to its original size requires a process known as unarchiving.

3.4.1.7.1 Standards. Table 3.4-7 presents standards for data storage and archiving.

TABLE 3.4-7 Data storage and archiving standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.4.1.7.2 Alternative specifications. The only available specifications are proprietary specifications and database utilities.

3.4.1.7.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.4.1.7.4 Tailoring guidance. No tailoring guidance is available because no standards exist.

3.4.1.7.5 Related standards. The following standards are related to data storage and archiving or data storage and archiving standards:

a. ISO 9595:1991: CMIS
b. ISO 9596:1991: CMIP
c. Forthcoming UNIX International specification for backup and archive

3.4.1.7.6 Recommendations. There are no standards to recommend.

3.4.1.8 Multidatabase Application Program Interfaces. Multidatabase Application Program Interface (APIs) specify the interaction among several heterogeneous databases.

3.4.1.8.1 Standards. Table 3.4-8 presents standards for multidatabase application program interfaces.

TABLE 3.4-8 Multidatabase Application Program Interfaces standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPN-C	Microsoft	Open Database Connectivity (ODBC) 2.0	ODBC	Mandated (Approved)
CPN-C	Microsoft	Open Database Connectivity(ODBC) 3.0	ODBC	Emerging (Draft)
CPN-C	Sun	Java Database Connectivity(JDBC)	JDBC	Informational (Formative)

3.4.1.8.2 Alternative specifications. The only other available specifications are proprietary database utilities.

3.4.1.8.3 Standards deficiencies. Deficiencies in the standards are unknown.

3.4.1.8.4 Portability caveats. Portability caveats in the standards are unknown.

3.4.1.8.5 Related standards. All standards for a single database are related to multidatabase API standards.

3.4.1.8.6 Recommendations. ODBC is recommended for this Base Service Area.

3.4.1.9 Models/Process/Workflow. Information standards in this BSA address activity models, data models and workflow. The information requirements identified in the activity model is used as the basis for developing a fully attributed data model. The data model identifies the logical information requirements and metadata, which forms a basis for physical database schema and data elements. Workflow defines the functionality required to support interoperabilty between workflow products.

3.4.1.9.1 Standards. Table 3.4-9 presents standards for models/process/workflow.

TABLE 3.4-9 Models/Process/Workflow standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Integration Definition for Information Modeling (IDEF1X)	FIPS PUB 184	Mandated (Approved)
GPC	NIST	Integration Definition for Function Modeling (IDEF0)	FIPS PUB 183	Mandated (Approved)
CPC	WFMC	Interoperability Abstract Specification	WFMC-TC-1012:1996	Informational (Approved)
NPC	IEEE	Conceptual Schema Modeling for Object Oriented	IDEF1X97	Informational (Draft)
CPC	WFMC	Interface 5 Audit Specification	TC1015	Informational (Draft)
CPC	WFMC	Application Program Interface	WFMC-TC-1009	Informational (Draft)

3.4.1.9.2 Alternative specification. The only other available specifications are proprietary.

3.4.1.9.3 Standard deficiencies. Deficiencies in the standards are unknown.

3.4.1.9.4 Portability caveats. Portability problems with the standards are unknown.

3.4.1.9.5 Related standards. No related standards are known at this time.

3.4.1.9.6 Recommendations. The mandated specifications are recommended.

3.4.2 Data management security. Security for data management services encompasses access control mechanisms for data that is either stored or manipulated in a database management system. In addition to access control, labeling and integrity concerns must be addressed. Programs and data can be secured by issuing identification numbers and passwords to authorized users of a computer. Passwords can be checked in the DBMS software, where each user can be assigned an individual view (subschema) of the database. Although precautions can be taken to detect an unauthorized user, determining whether a valid user is performing unauthorized tasks is extremely difficult.

3.4.2.1 Database security. (This BSA appears in part 4, part 9, and part 10.) Database security standards provide protection for stored data from unauthorized access, modification, and denial of service.

3.4.2.1.1 Standards. Table 3.4-10 presents standards for database security.

TABLE 3.4-10 Database security standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Database Language SQL (Adopts ANSI X3.135-1992 (same as ISO 9075:1992))	FIPS PUB 127-2:1993	Informational (Approved)
GPC	NIST	Information Resource Dictionary System (IRDS) (adopts ANSI X3.138-1988 and X3.138A-1991)	FIPS PUB 156:1989	Informational (Approved)
NPC	ANSI	Database Language SQL	X3.135-1992	Informational (Approved)
IPC	ISO	Database Language SQL (same as ANSI X3.135-1992)	9075:1992	Informational (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Framework	10027:1990	Informational (Approved)
IPC	ISO/IEC	OSI Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element	9804:1990	Informational (Approved)
IPC	ISO/IEC	OSI Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Service Element	9805:1990	Informational (Approved)
NPC	ANSI	Information Resource Dictionary System (IRDS)	X3.138-1988	Informational (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Services Interface Amendment 1: C Language Binding	10728 AMD 1:1994	Informational (Draft)

3.4.2.1.2 Alternate specifications. No alternate specifications are known. There are no alternative specifications.

3.4.2.1.3 Standards deficiencies. Deficiencies in the existing standard are unknown.

3.4.2.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.4.2.1.5 Related standards. DOD 5200.28-STD, 26 December 1995, DOD Trusted Computer Systems Evaluation Criteria, is related to NCSC-TG-021. The following specifications are related to DOD 5200.28-STD:

a. NCSC-TG-018, Version 1, July 1992, A Guide to Understanding Object Reuse in Trusted Systems

b. NCSC-TG-025, Version 2, September 1991, A Guide to Understanding Data Remnants in Automated Information Systems

3.4.2.1.6 Recommendations. The mandated standard is recommended.

3.4.2.2 System access control. (This BSA appears in part 4, part 9, part 10, and part 11.) System access control standards provide high-level guidance on access control frameworks and implementation.

3.4.2.2.1 Standards. Table 3.4-11 presents standards for system access control.

TABLE 3.4-11 System access control standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 9: Objects and Attributes for Access Control	10164-9:1995	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 3: Access Control	10181-3	Informational (Draft)

3.4.2.2.2 Alternate specifications. No alternate specifications are known.
There are no alternative specifications.

3.4.2.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.4.2.2.4 Portability caveats. Portability problems with the existing standards are unknown.

3.4.2.2.5 Related standards. The following guidelines support the TCSEC standard:

a. NCSC-TG-003, Version 1, September 1987, A Guide to Understanding Discretionary Access Control in Trusted Systems

b. NCSC-TG-028, Version 1, May 1992, Assessing Controlled Access Protection

c. NCSC-TG-020-A, August 1989, Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX System

3.4.2.2.6 Recommendations. The mandated standards are recommended.

3.4.2.3 Data management security labeling. (This BSA appears in part 4 and part 10.) Data management security labeling provides a security service for ensuring that data includes labeling information in support of mandatory access control security services, marking security services, handling security services, aggregation security services, sanitization security services, and release security services. Security labeling services produce and maintain the integrity of the security label and its binding to the data with which it is associated.

3.4.2.3.1 Standards. Table 3.4-12 presents standards for data management security labeling.

TABLE 3.4-12 Data management security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Informational (Approved)

3.4.2.3.2 Alternate specifications. There are no alternative standards.

3.4.2.3.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.4.2.3.4 Portability caveats. Portability problems with the existing standards are unknown.

3.4.2.3.5 Related standards. Data management security labeling should be compatible with MIL-STD-2045-48501, Common Security Label, for any system with a communications interface.

DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

3.4.2.3.6 Recommendations. The mandated standard is recommended. Data management security labeling should be based of the operating system security label standards. Data management security labeling should employ binding of strength equal to or greater than that of the operating system. Compatible security labeling standards include the ability to perform a one-for-one mapping or translation between security labeling standards.

3.4.2.4 Systems integrity. (This BSA appears in part 4 and part 10.) Systems integrity objectives ensure the integrity of information and resources by providing a level of protection in response to the threats of unauthorized modification, manipulation, and destruction which is commensurate with the importance and priority of the content. These standards provide the high-level framework with which to view the security service of integrity in open systems.

3.4.2.4.1 Standards. Table 3.4-13 presents standards for system integrity.

TABLE 3.4-13 Systems integrity standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 6: Integrity (same as ITU-TS X.815)	10181-6	Informational (Draft)
IPC	ITU-T	Security Frameworks in Open Systems: Integrity Framework (same as ISO 10181-6)	X.815: 1993	Informational (Draft)

3.4.2.4.2 Alternate specifications. No alternate specifications are known.
There are no alternative specifications.

3.4.2.4.3 Standards deficiencies. Deficiencies in the existing standard are unknown.

3.4.2.4.4 Portability caveats. Portability problems with the existing standards are unknown.

3.4.2.4.5 Related standards. The following NSA documents supplement the information on integrity found in the TCSEC:

a. C Technical Report 79-91, September 1991, "Integrity in Automated Information Systems:

b. C Technical Report 111-91, October 1991, "Integrity-Oriented Control Objectives: Proposed Revisions to the Trusted Computer System Evaluation (TCSEC), DOD 5200.28-STD."

3.4.2.4.6 Recommendations. The mandated standards are recommended.

3.4.2.5 Data integrity techniques. (This BSA appears in part 4 and part 10.) Data integrity techniques provide services that allow data integrity between communicating applications to be confirmed by means of a cryptographic check function using a block cipher algorithm, by electronic signature, electronic hashing, and encryption.

3.4.2.5.1 Standards. Table 3.4-14 presents standards for data integrity techniques.

TABLE 3.4-14 Data integrity techniques standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180-1:1995	Mandated (Approved)
GPC	NIST	Digital Signature Standard (DSS)	FIPS PUB 186:1994	Mandated (Approved)
IPC	ISO	Data Cryptographic Techniques - Data Integrity Mechanism Using a Cryptographic Check Function Employing a Block Cipher Algorithm	9797:1989	Informational (Approved)
CPC	IETF	IP Authentication Header (AH)	RFC 1826: 1995	Emerging (Draft)
CPC	IETF	IP Encapsulating Security Payload (ESP)	RFC 1827: 1995	Emerging (Draft)
CPC	IETF	Domain Name System (DNS) Security Extensions	RFC 2065:1997	Emerging (Draft)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180:1993	Informational (Superseded)

3.4.2.5.2 Alternate specifications. Alternative de facto specifications include RSA and MD-5.

3.4.2.5.3 Standards deficiencies. Deficiencies in the existing specifications are unknown.

3.4.2.5.4 Portability caveats. Portability problems with the existing specifications are unknown.

3.4.2.5.5 Related standards. There are no related standards.

3.4.2.5.6 Recommendations. The mandated standards are recommended.

FIPS PUB 180-1, which supersedes FIPS PUB 180, specifies a Secure Hash Algorithm (SHA-1) which can be used to generate a message digest. The SHA-1 is required for use with the Digital Signature Algorithm (DSA) as specified in FIPS PUB 186 and whenever an SHA is required in federal applications.

3.4.3 Data dictionary/directory services. Data dictionary/directory services are key computer software tools that manage data and information resources. Such services provide extensive facilities for recording, storing, and processing descriptions of an organization's significant data and data processing resources, and often provide facilities to use metadata (information about data).

3.4.3.1 Data dictionary. (This BSA appears in part 4 and part 9.) A data dictionary is a part of a database management system that transparently provides a centralized meaning, relationship to other data, origin, usage, and format. It also indicates which application programs use that data, so that when a change in a data structure is contemplated, a list of affected programs can be generated. The data dictionary a stand-alone system or may be an integral part of the DBMS and used to control it. Data integrity and accuracy is better ensured in the latter case.

3.4.3.1.1 Standards. Table 3.4-15 presents data dictionary standards.

TABLE 3.4-15 Data dictionary standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Information Resource Dictionary System (IRDS) (adopts ANSI X3.138-1988 and X3.138A-1991)	FIPS PUB 156:1989	Adopted (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Framework	10027:1990	Informational (Approved)
GPC	NIST	Guide for the Development, Implementation, and Maintenance of Standards for the Representation of Computer Processed Data Elements	FIPS PUB 45:1976	Informational (Approved)
GPC	NIST	Guidelines for Planning and Using a Data Dictionary System	FIPS PUB 76:1980	Informational (Approved)
NPC	ANSI	Information Resource Dictionary System (IRDS)	X3.138-1988	Informational (Approved)
NPC	ANSI	Information Resource Dictionary System (IRDS) Services Interface	X3.185-1992	Informational (Approved)
NPC	ANSI	Information Resource Dictionary System (IRDS) Export/Import File Format	X3.195-1991	Informational (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Services Interface	10728:1993	Informational (Approved)
CPC	Metadata Coalition	Metadata Interchange Specification (MDIS)	MDIS 1.0:1996	Informational (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Services Interface Amendment 1: C Language Binding	10728 AM1 1:1994	Informational (Draft)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Export/Import Support for SQL:1989 with Integrity Enhancement	JTC1/SC21/WG03 Nxxx	Informational (Formative)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Design Support for SQL Applications	JTC1/SC21/WG03 Nxxx	Informational (Draft)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Services Interface Amendment 2: Ada bindings (binding for Ada-83)	10728 WDAM 2:1993(E)	Informational (Draft)

3.4.3.1.2 Alternative specifications. No applicable consortia or de facto specifications for the data dictionary are available.

3.4.3.1.3 Standards deficiencies. The following deficiencies have been identified in the available standards:

a. APIs with the IRDS are not currently defined.

b. There are no IRDS bindings to Ada.

c. IRDS does not support the development of active functionality.

d. IRDS does not support object-oriented data structures. An upcoming major IRDS revision is expected to add support for object-oriented data structures and communications between data management tools. Computer Aided Software Engineering (CASE) tool proponents are lobbying for this revision.

e. IRDS does not support information communications among data management tools.

f. IRDS conformance tests do not exist, although they are being developed.

g. While DOD 8320.1-M-1 Data Element Standardization Procedures, January 1993, provides procedures for the approval and maintenance of data elements. The standard governing the design, definition, and naming rules for data elements comes from Integration Definition for Information Modeling (IDEF1X), Corporate Information Management Process Improvement Methodology for DOD Functional Managers (1992). This has been adopted as FIPS 184.

h. There are no implementations.

3.4.3.1.4 Portability caveats. The ANSI and ISO services interface standards have diverged and are not compatible. All attempts to converge these standards have failed because the ANSI and ISO IRDS specifiers have different data dictionary interests. As a result, the ISO model is geared toward developing an underlying interface between the dictionary and the DBMS. U.S. Federal agencies, the NIST, and ANSI focus on user interfaces.

One example of how ANSI and ISO IRDS diverge is concerned with whether or not relationships are permitted to have attributes. ISO says no, on the grounds that its simpler model, without attributes, is more easily integrated with SQL tables. ANSI says yes, claiming that even though a model permitting attributes is more complex and difficult to use, it provides greater flexibility for more IRDS users. People using IRDS for system planning processes, for example, might need to store certain items in the dictionary that would not necessarily be applicable for interfacing with DBMSs.

3.4.3.1.5 Related standards. The following standards are related to data dictionaries or data dictionary standards:

a. International Telecommunications Union - Telecommunications Standards Sector (ITU-T) (formerly International Telegraph and Telephone Consultative Committee (CCITT))/ISO X.500: Directory Services

b. Standard Textual Language (STL): IEEE 1175 (particularly for use with CASE tools)

c. Many CASE tools, because the IRDS acts as a focus for sharing data and metadata and can be applied to them.

d. NIST FIPS 183: IDEF0

e. NIST FIPS 184: IDEF1X

f. Data element standards in the data dictionary BSA, above.

3.4.3.1.6 Recommendations. IRDS, FIPS 156, is recommended. Most computer vendors claim that they are committed to IRDS, but few have it now. If specific IRDS documents are not specified explicitly in a procurement, vendors most likely will propose products that are not compatible with IRDS.

If a procurement is targeted at a traditional database environment and a simpler-to-use IRDS is desirable, consider the ISO specification. If other environments are at stake and attributes on relationships, or many-to-many relationships are needed to represent the relationships between hardware and programs, as well as between programs and data, then choose FIPS 156 IRDS and use ANSI IRDS wherever FIPS 156 has not specified certain capabilities. Whether the choice is for ISO, ANSI, or FIPS IRDS, be prepared to lock yourself in for other procurement, rather than mixing ISO and ANSI IRDS because of the incompatibilities.

3.4.3.2 Distributed directory services. (This BSA appears in part 4, part 9, and part 11.) A directory or naming service provides a standardized naming scheme, a standardized interface with the naming facilities, and the ability for the interface to provide transparent access to a variety of naming schemes and mechanisms (e.g., DCE).

Directory service applications convert a name into a physical address on a network, providing logical to physical conversion. Names can be user names, computers, printers, servers, or files. This enables users to find these resources without knowing their locations. The transmitting station sends a name to the server containing the naming service software, which sends back the actual address of the user or resource.

3.4.3.2.1 Standard. Table 3.4-16 presents standards for distributed directory services.

TABLE 3.4-16 Distributed directory services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Directory (Global and Cell) Service	DCE 1.1 Directory:1994	Mandated (Approved)
IPC	ISO	Open Systems Interconnection-Session Service Definition	8326:1987	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Connection-Oriented Session Protocol	8327:1987	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Basic Connection Oriented Presentation Service Definition	8822:1988	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Connection-Oriented Presentation Protocol	8823:1988	Informational (Approved)
IPC	ITU-T	The Directory: Models (X-ref: ISO 9594-2)	X.501 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Authentication Framework (X-ref: ISO 9594-8)	X.509, Version 3: 1993	Informational (Approved)
IPC	ITU-T	The Directory: Abstract Service Definition (X-ref: ISO 9594-3)	X.511 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Procedures for Distributed Operation (X-ref: ISO 9594-4)	X.518: 1993	Informational (Approved)
IPC	ITU-T	The Directory: Protocol Specification (X-ref: ISO 9594-5)	X.519 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Selected Attributes Types (X-ref: ISO 9594-6)	X.520 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Selected Object Classes (X-ref: ISO 9594-7)	X.521 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Replication (X-ref: ISO 9594-9)	X.525 (1993)	Informational (Approved)
CPC	X/Open	Federated Naming: The XFN Specification	C403 (7/95)	Informational (Approved)
NPC	IEEE	Directory services/Name space API	1224.2:1993	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Domain Name Service Profile (References IAB STD 13 (RFC 1034, 1035))	MIL-STD-2045-17505:1994	Informational (Approved)

3.4.3.2.2 Alternative specification. There are no alternative specifications available.

3.4.3.2.3 Standard deficiencies. Deficiencies in the existing specifications are unknown.

3.4.3.2.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.4.3.2.5 Related standards. There are no related standards.

3.4.3.2.6 Recommendations. OSF DCE directory services are recommended for DCE applications. For more information on non-DCE directory services, see the Host Application Support BSA in part 7, Communication Services.

3.4.3.3 Universal syntax. With the creation of a DOD Data Element Dictionary, an opportunity exists to create a universal syntax for the exchange of those data elements. This syntax will address the entire set of DOD information exchange requirements without regard to its current form. It would meld such diverse formatting approaches as the Tactical Digital Information Link (TADIL), United States Message Text Format (USMTF), and Electronic Document Interchange (EDI).

3.4.3.3.1 Standards. Table 3.4-17 presents universal syntax standards.

TABLE 3.4-17 Universal syntax standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.4.3.3.2 Alternative specifications. No other consortia or de facto specifications are available.

3.4.3.3.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.4.3.3.4 Portability caveats. This is a high portability risk area because no standards exist.

3.4.3.3.5 Related standards. No standards are related to universal syntax standards.

3.4.3.3.6 Recommendations. There are no standards to recommend.

3.4.3.4 Data repository. A repository provides a place and method to store metadata. It generally is broader and supports more kinds of data than a data dictionary.

3.4.3.4.1 Standards. Table 3.4-18 presents data repository standards.

TABLE 3.4-18 Data repository standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC/IPC	ANSI/ISO	Information Resources Dictionary System 2 (IRDS2) (Repository standard revision will include an interface with CASE tools)	JTC1/21.06.04,5; ANSI X3H4 Project 0754-D (or DT?)	Informational (Formative)
CPC	Various	Various groups of contractors working in cooperation with the US Navy and Air Force	ProSLCSE, STARS	Informational (Formative)

3.4.3.4.2 Alternative specifications. The only other available specifications are proprietary.

3.4.3.4.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.4.3.4.4 Portability caveats. The following portability problems have been identified:

a. There is a substantial overlap, and possible conflict, between the Portable Common Tool Environment (PCTE) and the ISO 10728 (IRDS) for data dictionary interfaces.

b. There is a high portability risk associated with repositories because no standards exist.

3.4.3.4.5 Related standards. The following standards are related to data repositories or data repository standards:

a. ISO 10027:1990: IRDS Framework. Current IRDS standards are covered only in the data dictionary sections because they are limited in their ability to handle metadata. However, IRDS work is underway to change the IRDS standards into a full fledged repository that can handle a variety of types of metadata.

b. ANSI X3.138 1988: IRDS Command Language and Panel Interface

c. ANSI X3.195-1991: IRDS Export/Import File Format

d. ANSI X3.185-1992: IRDS Services Interface

e. NIST FIPS 156: IRDS Base Document: Requirements, and Command Language and Panel Interface

f. ISO Draft Proposed (DP) 8800-1: IRDS Command Language and Panel Interface

g. ISO DIS 10728-X: IRDS Services Interface Module for C Language Binding

h. All the SQL standards (e.g., ISO 9075:1992 SQL; ANSI X3.135-1989 SQL; ANSI X3.168-1989: Embedded SQL; FIPS 127-2; FIPS 193)

i. Emerging standards for PCTE

j. Object Management Group's (OMG) Common Object Request Broker Architecture (CORBA) specification

3.4.3.4.6 Recommendations. There are no standards to recommend.

3.4.4 Distributed data. These services support applications that use a partitioned database acting like a single coherent database.

3.4.4.1 Remote data access. (This BSA appears in part 4 and part 11.) RDA specifications are extensions of a data access (RDA) language to allow remote access to a database in a client-server environment. RDA refers to the interfaces, protocols, and formats needed to allow remote database access in a client-server environment, where the databases may be heterogeneous and from multiple vendors.

3.4.4.1.1 Standards. Table 3.4-19 presents standards for remote data access.

TABLE 3.4-19 Remote data access standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	OSI Remote Database Access (RDA), Part 1: Generic Model, Service and Protocol	9579-1:1993	Adopted (Approved)
IPC	ISO/IEC	OSI Remote Database Access, Part 2: SQL Specialization	9579-2:1993	Adopted (Approved)
CPC	X/Open	Data Management: SQL Remote Database Access	C307 (8/93)	Informational (Approved)
CPC	X/Open	Data Management: SQL Call Level Interface (CLI)	C451 (4/95) (Supersedes P303)	Informational (Approved)
CPC	SAG	Database Language SQL, Access Formats & Protocols (FAP) Specification:1991 (Based on SQL)	SQL Access FAP Specs:1991	Informational (Approved)
CPC	SAG	Database Language SQL Call Level Interface (CLI)	SQL-89	Informational (Approved)

3.4.4.1.2 Alternative specifications. The only other available specifications are proprietary.

3.4.4.1.3 Standards deficiencies. RDA specifies the service and protocol between only a single client and server. This is one reason that caused the formation of the SAG to put more distributed functionality into RDA. RDA does not consider multiple connections and, therefore, does not specify distributed database access. APIs and Ada bindings to the RDA standards are not defined.

RDA is aligned closely with the SQL-2 Entry Level. However, the integrity enhancement is optional. Also, RDA is not aligned currently with the FIPS 127-2 Transition Level, which the NIST considers very important for SQL use.

The ISO RDA and CLI are only a subset of the SAG's RDA and CLI.

3.4.4.1.4 Portability caveats. RDA's use of ISO Remote Operations Service Elements (ROSE) hinders precision, adds needlessly to the text and Abstract Syntax Notation (ASN).1, and incorporates assumptions that limit the usefulness of RDA. Furthermore, an implementation conforming to ISO 9545 (the OSI standard that refines the basic OSI Reference Model to provide

a framework for coordinating the development of existing and future application layer standards) could not use ROSE, since they both claim to be application service elements.

RDA's optional integrity enhancement and the lack of alignment with the FIPS 127-2 Transition Level can result in differences among systems compliant with RDA that impede portability and interoperability.

3.4.4.1.5 Related standards. The following standards are related to remote data access or remote data access standards:

a. ISO 9072: ROSE
b. ISO 9075:1992: SQL Third Edition (same as NIST FIPS PUB 127-2:1993)
c. ISO 10026-1..3: Distributed Transaction Processing Model, Service, & Protocol
d. ANSI X3.135-1989: SQL
e. ANSI X3.168-1989: Embedded SQL
f. X/Open C193: Distributed TP: The XA Specification

3.4.4.1.6 Recommendations. The first choice for a standard would be RDA, ISO 9579, and RDA: SQL Specialization, ISO 9579-2, unless the additional functionalities provided by the SAG are needed.

Where RDA lacks desired capabilities for a procurement, consider SQL Access Formats and Protocols Specifications or the X/Open RDA. The SAG and X/Open are tracking the RDA standard and both support RDA extensions that are being adopted by the emerging RDA standard. Consider the X/Open specified ASN.1 replacement module that eliminates the use of ROSE.

3.4.4.2 Database recovery. (This BSA appears in both part 4 and part 9.) Database recovery refers to the ability to detect a failure in a system, recover from failure, and permit a slave copy to become a master copy, assuring data integrity and consistency.

3.4.4.2.1 Standards. Table 3.4-20 presents standards for database recovery.

TABLE 3.4-20 Database recovery standards

Standard Type	Sponsor	Standard	Standard Reference	Status (Lifecycle)
IPC	ISO/IEC	OSI Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element	9804 1990	Informational (Approved)
IPC	ISO/IEC	OSI Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Service Element	9805:1990	Informational (Approved)

3.4.4.2.2 Alternative specifications. No other consortia or de facto specifications are available.

3.4.4.2.3 Standards deficiencies. Deficiencies in database recovery standards are unknown.

3.4.4.2.4 Portability caveats. At present, CCR is not widely implemented, although most vendors intend to implement it. Therefore, one should make no assumptions about the degree of portability and interoperability existing for any database recovery utilities.

3.4.4.2.5 Related standards. The following standards are related to database recovery or database recovery standards:

a. ISO/IEC 10026 Parts 1, 2, and 3: Distributed Transaction Processing (DTP) protocol

b. X/Open XA Interface specification, which includes CCR's two-phase commitment

3.4.4.2.6 Recommendations. If CCR is desired (and it is necessary for multivendor, distributed database and distributed transaction processing), it must be referenced specifically in procurement specifications. Otherwise, vendors probably will propose products that do not meet this specification.

For the greatest portability, design applications as if CCR were not present.

3.4.4.3 Distributed database. Distributed database services allow partitioning (including physical partitioning) and, possibly, partial replication of a database so that the partitioned database, which is distributed at different sites, still behaves like a single, coherent database. If redundant data are stored in separate databases to meet performance requirements, updates to one set of data will update the additional sets automatically in a timely and controlled manner. A Client-Server Data Management Model for Distributed Processing, such as the Distributed Computing Environment (DCE), also is required.

3.4.4.3.1 Standards. Table 3.4-21 presents standards for distributed databases.

TABLE 3.4-21 Distributed database standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	OSI Remote Database Access (RDA): Some distributed database capabilities in future RDA revisions	9579 (future)	Informational (Formative)
NPC/IPC	ANSI/ISO	Information Resources Dictionary System 2 (IRDS2) (Repository standard revision will include an interface with CASE tools)	JTC1/21.06.04,5; ANSI X3H4 Project 0754-D (or DT?)	Informational (Formative)

3.4.4.3.2 Alternative specifications. The only other available specifications are proprietary.

3.4.4.3.3 Standards deficiencies. No standards exist to ensure data integrity across data residing at multiple locations. The term distributed databases does not have a standard definition. Databases ranging from traditional databases that are accessed from distributed locations to databases that support distributed query and distributed query and update, are called distributed databases.

3.4.4.3.4 Portability caveats. Vendors' SQLs are not exactly the same. Distributing such not-quite-the-same databases can cause portability problems. If the meaning and identity of the data administered at different sites and on different systems are different, users will lose portability. Worse, they will receive wrong answers to their queries and will not be able to recognize that the answers are wrong.

3.4.4.3.5 Related standards. The following standards are related to distributed databases or distributed database standards:

a. ISO 9075:1992: SQL Third Edition (same as NIST FIPS PUB 127-2:1993)

b. ISO 9804/9805: CCR

c. ISO 10026-1,2,3: Distributed Transaction Processing Model, Service, and Protocol

d. X/Open C193 (1992): Distributed TP: The XA Specification

3.4.4.3.6 Recommendations. There are no standards to recommend. Distributed database products must support ISO 9804/9805 CCR (for the two-phase commit specification).

3.4.5 Object database. An object-oriented database is one that holds abstract data types (objects). It can store objects directly from an object-oriented programming language. Because any type of data can be stored (the rules for processing the data are part of an object), the object database promises fully integrated databases that will hold data, text, pictures and voice, essentially an endless variety of ever-changing formats. It is capable of handling complex queries about objects that would be difficult in relational database programs.

3.4.5.1 Object-oriented database management. (This BSA appears in both Part 4 and Part 9.) Standards for object-oriented database management provide facilities and interfaces to manage object databases (databases that store, manipulate, and retrieve data represented as objects).

3.4.5.1.1 Standards. Table 3.4-22 presents standards for object-oriented database management.

TABLE 3.4-22 Object-oriented database management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	ODMG	Object Database Management Group (ODMG) - 93	ODMG-93, Release 1.1	Informational (Approved)
CPC	ODMG	Object Database Management Group (ODMG) 9x	ODMG-9x	Emerging (Formative)
NPC	ANSI	X3 Database System Study Group (DBSSG)	X3 Study	Informational (Formative)
CPC	OMG	Preliminary work on object-oriented database management	TBD-Preliminary work on object-oriented database management	Informational (Formative)

3.4.5.1.2 Alternative specifications. Microsoft's Object Database Connectivity (OBDC) API specification for MS-Windows applications is also available.

3.4.5.1.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard, but the Microsoft specification has insufficient drivers available.

3.4.5.1.4 Portability caveats. This is a high portability risk area because no standards exist, and many Microsoft PC products do not comply with most Unix- and Portable Operating System Interfaces for Computers (POSIX)-based systems.

3.4.5.1.5 Related standards. No standards are related to object-oriented database management standards.

3.4.5.1.6 Recommendations. There is no recommendation at this time.

3.4.6 Transaction processing. Orders, purchases, changes, additions, and deletions are examples of transactions recorded in a business information environment. Queries and other requests are also transactions to the computer, but usually are just acted upon and not recorded in the system. A transaction is a completed event that can be assembled in chronological sequence for an audit trail. Transaction processing systems, also called on-line or real time systems, update master files as soon as they are entered at terminals or arrive over communications lines. Contrast this with batch processing, which stores transactions and updates the necessary files at a later date.

3.4.6.1 Protocol for interoperability in heterogeneous transaction processing systems. These specifications support Transaction Processing (TP) systems containing components from diverse sources and between dissimilar transaction processing systems.

3.4.6.1.1 Standards. Table 3.4-23 presents standards for protocols for interoperability in heterogeneous transaction processing systems.

TABLE 3.4-23 Protocol for interoperability in heterogeneous transaction processing systems standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	OSI Distributed Transaction Processing (DTP) - Part 1: OSI TP Model	10026-1:1992	Adopted (Approved)
IPC	ISO/IEC	OSI Distributed Transaction Processing (DTP) - Part 2: OSI TP Service	10026-2:1996	Adopted (Approved)
IPC	ISO/IEC	OSI Distributed Transaction Processing (DTP) - Part 3: Protocol Specification	10026-3:1996	Adopted (Approved)
IPC	ISO/IEC	OSI Distributed Transaction Processing (DTP), Part 4: Protocol Implementation Conformance Statement (PICS) Proforma	10026-4:1995	Informational (Approved)
IPC	ISO/IEC	OSI Distributed Transaction Processing (DTP), Part 6: Unstructured Data Transfer	10026-6:1995	Informational (Approved)
IPC	ISO/IEC	OSI Distributed Transaction Processing (DTP), Part 5: Application Context Proforma and Guidelines When Using OSI TP	10026-5	Informational (Draft)
IPC	ISO/IEC	OSI Distributed Transaction Processing (DTP), Part 7: Message Queueing	10026-7	Informational (Draft)

3.4.6.1.2 Alternative specifications. No other consortia or de facto specifications are available.

3.4.6.1.3 Standards deficiencies. The following deficiencies have been identified in the available standards:

a. No standardized API to the ISO DTP protocol.
b. No Ada binding to the ISO 10026 services or protocol.
c. The ISO 10026 DTP model does not address the overall environment.

3.4.6.1.4 Portability caveats. Portability problems for the ISO TP protocol are unknown. The IEEE P1003.11 Group is disbanded. P1003.11 draft documents and current work are being transferred to the P1003.0 Group.

3.4.6.1.5 Related standards. The following standards are related to interoperability in heterogeneous TP systems:

a. ISO 9041-1: Basic Class Virtual Terminal Protocol Specification

b. ISO 9075:1992: SQL Third Edition (same as NIST FIPS PUB 127-2:1993)

c. ISO 9579-1: RDA (Generic Model, Service and Protocol)

d. ISO 9579-2: RDA (SQL Specialization)

e. ISO 9594 Parts 1-8: Directory Services

f. ISO 9804/9805: CCR

g. ISO DIS 10148: RPC

h. ISO Working Draft (WD) 10181-1: Security Frameworks in Open Systems: Part 1:Overview

i. ISO DIS 10181-2: Security Frameworks in Open Systems: Part 2: Authentication Framework

j. ISO DIS 10181-3: Security Frameworks in Open Systems: Part 3: Access Control Framework

k. ISO 11578: RPC

l. ITU-T Recommendation X.500: Directory Services

m. IEEE P1003.1b: Real-Time Extension to POSIX

n. IEEE P1003.1c: Threads Extension to POSIX

o. IEEE P1003.17: Directory Services API

p. European Computer Manufacturers' Association (ECMA) 127: RPC

q. ECMA Technical Report: Support Environment for Open Distributed Processing (SE-ODP)

r. OSF: DCE RPC

s. X/Open C193, S423: XA and XA+ Interfaces

3.4.6.1.6 Recommendations. ISO 10026, parts 1, 2, and 3, is recommended.

3.4.6.2 Transaction manager-to-resource manager interface. These standards specify the interface from the transaction manager to the resource manager. In some models, only transaction managers can communicate.

3.4.6.2.1 Standards. Table 3.4-24 presents standards for the transaction manager to resource manager interface.

TABLE 3.4-24 Transaction manager-to-resource manager interface standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Distributed TP: The XA Specification	C193 (2/92)	Adopted (Approved)
CPC	X/Open	Distributed TP: Reference Model, Version 2	G307 (11/93)	Informational (Approved)
CPC	X/Open	Distributed TP: Reference Model, Version 3	G504 (2/96)	Informational (Approved)

3.4.6.2.2 Alternative specifications. The following specifications are also available:

a. USL: Tuxedo
b. Transarc: Encina
c. NCR: Top End

3.4.6.2.3 Standards deficiencies. No Ada binding to the X/Open XA Specification exists. The XA interfaces do not address, or directly accept hash values for global transaction identifiers. (Hash value handling capabilities were addressed in the preliminary specification, but were dropped in the final specification.) The comparison of global IDs is indirect and convoluted, rather than explicit.

3.4.6.2.4 Portability caveats. In the X/Open distributed transaction processing model, the major and most accepted model to date, the transaction manager is bundled with the communications manager. Although this can enhance transaction communications efficiency, it also makes it more difficult to define a portable and interoperable interface with a multitude of communications systems, including legacy systems.

3.4.6.2.5 Related standards. The following standards are related to transaction manager-to-resource manager interface standards:

a. ISO 9041-1: Basic Class Virtual Terminal Protocol Specification

b. ISO 9075:1992: SQL Third Edition (same as NIST FIPS PUB 127-2:1993)

c. ISO 9579-1: RDA (Generic Model, Service and Protocol)

d. ISO 9579-2: RDA (SQL Specialization)

e. ISO 9594 Parts 1-8: Directory Services

f. ISO 9804/9805: CCR

g. ISO 10026: DTP Model, Services, and Protocol

h. ISO DIS 10148: RPC

i. ISO WD 10181-1: Security Frameworks in Open Systems: Part 1: Overview

j. ISO DIS 10181-2: Security Frameworks in Open Systems: Part 2: Authentication Framework

k. ISO DIS 10181-3: Security Frameworks in Open Systems: Part 3: Access Control Framework

l. ISO DP 11578: RPC

m. ITU-T Recommendation X.500: Directory Services

n. IEEE P1003.1b: Real-Time Extension to POSIX

o. IEEE P1003.1c: Threads Extension to POSIX

p. IEEE P1003.17: Directory Services API

q. ECMA 127: RPC

r. ECMA Technical Report: SE-ODP

s. OSF: DCE RPC

3.4.6.2.6 Recommendations. Open distributed TP systems must support X/Open XA interfaces, because no other specification exists for transaction manager-to-resource manager interfaces.

Unless the communications manager is decoupled from the transaction manager, be very careful about any distributed transaction processing systems that claim to provide portability with legacy communications systems.

3.4.6.3 Transaction manager-to-communications manager interface. These standards specify the interface from the transaction manager to the communications manager. In some specifications the communications manager was part of the transaction manager. These specifications cover the case in which the communications manager has been extracted and decoupled from the transaction manager.

3.4.6.3.1 Standards. Table 3.4-25 presents standards for the transaction manager to communications manager interface.

TABLE 3.4-25 Transaction manager-to-communications manager interface standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Distributed TP: The TxRPC Specification	C505 (11/95)	Adopted (Approved)
CPC	X/Open	Distributed TP: The XATMI Specification	C506 (11/95)	Adopted (Approved)
CPC	X/Open	Distributed TP: The XA+ Specification, Version 2 (Based on CPI-C, Version 2)	S423 (7/94)	Adopted (Approved)
CPC	X/Open	Distributed TP: TxRPC Specification (Based on X/Open DCE RPC paradigm)	P305 (7/93)	Informational (Superseded)
CPC	X/Open	Distributed TP: XATMI Specification (Based on Tuxedo ATMI Interface)	P306 (7/93)	Informational (Superseded)

3.4.6.3.2 Alternative specifications. The following specification is also available:

a. Transarc: Encina

3.4.6.3.3 Standards deficiencies. No Ada binding is being developed for the XA+ Interface.

3.4.6.3.4 Portability caveats. The XA+ Interface is highly controversial because although decoupling the communications manager from the transaction manager makes it easier to integrate different communications systems and paradigms, such decoupling can result in a loss of communications efficiency and performance. Consequently with good reason, various vendors may bundle the communications and transaction managers together with the resulting loss of portability because of the need to write different communications interfaces.

3.4.6.3.5 Related standards. The following standards are related to transaction manager-to-communications manager interface:

a. ISO 9041-1: Basic Class Virtual Terminal Protocol Specification

b. ISO 9594 Parts 1-8: Directory Services

c. ISO 9804/9805: CCR

d. ISO 10026: DTP Model, Services, and Protocol

e. ISO DIS 10148: RPC

f. ISO WD 10181-1: Security Frameworks in Open Systems: Part 1: Overview

g. ISO DIS 10181-2: Security Frameworks in Open Systems: Part 2: Authentication Framework

h. ISO DIS 10181-3: Security Frameworks in Open Systems: Part 3: Access Control Framework

i. ISO DP 11578: RPC

j. ITU-T Recommendation X.500: Directory Services

k. IEEE P1003.1b: Real-Time Extension to POSIX

l. IEEE P1003.1c: Threads Extension to POSIX

m. IEEE P1003.[illegible] ectory Services API

n. ECMA 12[illegible] RPC

o. OSF: DCE RPC

p. X/Open C193: XA Interface

3.4.6.3.6 Recommendations. If it is desirable to decouple the transaction manager from the communications manager, such decoupling, as well as the XA+ specification, must be specified explicitly in procurement specifications. Otherwise, vendors probably will propose products that do not meet this specification. X/Open S423, P306, and P305 are recommended.

For ease of integration with legacy communications and transaction processing systems, be sure the communications manager is decoupled from the transaction manager. If performance is an issue, at least for the near term, require the communications and transaction manager to be bundled together.

3.4.6.4 Application-to-communications resource manager interface. These specifications define the interface between the application and the communications manager, which is a type of resource manager.

3.4.6.4.1 Standards. Table 3.4-26 presents standards for application to communications resource manager interfaces.

TABLE 3.4-26 Application-to-communications resource manager interface standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPN-C	UI	CM Reference Specification	TP Standards Strategy White Paper, Rev. 4.0	Informational (Approved)
CPC	X/Open	CM Specification	Working Papers	Informational (Formative)

3.4.6.4.2 Alternative specifications. The following specifications are also available:

a. Transarc: Encina
b. NCR: Top End

3.4.6.4.3 Standards deficiencies. Neither an Ada nor a Cobol binding is being developed for the Communications Manager (CM) interface, although the architecture of the CM interface is easily adaptable to the Ada language.

3.4.6.4.4 Portability caveats. The CM Interface is controversial because it implies that the communications manager is decoupled from the transaction manager. This is controversial as explained further in the section on the XA+ interface. For example, AT&T/USL's Tuxedo bundles the transaction manager with the communications manager. Thus, Tuxedo is not likely to be compatible with the CM interface.
The number of vendors committed to implementing the CM interface probably will make it a de facto standard once it is adopted by X/Open. This may create portability problems with Tuxedo, which is currently the most widely used transaction manager.

3.4.6.4.5 Related standards. The following standards are related to application-to-communications resource manager interface:

a. ISO 9041-1: Basic Class Virtual Terminal Protocol Specification

b. ISO 9594 Parts 1-8: Directory Services

c. ISO 9804/9805: CCR

d. ISO 10026: DTP Model, Services, and Protocol

e. ISO DIS 10148: RPC

f. ISO WD 10181-1: Security Frameworks in Open Systems: Part 1: Overview

g. ISO DIS 10181-2: Security Frameworks in Open Systems: Part 2: Authentication Framework

h. ISO DIS 10181-3: Security Frameworks in Open Systems: Part 3: Access Control Framework

i. ISO DP 11578: RPC

j. ITU-T Recommendation X.500: Directory Services

k. IEEE P1003.1b: Real-Time Extension to POSIX

l. IEEE P1003.1c: Threads Extension to POSIX

m. IEEE P1003.17: Directory Services API

n. ECMA 127: RPC

o. OSF: DCE RPC

p. X/Open C193: XA Interface

q. X/Open S423: XA+ Specification

3.4.6.4.6 Recommendations. If it is desirable to decouple the transaction manager from the communications manager, such decoupling, as well as the emerging CM specification, must be specified explicitly in procurement specifications. Otherwise, vendors probably will propose products that do not meet this specification.

For ease of integration with legacy communications and transaction processing systems, be sure the communications manager is decoupled from the transaction manager. If performance is an issue at least for the near term, require the communications and transaction manager to be bundled together.

3.4.6.5 Communications manager-to-protocol stack interface. These specifications define the interface between the communications manager and the underlying protocol stacks. They allow a single communications manager to interface with multiple, independently provided protocol stack implementations, and multiple CMs to be integrated with a single protocol stack implementation.

3.4.6.5.1 Standards. Table 3.4-27 presents standards for the communications manager to protocol stack interface.

TABLE 3.4-27 Communications manager-to-protocol stack interface standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	ACSE/Presentation: Transaction Processing API (XAP-TP)	C409 (4/95)	Informational (Approved)
NPC	IEEE	XAP-TP Specification (Based on X/Open's XAP-TP Specification)	Number not yet assigned	Informational (Draft)

3.4.6.5.2 Alternative specifications. No other consortia or de facto specifications are available.

3.4.6.5.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.4.6.5.4 Portability caveats. This is a high portability risk area because no standards have been completed.

3.4.6.5.5 Related standards. The following standards are related to communications manager-to-protocol stack interface standards:

a. ISO 9041-1: Basic Class Virtual Terminal Protocol Specification

b. ISO 9594 Parts 1-8: Directory Services

c. ISO DIS 10148: RPC

d. ISO WD 10181-1: Security Frameworks in Open Systems: Part 1: Overview

e. ISO DIS 10181-2: Security Frameworks in Open Systems: Part 2: Authentication Framework

f. ISO DIS 10181-3: Security Frameworks in Open Systems: Part 3: Access Control Framework

g. ISO DP 11578: RPC

h. ITU-T Recommendation X.500: Directory Services

i. IEEE P1003.1b: Real-Time Extension to POSIX

j. IEEE P1003.1c: Threads Extension to POSIX

k. IEEE P1003.17: Directory Services API

l. ECMA 127: RPC

m. OSF: DCE RPC

4.6.5.6 Recommendations. The X/Open ACSE/Presentation - Transaction Processing API (XAP-TP) specification must be referenced specifically in procurement specifications, and a requirement to move to the XAP-TP specification as soon as it is adopted by X/Open also must be stated there specifically. Otherwise, vendors probably will propose products that do not meet this specification.

To maximize interoperability and portability, the emerging XAP-TP interface should be used when it is adopted by X/Open for the interface between the communications manager and the protocol stack(s) being used.

3.4.6.6 Transaction demarcation. These specifications define the interface between the transaction manager and the application, taking transaction demarcation information from the application and delimiting the transaction to the resource manager.

3.4.6.6.1 Standards. Table 3.4-29 presents standards for transaction demarcation.

TABLE 3.4-28 Transaction demarcation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Distributed TP: The TX (Transaction Demarcation) Specification	C504 (4/95)	Adopted (Approved)
CPC	X/Open	Distributed TP: The XA Specification	C193 (2/92)	Informational (Approved)
CPC	X/Open	Structured Transaction Definition Language (STDL)	P536 (12/95)	Informational (Approved)
CPC	MIA Consortia	Standardized Transaction Definition Language (STDL)	TBD-Standardized Transaction Definition Language (STDL)	Informational (Approved)
CPN-C	UI	ATMI (Application to Transaction Manager Interface) Specification	Trans. Monitor I/F Spec. Ver. 1.0:1991	Informational (Approved)
CPC	X/Open	Distributed TP: The TX (Transaction Demarcation) Specification	P209 (11/92)	Informational (Superseded)

3.4.6.6.2 Alternative specifications. The following specifications are also available:

a. USL: Tuxedo
b. Transarc: Encina
c. NCR: Top End

3.4.6.6.3 Standards deficiencies. The TX specification does not support traditional transaction monitor functions such as screen management and terminal management.

3.4.6.6.4 Portability caveats. Unlike the XA interface, which had no installed base to displace, every transaction processing system has its own interface between the application and the transaction manager that delimits a transaction. Therefore gains in multivendor portability for new systems are offset by a decrease in portability across legacy TP systems.
Without a standard API between transaction processing applications and transaction managers, portable formal and de facto standardized Fourth Generation Languages (4GLs) are unlikely to be developed. Furthermore, vendors will develop and port their 4GLs only to the most popular, best-selling transaction processing platforms.

The IEEE P1003.11 group, which was developing a profile for transaction processing environments, has been disbanded. The P1003.11 draft documents and current work are being transferred to the P1003.0 group.

3.4.6.6.5 Related standards. The following standards are related to transaction demarcation or transaction demarcation standards:

a. ISO 9579-1: RDA (Generic, Model, Service and Protocol)

b. ISO 9579-2: RDA (SQL Specialization)

c. ISO 9594 Parts 1-8: Directory Services

d. ISO 10026-1, -2, -3: DTP Protocol

e. ISO DIS 10148: RPC

f. ISO WD 10181-1, -2, -3: Security Frameworks in Open Systems, Part 1: Overview, Part 2: Authentication Framework, Part 3: Access Control Framework

g. ISO 11578: RPC

h. IEEE P1003.1b: Real-Time Extension to POSIX

i. IEEE P1003.1c: Threads Extension to POSIX

j. IEEE P1003.17: Directory Services API

k. ECMA TR/SE-ODP

l. ECMA TR/29: Open Systems Interconnection - Distributed Interactive Processing Environment

m. ECMA 127: RPC

n. OSF: DCE RPC

o. X/Open S423: XA+ Interfaces

3.4.6.6.6 Recommendations. The TX specification is recommended and must be referenced specifically in procurement specifications. Otherwise, vendors probably will propose products that do not meet this specification.

Plan for at least two interfaces: the TX interface for new multivendor, distributed systems and the legacy TP interface for existing TP systems. The TX Specification and XA Specification are complementary specifications the MIA consortia's STDL (Standardized Transaction Definition Language) However, may provide great acceptance by certain large vendors.

3.4.6.7 Transaction monitoring services and interfaces. Transaction management systems monitor network transaction flow and workload balance.

3.4.6.7.1 Standards. Table 3.4-29 presents standards for transaction monitoring services and interfaces.

TABLE 3.4-29 Transaction monitoring services and interfaces standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.4.6.7.2 Alternative specifications. The following specifications are also available:

a. USL: Tuxedo
b. Transarc: Encina
c. NCR: Top End

3 4.6.7.3 Standards deficiencies. A requirement has been identified for a standardized transaction management system to manage network transaction flow and workload balancing.

3.4.6.7.4 Portability caveats. This is a high portability risk area because no standards exist.

3.4.6.7.5 Related standards. The following standards are related to transaction monitoring or transaction monitoring standards:

a. ISO 9041-1: Basic Class Virtual Terminal Protocol Specification

b. ISO 9075:1992: SQL Third Edition (same as NIST FIPS PUB 127-2:1993)

c. ISO 9579-1: RDA (Generic Model, Service and Protocol)

d. ISO 9579-2: RDA (SQL Specialization)

e. ISO 9804/9805: CCR

f. ISO DIS 10148: RPC

g. ISO WD 10181-1, -2, -3: Security Frameworks in Open Systems: Part 1: Overview; Part 2 Authentication Framework; Part 3: Access Control Framework

h. ISO 11578: RPC

i. IEEE P1003.1b: Real-Time Extension to POSIX

j. IEEE P1003.1c: Threads Extension to POSIX

k. ECMA 127: RPC

l. OSF: DCE RPC

m. X/Open C193: XA Interfaces

3.4.6.7.6 Recommendations. USL's Tuxedo and Transarc's Encina show signs of becoming de facto standards. Tuxedo is the only DTP system that is not beginning to emerge and has field experience (e.g., Version 4.X is offered, rather than Version 1.X). Tuxedo also formed the base document for X/Open's XA and TX interfaces. On the other hand, Encina is designed to be integrated more easily integrated with legacy TP systems. Therefore, Encina is central to the TP directions and strategies of several major TP vendors, however, there are no standards to recommend.

3.4.6.8 Terminal communications. These standards provide support for terminal communications in a transaction processing system.

3.4.6.8.1 Standards. Table 3.4-30 presents standards for terminal communications.

TABLE 3.4-30 Terminal communications standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.4.6.8.2 Alternative specifications. The following specifications are also available:

a. USL: Tuxedo
b. Transarc: Encina
c. NCR: Top End

3.4.6.8.3 Standards deficiencies. Deficiencies in the standards are unknown.

3.4.6.8.4 Portability caveats. This is a high portability risk area because no standards exist. The IEEE P1003.11 group, which was developing a profile for transaction processing environments, has been disbanded. The P1003.11 draft documents and current work are being transferred to the P1003.0 group.

3.4.6.8.5 Related standards. The following standards are related to terminal communications or terminal communications standards:

a. ISO 9041-1: Basic Class Virtual Terminal Protocol Specification

b. ISO 9075:1992: SQL Third Edition (same as NIST FIPS PUB 127-2:1993)

c. ISO 9579-1: RDA (Generic Model, Service and Protocol)

d. ISO 9579-2: RDA (SQL Specialization)

e. ISO 9594 Parts 1-8: Directory Services

f. ISO 9804/9805: CCR

g. ISO DIS 10148: RPC

h. ISO WD 10181-1: Security Frameworks in Open Systems: Part 1: Overview

i. ISO DIS 10181-2: Security Frameworks in Open Systems: Part 2: Authentication Framework

j. ISO DIS 10181-3: Security Frameworks in Open Systems: Part 3: Access Control Framework

k. ISO 11578: RPC

l. ITU-T Recommendation X.500

m. IEEE P1003.1b: Real-Time Extension to POSIX

n. IEEE P1003.1c: Threads Extension to POSIX

o. IEEE P1003.17: Directory Services API

p. ECMA TR/SE-ODP

q. ECMA TR/29: Open Systems Interconnection - Distributed Interactive Processing Environment

r. ECMA 127: RPC

s. OSF: DCE RPC

t. X/Open C193: XA Interfaces

3.4.6.8.6 Recommendations. USL's Tuxedo and Transarc's Encina have interfaces in this area. Both show signs of becoming de facto standards. Tuxedo also formed the base document for X/Open's XA and TX interfaces. On the other hand, Encina is designed to be integrated more easily with legacy TP systems including IBM mainframes. Therefore, Encina is central to the TP directions and strategies of several major TP vendors. There are no standards to recommend.

3.4.6.9 Transaction program scheduling. These standards provide scheduling support for transaction processing.

3.4.6.9.1 Standards. Table 3.4-31 presents standards for transaction program scheduling.

TABLE 3.4-31 Transaction program scheduling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.4.6.9.2 Alternative specifications. The following specifications are also available:

a. USL: Tuxedo
b. Transarc: Encina
c. NCR: Top End

3.4.6.9.3 Standards deficiencies. Deficiencies in the emerging IEEE standard are unknown.

3.4.6.9.4 Portability caveats. This is a high portability risk area because no standards exist. The IEEE P1003.11 group, which was developing a profile for transaction processing environments, has been disbanded. The P1003.11 draft documents and current work are being transferred to the P1003.0 group.

3.4.6.9.5 Related standards. The following standards are related to transaction program scheduling or transaction program scheduling standards:

a. ISO 9041-1: Basic Class Virtual Terminal Protocol Specification
b. ISO 9075: 1992: SQL Third Edition (same as NIST FIPS PUB 127-2: 1993)
c. IEEE P1003.1c: Threads Extension to POSIX

3.4.6.9.6 Recommendations. There are no standards to recommend.

3.4.6.10 Transaction message queuing. These standards provide specifications for a message queue in a transaction processing environment.

3.4.6.10.1 Standards. Table 3.4-32 presents standards for transaction message queuing.

TABLE 3.4-32 Transaction message queuing standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.4.6.10.2 Alternative specifications. The following specifications are also available:

a. USL: Tuxedo
b. Transarc: Encina
c. NCR: Top End

3.4.6.10.3 Standards deficiencies. Deficiencies in the emerging IEEE standard are unknown.

3.4.6.10.4 Portability caveats. This is a high portability risk area because no standards exist. The IEEE P1003.11 group, which was developing a profile for transaction processing environments, has been disbanded. The P1003.11 draft documents and current work are being transferred to the P1003.0 group.

3.4.6.10.5 Related standards. The following standards are related to transaction message queuing or transaction message queuing standards:

a. ISO 9041-1: Basic Class Virtual Te[illegible] Protocol Specification
b. ISO 9075:1992: SQL 3rd edition
c. IEEE P1003.1b: Real-Time Extension to POSIX
d. IEEE P1003.1c: Threads Extension to POSIX

3.4.6.10.6 Recommendations. There are no standards to recommend.

3.4.6.11 Recovery and restart services for long running transactions. (This RSA appears in both part 4 and part 9.) Checkpoint and restart is provided for interactive transactions on centralized systems via the SQL "commit" and "rollback" commands, and for short-running transactions on distributed systems via the 2-Phase Commit specified in the ISO CCR standard. However, long running transactions require standardized checkpointing, restarting, and migration services and interfaces to prevent the loss of the transaction if a system fails or shuts down. Two APIs must be standardized for this purpose. One will allow application control of the checkpoint. The other will allow the transaction manager to control the checkpointing and restart activity over a range of heterogeneous resource managers.

3.4.6.11.1 Standards. Table 3.4-33 presents standards for recovery and restart services for long running transactions.

TABLE 3.4-33 Recovery and restart services for long running transactions standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 2:Shell and Utilities - Amendment 1: Batch Environment	1003.2d:1994	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1a	Informational (Draft)
NPC	IEEE	POSIX, Part 1: System API - Amendment x: Checkpoint/Restart Interfaces (C Language)	P1003.1m	Informational (Formative)

3.4.6.11.2 Alternative specifications. The following specifications are also available:

a. USL: Tuxedo
b. Transarc: Encina
c. NCR: Top End

3.4.6.11.3 Standards deficiencies. Based on a requirement from the P1003.15 Batch Queuing Extensions Standards Group, the POSIX.1 revision will specify application control of checkpointing. But this specification is geared to batch environments, and does not address the transaction manager's control of checkpoint, restart, or migration of services needed for a transaction processing environment. This need is not being addressed other than by de facto solutions.

P1003.2d specifies some capabilities needed for checkpointing and restart in batch environments, but as a standard geared to batch environments, it does not address the transaction manager's control of checkpoint, restart, or migration of services.

3.4.6.11.4 Portability caveats. Without standardized interfaces to allow application control of checkpointing and transaction manager's control of checkpointing and restart activity, portability and interoperability across heterogeneous resource managers are nonexistent, except for short-

running transactions (which are controlled via SQL's "commit" and "rollback" commands and via ISO's CCR standard).

3.4.6.11.5 Related standards. The following standards are related to recovery and restart services or standards:

a. ISO 9041-1: Basic Class Virtual Terminal Protocol Specification
b. ISO 9075:1992: SQL 3rd edition
c. IEEE 1003.1b:1993: Real-Time Extension to POSIX
d. IEEE 1003.1c:1995: Threads Extension to POSIX

3.4.6.11.6 Recommendations. There is no recommendation for recovery and restart services.

3.4.6.12 Interface to resource manager device drivers. For on-line transaction processing (OLTP) environments, device driver interfaces are needed for devices commonly requiring transaction control (e.g., ticket dispensers, automated teller machines (ATMs)). This will require two types of APIs. One API type would be extensions to the XA and XA+ interfaces, so these interfaces can support device drivers as though they were resource managers. The other API is the interface between the application and the device driver-resource manager.

3.4.6.12.1 Standards. Table 3.4-34 presents standards for interfaces to resource manager device drivers.

TABLE 3.4-34 Interface to resource manager device drivers standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.4.6.12.2 Alternative specifications. The only other available specifications are proprietary.

3.4.6.12.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.4.6.12.4 Portability caveats. This is a high portability risk area because no standards exist.

3.4.6.12.5 Related standards. The following standards are related to resource manager device driver interfaces:

a. X/Open C193: Distributed TP: The XA Interface
b. X/Open S423: Distributed TP: The XA+ Specification, version 2

3.4.6.12.6 Recommendations. There are no standards to recommend.

3.4.6.13 Distributed queuing. Distributed queuing is the waiting for services in a distributed computing environment.

3.4.6.13.1 Standards. Table 3.4-35 presents standards for distributed queuing.

TABLE 3.4-35 Distributed queuing standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 2:Shell and Utilities - Amendment 1: Batch Environment	1003.2d:1994	Mandated (Approved)
CPC	X/Open	Distributed TP: Reference Model, Version 3	G504 (2/96)	Informational (Approved)

3.4.6.13.2 Alternative specifications. The following specifications are also available:

a. AT&T/USL: Tuxedo
b. Transarc: Encina
c. NCR: Top End

3.4.6.13.3 Standards deficiencies. The 1003.2d standard is geared to batch requests, not transactional requests with associated persistence and rollback capabilities.

3.4.6.13.4 Portability caveats. Most internally built recoverable messaging and queuing facilities depend upon the underlying transport mechanism.

3.4.6.13.5 Related standards. The IEEE P1003.1a: POSIX.1 Revision is essential to the use of IEEE P1003.2d.

3.4.6.13.6 Recommendations. Use the P1003.1a (POSIX.1 Revision) checkpoint and restart interface with IEEE 1003.2d.

At present, building a recoverable messaging and queuing facility on top of whatever transport scheme is used to perform peer-to-peer communications may be necessary. Where applicable, use the emerging P1003.1a (POSIX.1 Revision) checkpoint and restart interface. If possible, establish an internal standardized interface that is independent of the underlying transport mechanism.

3.4.6.14 Modeling services. Modeling service standards simulate a condition or activity in a transaction processing system by performing a set of equations on a set of data. A model is a mathematical representation of a device or process used for analysis and planning.

3.4.6.14.1 Standards. Table 3.4-36 presents standards for modeling services.

TABLE 3.4-36 Modeling services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.4.6.14.2 Alternative specifications. The only other available specifications are proprietary.

3.4.6.14.3 Standards deficiencies. Deficiencies in the modeling services standards are unknown.

3.4.6.14.4 Portability caveats. This is a high portability risk area because no standards exist.

3.4.6.14.5 Related standards. The following standards are related to modeling services or modeling services standards:

a. ISO 9075:1992: SQL 3rd edition

b. ISO 10027:1990 (IRDS Framework)

c. ISO DP 10728 (IRDS Services Interface)

d. ANSI X3.138-1988 (IRDS Requirements and Command Language & Panel Interface)

e. ANSI X3.185-1992 (IRDS Software Services Interface)

f. NIST FIPS 156 (IRDS)

3.4.6.14.6 Recommendations. There are no standards to recommend.

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 5 of 14 parts)

DATA INTERCHANGE SERVICES

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

TABLE OF CONTENTS

LIST OF TABLES

3.5 Data interchange services. Data interchange services provide specialized support for representing, storing, accessing, and transmitting data (primarily through defining formats).

NOTE: Throughout Part 5, all tables shall have abbreviations listed under the column (Standard Type) as follows:

a. National Public Consensus = NPC
b. International Public Consensus = IPC
c. Government Public Consensus = GPC
d. Consortia Public Consensus = CPC
e. Corporate Private Non-Consensus = CPN-C

3.5.1 Characters and symbols. The characters and symbols (not symbology) midlevel service area includes standards for services such as character sets and typefaces.

3.5.1.1 Coded character sets. (This BSA appears in both part 5, Data Interchange, and part 14, Internationalization.) A character set is a subset of all letters in different alphabets, numbers, punctuation marks, mathematical symbols, and other characters used by computers. These services include the capability to input, store, manipulate, retrieve, communicate, and present data independent of the coding scheme used.

3.5.1.1.1 Standards. Table 3.5-1 presents standards for coded character sets.

TABLE 3.5-1 Coded character sets standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Coded Graphic Character Set for Text Communication - Latin Alphabet Second Edition (replaces 6937 pt.1 & pt. 2)	6937:1994	Adopted (Approved)
IPC	ISO/IEC	Coded Graphic Character Set for Use in the Preparation of Documents used in Electrotechnology and for Information Exchange	1286:1995	Informational (Approved)
IPC	ISO/IEC	Coded Graphic Character Set for Text Communication	6913	Informational (Draft)
IPC	ISO	Mathematical coded character set for bibliographic information interchange	6862	Informational (Draft)
IPC	ISO	Hebrew alphabet coded character sets for bibliographic information interchange	8957	Informational (Draft)
IPC	ISO	Armenian alphabet coded character set for bibliographic information interchange	10585	Informational (Draft)
IPC	ISO	Georgian alphabet coded character set for bibliographic information interchange	10586	Informational (Draft)
IPC	ISO/IEC	Coded Character Sets for Text Communication, Parts 0, 3, 7, 8	6937-0,3,7,8:1994	Informational (Draft)
IPC	ISO/IEC	Coded Character Sets for Text Communication, Parts 4, 5, 6	6937-4,5,6	Informational (Formative)

3.5.1.1.2 Alternative specifications. Alternative character coding schemes include Encoded Binary Decimal (EBCDC) and the Macintosh character set.

3.5.1.1.3 Standards deficiencies. The greatest deficiency any of these standards have is narrow applicability to a single application or language or no standard means of translation from set to set.

3.5.1.1.4 Portability caveats. Character sets are generally portable, but there are sometimes questions about conversion between sets.

3.5.1.1.5 Related standards. The following standards are related to coded character set standards:

a. NIST FIPS 19-2: Catalog of Widely Used Code Sets

b. Optical Character Recognition (OCR) Character Code Sets:

(1) SO 1073-1:1976: Alphanumeric character sets for optical recognition- Part 1: Character set OCR-A -- Shapes and dimensions of the printed image

(2) SO 1073-2:1976: Alphanumeric character sets for optical recognition- Part 2: Character set OCR-B -- Shapes and dimensions of the printed image

(3) SO 1831:1980: Printing specifications for optical character recognition

(4) SO 2033:1983: Information processing -- Coding of machine readable characters (MICR and OCR)

c. Magnetic Ink Character Recognition (MICR) Character Sets

(1) SO 2033:1983: Information processing -- Coding of machine readable characters (MICR and OCR)

(2) SO 1004:1995: Information Processing - Magnetic ink character recognition - Print specifications

3.5.1.1.6 Recommendations. ISO 6937 is recommended for ordinary English-only alphabetic applications.

3.5.1.2 Font information interchange. (This BSA appears in part 5, Data Interchange, and part 12, Multimedia.) Font information interchange standards specify the encoding of font resource information for use in document processing environments. Font interchange deals with the exchange of character fonts, such as Times Roman or Helvetica, and related information as opposed to simple exchange of character encodings, which do not include font information.

3.5.1.2.1 Standards. Table 3.5-2 presents standards for font information interchange.

TABLE 3.5-2 Font information interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Font Information Interchange, Part 1: Architecture (Corrigendum 1-1992, Corrigendum 2-1994)	9541-1:1991	Adopted (Approved)
IPC	ISO/IEC	Font Information Interchange, Part 2: Interchange Format (Corrigendum 1-1993)	9541-2:1991	Adopted (Approved)
IPC	ISO/IEC	Font Information Interchange, Part 3: Glyph Shape Representation	9541-3:1994	Adopted (Approved)
IPC	ISO/IEC	Font Information Interchange - Procedure for Registration of Glyph and Glyph Collection Identifiers	10036:1993	Informational (Approved)
GPC	NIST	Guideline for Optical Character Recognition Print Quality (adopts ANSI X3.99-1983)	FIPS PUB 90:1983	Informational (Approved)
CPN-C	Adobe	PostScript Type 1 - Outlines	PS Tech. Manuals	Informational (Approved)
CPN-C	Microsoft	TrueType - Outlines	TT Tech. Manuals	Informational (Approved)
IPC	ISO/IEC	Font Information Interchange, Part 4: Character Collections	9541-4	Informational (Draft)
IPC	ISO/IEC	Font Information Interchange, Part 5: Font Attributes and Character Model	9541-5	Informational (Draft)
IPC	ISO/IEC	Font Information Interchange, Part 6: Font and Character Attribute Subsets and Application	9541-6	Informational (Draft)
IPC	ISO/IEC	Font Information Interchange, Part 7: Font Interchange Format	9541-7	Informational (Draft)

3.5.1.2.2 Alternative specifications. Alternative specifications include TrueType and PostScript.

3.5.1.2.3 Standards deficiencies. There is and will be very little standardization of font names, because of copyright concerns. None of the existing font interchange standards accurately enable font substitution. However, many systems are attempting font substitution, that is, replacing a specified font with one that is similar, such as substituting TrueType Arial for PostScript Helvetica.

No standard exists for three-dimensional font families, although such text is becoming popular in display text applications, such as advertising and presentations.

3.5.1.2.4 Portability caveats. Target presentation systems and viewers may not have the required fonts to construct the called-for text in a presentation system. Font substitution may result in an unexpected text presentation. Outline font geometry also can be represented as two-dimensional graphics geometry, which eliminates the need to support a specific font on a target platform.

3.5.1.2.5 Related standards. Standards related to font information interchange standards are:

a. ISO 8632: Computer Graphics Metafile (CGM)
b. X Logical Font Description (see part 3)
c. PostScript Level 2 (starting to be used for colored text)

3.5.1.2.6 Recommendations. If CGM is being used, then ISO 8632-1 DAM 3 also is needed for font information exchange along with ISO 9541. The ISO 9541 specifies the architecture and format for various shape descriptions to be used in document processing environments that recognize Abstract Syntax Notation (ASN).1 or SGML parsing algorithms. ISO 9541 uses Adobe System's PostScript Type-I font technology and file formats. The ISO 9541 is recommended for font information exchange.

For some applications, such as view-only kiosks and presentations, convert text to a graphics format to avoid unknown font resource issues. Use fonts that are in common usage for cross-platform work.

3.5.1.3 Date and time representation. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Date and time representation and storage require consideration and standardization. Problems include representation of twelve or twenty-four hour time, the order in which the day and month are presented, and dropping of the century digits from the year.

3.5.1.3.1 Standards. Table 3.5-3 presents standards for date and time representation.

TABLE 3.5-3 Date and time representation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Defense Data Dictionary System (DDDS), Version 3.2, May 1996	DDDS Ver. 3.2	Mandated (Approved)
GPC	NIST	Representation of Calendar Date and Ordinal Date for Information Interchange (adopts ANSI X3.30-1985/R1991)	FIPS PUB 4-1:1988 Change Notice 3/25/96	Informational (Approved)
GPC	NIST	Representation of Local Time of the Day for Information Exchange (adopts ANSI X3.43-1986)	FIPS PUB 58-1:1988	Informational (Approved)
GPC	NIST	Representations of Universal Time, Local Time Differentials, and US Time Zone References for Information Interchange (Adopts ANSI X3.51-1979)	FIPS PUB 59:1979	Informational (Approved)
IPC	ISO	Representation of Dates and Times	8601:1988	Informational (Approved)
NPC	ANSI	Representation of Calendar Date and Ordinal Date for Information Interchange	X3. 30-1985 (R1991)	Informational (Approved)
NPC	ANSI	Representation of Local Time of Day for Information Interchange	X3. 43-1986 (R1992)	Informational (Approved)
NPC	ANSI	Representations of Universal Time, Local Time Differentials, and US Time Zone References	X3. 51-1994	Informational (Approved)
NPC	ANSI/EIA	Source and Date Code Marking	476-A:1987	Informational (Approved)

3.5.1.3.2 Alternative specifications. There are no other available specifications.

3.5.1.3.3 Standards deficiencies. In the early days of computer technology, information storage space was at a premium. Engineers saved space by using only the last two digits of the year rather than using full four-digit year representation since they did not anticipate that existing systems would still be in operation in the year 2000. This is a problem to be kept in mind during data design for information systems and their databases. The internal representation of the year and dates is expected to cause enormous difficulties as the year 2000 arrives.

3.5.1.3.4 Portability caveats. The difference between a little-endian (i.e., 11 May 1995), a big-endian (i.e., 1995 May 11), and mixed mode (i.e., May 11, 1995) date representation can be a portability problem for systems. The stated DoD data element for date format is "YYYYMMDD" where YYYY is the year, MM is the month, and DD is the day. NIST highly recommends that four-digit year elements be used and that two-digit year elements NOT be used for data interchange. On March 25, 1996 NIST published a change notice to FIPS 4-1 that highly recommends four-digit year elements, and states that two-year elements specified in ANSI

X3.30:1985 (R1991) should not be used for the purpose of any data interchange among U.S. Government agencies.

The eight-digit date format is required for all system interfaces and data exchanges in DoD. The Defense Data Dictionary System (DDDS) Generic Element Name: Date is mandatory in the design of DoD databases (DoD Directive 8320.1, Sept 26, 1991). The DoD data standard is required to be used in new systems developments, including commercial off-the-shelf replacements; migration systems; and any system receiving major changes.

3.5.1.3.5 Related standards. The following standard is related to date and time representation:

a. NIST FIPS 34, Guide for the Use of International System of Units in FIPS PUBS

3.5.1.3.6 Recommendations. For purposes of data interchange, DoD requires that year, month, and day be represented as 'YYYYMMDD'.

3.5.1.4 Seven-bit coded character sets. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Character sets which contain only as many characters as can be uniquely identified using a seven-bit number (i.e., 128 characters numbered 0 to 127).

3.5.1.4.1 Standards. Table 3.5-4 presents standards for seven-bit coded character sets.

TABLE 3.5-4 Seven-bit coded character sets standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Code for Information Interchange, Its Representations, Subsets, and Extensions (ASCII) (adopts ANSI X3.4-1986/R 1992, X3.32-1990, X3.41-1974)	FIPS PUB 1-2:1984	Adopted (Approved)
IPC	ISO	ISO 7-Bit Coded Character Set for Information Exchange	646:1991	Adopted (Approved)
IPC	ISO	Information Processing - Representation of the 7-Bit Coded Character Set on Punched Tape	1113:1979	Informational (Approved)
NPC	ANSI	Code Extension Techniques for Use with the 7-Bit Coded Character Set of American National Standard Code for Information Interchange	X3. 41-1974	Informational (Approved)
IPC	ISO	Information Processing - Arabic 7-Bit Coded Character Set for Information Interchange	9036:1987	Informational (Approved)
IPC	NATO	Parameters and Practices for the Use of the NATO 7-Bit Code	STANAG 5036	Informational (Approved)
IPC	NATO	Interoperable Characters for Teleprinters Using NATO 7-Bit Code	STANAG 5045	Informational (Approved)

ISO 646 describes a set of 128 control, alphabetic, digit, and symbol characters. It includes the use of the control characters and describes the option of national replacement characters. It is the standard that formed the basis for creating additional standards that extend the character set to include many languages. A variant, ISO 646:1991 IRV, left open an additional 128 codes to be used to represent symbols for other languages.

3.5.1.4.2 Alternative specifications. Alternative character coding schemes include Encoded Binary Decimal (EBCDC) and the Macintosh character set.

3.5.1.4.3 Standards deficiencies. The greatest deficiency any of these standards have is narrow applicability to a single application or language or no standard means of translation from set to set.

3.5.1.4.4 Portability caveats. Character sets are generally portable, but there are sometimes questions about conversion between sets. FIPS 19-2, a catalog of widely used code sets that lists and briefly describes code sets in wide use in the United States and might be used in Federal data systems, may be helpful to consult.

3.5.1.4.5 Related standards. The following standards are related to seven-bit coded character sets:

a. NIST FIPS 19-2: Catalog of Widely Used Code Sets

b. Optical Character Recognition Character Code Sets

c. ISO 3275:1974-- Implementation of the 7-bit coded character set and its 7-bit and 8-bit extensions on 3,81 mm magnetic cassette for data interchange

d. ISO 6586:1980 -- Implementation of the ISO 7-bit and 8-bit coded character sets on punched cards

e. ISO 1113:1979 -- Representation of the 7-bit coded character set on punched tape

3.5.1.4.6 Recommendations. FIPS 1-2, which adopts the ASCII character set, is recommended for common applications. ISO 646 is also recommended.

3.5.1.5 Eight-bit coded character sets. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Character sets which contain only as many characters as can be uniquely identified using an eight-bit number (typically, 256 characters numbered 0 to 255).

3.5.1.5.1 Standards. Table 3.5-5 presents standards for eight-bit coded character sets.

TABLE 3.5-5 Eight-bit coded character sets standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC/IPC	ANSI/ISO/IEC	ISO 8-Bit Code for Information Interchange - Structure and Rules for Implementation (8-Bit ASCII) (Revision and redesignation of ANSI X3.134.1)	4873:1991	Adopted (Approved)
IPC	ISO/IEC	Standardized Coded Graphic Character Sets for Use in 8-Bit Codes	10367:1991	Informational (Approved)
IPC	ECMA	8-Bit Coded Character Set	6 (1991)	Informational (Approved)
IPC	ECMA	8-Bit Coded Character Set Structure and Rules	43 (1991)	Informational (Approved)

3.5.1.5.2 Alternative specifications. Alternative character coding schemes include EBCDC and the Macintosh character set.

3.5.1.5.3 Standards deficiencies. The greatest deficiency any of these standards have is narrow applicability to a single application or language or no standard means of translation from set to set.

3.5.1.5.4 Portability caveats. Character sets are generally portable, but there are sometimes questions about conversion between sets.

3.5.1.5.5 Related standards. The following standards are related to eight-bit coded character sets:

a. NIST FIPS 19-2: Catalog of Widely Used Code Sets

b. OCR Character Code Sets

c. ISO 3275:1974-- Implementation of the 7-bit coded character set and its 7-bit and 8-bit extensions on 3,81 mm magnetic cassette for data interchange

d. ISO 6586:1980 -- Implementation of the ISO 7-bit and 8-bit coded character sets on punched cards

3.5.1.5.6 Recommendations. ISO 4873 is recommended.

3.5.1.6 Eight-bit single byte character sets. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Character sets which contain only as many characters as can be uniquely identified using an eight-bit number in a single byte (typically. but not always, 256 characters numbered 0 to 255).

3.5.1.6.1 Standards. Table 3.5-6 presents standards for eight-bit single byte character sets.

TABLE 3.5-6 Eight-bit single byte character sets standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	ISO 8-Bit Single-Byte Coded Graphic Character Sets: Parts 1-9	8859-1 to 9:1987-1989	Mandated (Approved)
IPC	ISO/IEC	ISO 8-Bit Single-Byte Coded Graphic Character Sets: Part 10: Latin Alphabet Set No. 6	8859-10:1992	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets, Latin Alphabets No. 1 to No. 4	94 (1986)	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets - Latin/Cyrillic Alphabet	113 (1988)	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets - Latin/Arabic Alphabet	114 (1986)	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets - Latin/Greek Alphabet	118 (1986)	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets - Latin/Hebrew Alphabet	121 (1987)	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets, Latin Alphabet No. 5	128 (1988)	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets - Latin Alphabet No. 6	144 (1992)	Informational (Approved)

ISO 8859 defines a set of 191 graphic characters with a single 8-bit byte. It uses the characters 0x20 through 0x7F to represent those used in the US-ASCII (ISO 646) set.

3.5.1.6.2 Alternative specifications. Alternative character coding schemes include EBCDC and the Macintosh character set.

3.5.1.6.3 Standards deficiencies. The greatest deficiency any of these standards have is narrow applicability to a single application or language or no standard means of translation from set to set.

3.5.1.6.4 Portability caveats. Character sets are generally portable, but there are sometimes questions about conversion between sets.

3.5.1.6.5 Related standards. The following standards are related to eight-bit single byte character sets:

a. NIST FIPS 19-2: Catalog of Widely Used Code Sets
b. Optical Character Recognition Character Code Sets

3.5.1.6.6 Recommendations. ISO 8859, parts 1-9, is recommended.

3.5.1.7 Control functions. (This BSA appears in part 5, Data Interchange and part 14, Internationalization.) This service area is for definition and coding of control functions for inclusion in character sets.

3.5.1.7.1 Standards. Table 3.5-7 presents standards for control functions.

TABLE 3.5-7 Control functions standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Control Functions for ISO 7-Bit and 8-Bit Coded Character Sets	6429:1992	Adopted (Approved)
GPC	NIST	Additional Controls for Use with American National Standard Code for Information Interchange (adopts ANSI X3.64-1979/R1990)	FIPS PUB 86:1981	Informational (Approved)
IPC	ISO	Information Processing - Graphical Representations for the Control Characters of the 7-Bit Coded Character Set	2047:1975	Informational (Approved)
IPC	ISO	Bibliographic control characters	6630:1986	Informational (Approved)
IPC	ECMA	Control Functions for Coded Character Sets	48 (1991)	Informational (Approved)
IPC	ECMA	Graphic Representation of the Control Characters of the ECMA 7-Bit Coded Character Set for Information Interchange	17 (1968)	Informational (Canceled)

ISO 6429 defines a 7-bit, 7-bit extended, 8-bit, and an 8-bit extended character set control.

3.5.1.7.2 Alternative specifications. There are no alternative specifications.

3.5.1.7.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.1.7.4 Portability caveats. Portability problems with the existing standards are unknown.

3.5.1.7.5 Related standards. There are no related standards.

3.5.1.7.6 Recommendations. ISO 6429 is recommended.

3.5.1.8 Character set conversion. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Character set conversion deals with the problem of translating from one character set to another.

3.5.1.8.1 Standards. Table 3.5-8 presents standards for character set conversion.

TABLE 3.5-8 Character set conversion standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Conversion Between the Two Coded Character Sets of ISO 646 and ISO 6937-2 and the CCITT International Telegraph Alphabet No. 2 (ITA2)	6936:1988	Informational (Approved)
IPC	ISO	Conversion Between the Two Coded Character Sets of ISO 646 and ISO 6937-2 and the CCITT International Telegraph Alphabet No. 2 (ITA2): Revisions	6936 Revisions	Informational (Formative)

ISO 6936 specifies conversion between the 58 character ITA2 set and the 128 character ISO 646 set.

3.5.1.8.2 Alternative specifications. There are alternative specifications that are sometimes necessary:

a. Mac to ASCII
b. EBCDC to ASCII

3.5.1.8.3 Standards deficiencies. The greatest deficiency any of these standards have is narrow applicability to a single application or language or no standard means of translation from set to set.

3.5.1.8.4 Portability caveats. Character sets are generally portable, but there are sometimes questions about conversion between sets.

3.5.1.8.5 Related standards. The following standards are related to character sets conversion:

a. Transliteration standards.

3.5.1.8.6 Recommendations. There are no recommendations. Character set conversion standards depend on which sets are involved.

3.5.1.9 Code extension techniques. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) There is also a need to define standard techniques for expanding the number of characters represented by a character set. Switching between character sets in mid-string is done by escape sequences.

3.5.1.9.1 Standards. Table 3.5-9 presents standards for code extension techniques.

TABLE 3.5-9 Code extension techniques standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Character Code Structure and Extension Techniques	2022:1994	Adopted (Approved)
IPC	ISO	Information Processing - Implementation of the 7-Bit Coded Character Set and Its 7-Bit and 8-Bit Extensions on 3,81 mm Magnetic Tape Cassette for Data Interchange	3275:1974	Informational (Approved)
IPC	ISO	Extension of the Latin Alphabet Coded Character Set for Bibliographic Information Interchange	5426:1983	Informational (Approved)
IPC	ISO	Extension of the Cyrillic Alphabet Coded Character Set for Bibliographic Information Interchange	5427:1984	Informational (Approved)
IPC	ISO	Greek Alphabet Coded Character Set for Bibliographic Information Interchange	5428:1984	Informational (Approved)
IPC	ISO	Documentation - African Coded Character Set for Bibliographic Information Interchange	6438:1983	Informational (Approved)
IPC	ECMA	Code Extension Techniques	35 (1994)	Informational (Approved)
IPC	ISO	Extension of the Cyrillic alphabet coded character set for non-Slavonic languages for bibliographic information interchange	10754	Informational (Draft)
IPC	ISO/IEC	ISP for Code Structures Based on ISO/IEC 2022 Part 1: FCS111-2022 Option 1	12070-1:1995	Informational (Draft)
IPC	ISO	Extension of the Latin Alphabet Coded Character Set for Bibliographic Information Interchange: part 2: Latin characters used in minor European languages and obsolete typography	5426-2	Informational (Draft)
IPC	ISO	Extensions of the Arabic alphabet coded character set for bibliographic information interchange	11822	Informational (Draft)
IPC	ISO/IEC	ISO 7-Bit and 8-Bit Coded Character Sets - Code Extension Techniques	2022:1986	Informational (Superseded)

3.5.1.9.2 Alternative specifications. Alternative specifications would include other, larger, forms of character sets (8-bit instead of 7-bit, or multiple-octet sets instead of 8-bit).

3.5.1.9.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.1.9.4 Portability caveats. Few systems support the ISO 2022 encoding architecture because escape sequences present difficulties to processing.

3.5.1.9.5 Related standards. There are no related standards.

3.5.1.9.6 Recommendations. ISO 2022 is recommended.

3.5.1.10 Universal character sets. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Universal character sets are an approach to defining the broadest possible character set. This involves using more than an 8-bit code. Use of a 16-bit code allows for a character set of 32,768 characters, which is sufficient to cover several complete alphabets, including accented letters. The object of UCS is to represent the written form of world languages unambiguously to facilit information interchange

3.5.1.10.1 Standards. Table 3.5-10 presents standards for universal character sets.

TABLE 3.5-10 Universal character sets standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Universal Multiple-Octet Coded Character Set (UCS), Part 1: Architecture and Basic Multilingual Plane (with Technical Corrigendum 1: 1996)	10646-1:1993	Mandated (Approved)
CPC	X/Open	Universal Multiple-Octet Coded Character Set Coexistence and Migration	E401 (3/94)	Informational (Approved)
CPC	Unicode Consortium	Unicode version 1.1	UCS-2	Informational (Approved)
IPC	ISO/IEC	Universal Multiple-Octet Coded Character Set, Part 1: Architecture and Basic Multilingual Plane, Amend 1: Transform Format for 16 Planes of Group 00 (UTF-16), Amend 2: UCS Transform Format 8 (UTF-8), Amend 3: control characters, Amend 4: remove UTF-1 to a	10646-1, Am 1-4:1993	Informational (Draft)
IPC	ISO	Universal Multiple-Octet Coded Character Set, Part 1: Architecture and Basic Multilingual Plane, Amend 5: Korean Hangul, Amend 6: Tibetan additions, Amend 7, Amend 8: Han unification	10646-1: DAM 5-8	Informational (Draft)

ISO 10646 is an extension of ISO 8859. A separate part of 8859 is defined for a variety of character sets. The 10646 is multiple-octet character set that can be encoded using 8-, 16-, or 32-bit character sizes. All existing character sets in 8859 are included as pages in the 10646 encoding, along with virtually all known characters on the planet. The 10646 is effectively the dictionary of coded character sets.

3.5.1.10.2 Alternative specifications. There are no alternatives for a universal character set.

3.5.1.10.3 Standards deficiencies. Only a small number of modern languages are unrepresentable by these standards, but are expected to be supported soon.

3.5.1.10.4 Portability caveats. The portability problems with universal character sets involve their multi-byte nature. Translation to and from single-byte sets is full of chances for errors.

3.5.1.10.5 Related standards. There are no related standards.

3.5.1.10.6 Recommendations. If multiple-octet representations (16- or 32-bit) of characters are required, ISO 10646 is recommended.

3.5.1.11 External data representation. External data representation standards specify the encoding for common, low-level data types to resolve the differences in data type representation between platforms and applications.

3.5.1.11.1 Standards. Table 3.5-11 presents standards for external data representation.

TABLE 3.5-11 External data representation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ITU-T	External Data Representation (XDR) for use with X.400	X.409	Adopted (Approved)
NPC	IEEE	Open Systems Interconnection (OSI) Abstract Data Manipulation - Application Program Interface (API) (Language Independent)	1224:1993	Informational (Approved)
NPC	IEEE	Test Methods for Measuring Conformance to Open Systems Interconnection (OSI) Abstract Data Manipulation - Application Program Interface (API) (Language Independent)	1326:1993	Informational (Approved)
NPC	IEEE	Open Systems Interconnection (OSI) Abstract Data Manipulation C Language Interfaces - Binding for Application Program Interface (API)	1327:1993	Informational (Approved)
NPC	IEEE	Test Methods for Measuring Conformance to Open Systems Interconnection (OSI) Abstract Data Manipulation C Language Interfaces - Binding for Application Program Interface (API)	1328:1993	Informational (Approved)
IPC	ISO	Specification for a Data Descriptive File for Information Interchange (DDF)	8211:1985	Informational (Approved)
IPC	ISO/IEC	OSI Specification of Abstract Syntax Notation One (ASN.1)	8824:1990	Informational (Approved)
IPC	ISO/IEC	OSI Abstract Syntax Notation One (ASN.1): Specification of Basic Notation	8824-1:1995	Informational (Approved)
IPC	ISO/IEC	OSI Abstract Syntax Notation One (ASN.1): Information Object Specification	8824-2:1995	Informational (Approved)
IPC	ISO/IEC	OSI Abstract Syntax Notation One (ASN.1): Constraint Specification	8824-3:1995	Informational (Approved)
IPC	ISO/IEC	OSI Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 Specifications	8824-4:1995	Informational (Approved)
IPC	ISO/IEC	OSI Specification of Basic Encoding Rules (BER) for Abstract Syntax Notation One (ASN.1)	8825:1990	Informational (Approved)
IPC	ISO/IEC	OSI -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)	8825-1:1995	Informational (Approved)
IPC	ISO/IEC	OSI -- ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)	8825-2:1996	Informational (Approved)
CPC	X/Open	Protocols for X/Open PC Internetworking: (PC)NFS	D030 (8/90)	Informational (Approved)
CPC	OSF	External Data Representation (XDR) (For use with DCE's RPC)	DCE XDR	Informational (Approved)
GPC	NIST	Catalog of Widely Used Code Sets	FIPS PUB 19-2:1992	Informational (Approved)
GPC	NIST	Specification for a Data Descriptive File for Information Interchange (DDF) (adopts ANSI/ISO 8211:1985/R1992)	FIPS PUB 123:1986	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	IETF	XDR: External Data Representation Standard (same as X/Open XDR)	RFC 1014:1987	Informational (Approved)
IPC	NATO	NATO Reference Model for Open Systems Interconnections - Specification of Abstract Syntax Notation 1 (ASN.1)	STANAG 4258 1993	Informational (Approved)
IPC	NATO	NATO Reference Model for Open Systems Interconnection - Encoding Rules for ASN.1	STANAG 4259	Informational (Approved)
IPC	ITU-T	Specification of Abstract Syntax Notation one (ASN.1) - OSI Model and Notation, Service Definition	X.208 (1989)	Informational (Approved)
IPC	ITU-T	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) - Data Communication Networks - Open Systems Interconnection (OSI) Model and Notation, Service Definition	X.209 (1989)	Informational (Approved)
IPC	ISO/IEC	Open Systems Interconnection - Conformance Test Suite for the Presentation Layer - Part 2: Test Suite Structure and Test Purposes for the ASN.1 Basic Encodings	10729-2:1993	Informational (Draft)
IPC	ISO/IEC	OSI Abstract Syntax Notation one (ASN.1) Revision: Part 5: Character Sets	8824-5	Informational (Formative)
IPC	ISO/IEC	OSI Specification of ASN.1 Basic Encoding Rules Revision: Part 4: Light Weight Encoding Rules (LWER)	8825-4	Informational (Formative)

3.5.1.11.2 Alternative specifications. No other consortia or de facto specifications are available.

3.5.1.11.3 Standards deficiencies. ASN.1 is a highly complex, difficult-to-use language for describing Open Systems Interconnect (OSI) objects, with a complicated set of Basic Encoding Rules. Neither the ASN.1 nor the X.409 standards are suitable for use with generic remote procedure calls used in application development. The 1987 Basic Encoding Rules (BER) international standard, which is specified by the Government Open Systems Interconnection Profile (GOSIP), provides a lengthy, verbose representation, compared to the more compact representation achieved by the Distinguished Encoding Rules (DER) (8824 Revision: Part 2). It encodes and decodes data slower than the Light Weight Encoding Rules (LWER) (8825 Revision: Part 4). Request for Comment (RFC) 1014, developed originally by Sun Microsystems for use with the Network File System (NFS), is an external data representation specification to describe C language data types only.

3.5.1.11.4 Portability caveats. ISO 8824 ASN.1 specifications are compatible with the International Telecommunications Union (ITU) X.208 ASN.1, except for a few ISO extensions that are not backward compatible with X.208.

X/Open's External Data Representation (XDR) specification, developed initially by Sun Microsystems for use with NFS, is not compatible with the Open Software Foundation's (OSF's) Distributed Computing Environment (DCE) Remote Procedure Call (RPC) XDR (developed initially by Apollo Computer).

3.5.1.11.5 Related standards. The following standards are related to external data representation or external data representation standards:

a. X/Open C180: OSI-Abstract-Data-Manipulation API (XOM), which provides an easier-to-use canonical representation and tools for manipulating ASN.1 objects

b. RPC: ISO DIS 11578, Parts 1-4, which will need a standardized external data representation for use in open-client server computing and cooperative processing

3.5.1.11.6 Recommendations. Specification of the 1987 versions of ASN.1 and BER (ISO IS 8824/8825) is not advisable. These standards have been revised. The earlier standards are specified in GOSIP 2 because nothing else was available when GOSIP 2 was defined. X.409 is recommended. OSF DCE XDR is recommended for use in distributed computing environments.

3.5.1.12 Character set registration. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Character set registration provides a mechanism for identifying and defining graphic character sets

3.5.1.12.1 Standards. Table 3.5-12 presents standards for character set registration.

TABLE 3.5-12 Character set registration standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Registration of Repertoires of Graphic Characters from ISO/IEC 10367	7350:1991	Informational (Approved)
IPC	ISO	Procedure for registration of escape sequences	2375:1985	Informational (Approved)

ISO 7350 specifies procedures for preparing, registering, publishing, and maintaining the register of graphic character sets and procedures for assigning identifiers to the sets.

3.5.1.12.2 Alternative specifications. There are no alternative specifications.

3.5.1.12.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.1.12.4 Portability caveats. Portability problems in the existing standards are unknown.

3.5.1.12.5 Related standards. The following standards are related to character set registration:

a. Character set standards
b. Localization standards
c. Symbols for use with data such as currency, date, time, numerical values

3.5.1.12.6 Recommendations. There are no recommendations.

3.5.1.13 Currency and funds representation. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Covers characters for and the representation of currency and monetary values.

3.5.1.13.1 Standards. Table 3.5-13 presents standards for currency and funds representation.

TABLE 3.5-13 Currency and funds representation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Codes for the Representation of Currencies and Funds	4217:1990	Informational (Approved)

3.5.1.13.2 Alternative specifications. There are no alternative specifications.

3.5.1.13.3 Standards deficiencies. Deficiencies in the standard are unknown.

3.5.1.13.4 Portability caveats. Portability problems in the standard are unknown.

3.5.1.13.5 Related standards. Numerical value representation standards and internationalization locale specifications are related.

3.5.1.13.6 Recommendations. ISO 4217 is recommended.

3.5.1.14 Country name representation. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) These standards provide for a short character combination that can be used to represent the names of countries.

3.5.1.14.1 Standards. Table 3.5-14 presents standards for country name representation.

TABLE 3.5-14 Country name representation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Countries, Dependencies, Areas of Special Sovereignty and their Principal Administrative Divisions	FIPS PUB 10-4 April 1995	Informational (Approved)
GPC	NIST	American National Standard codes for Representation of Names of Counties, Dependencies, Areas of Special Sovereignty and their Principal Administrative Divisions	FIPS PUB 104-1	Informational (Approved)
IPC	ISO	Codes for Representation of Names of Countries	3166:1993	Informational (Approved)

ISO 3166 defines a 2-letter, a 3-letter, and a numeric code for each country. The 2-letter names are well-known and accepted as internet domain names. The 3-letter codes are often used in international sports.

3.5.1.14.2 Alternative specifications. Alternative specifications would include the international codes to designate the country of registration of automobiles.

3.5.1.14.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.1.14.4 Portability caveats. Portability problems with the existing standards are unknown.

3.5.1.14.5 Related standards. There are no related standards.

3.5.1.14.6 Recommendations. There is no recommendation.

3.5.1.15 Representation of human sexes. This BSA concerns the uniform representation of human sexes for the interchange of information.

3.5.1.15.1 Standards. Table 3.5-15 presents standards for representation of human sexes.

TABLE 3.5-15 Representation of human sexes standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Representation of Human Sexes	5218:1977	Informational (Approved)

3.5.1.15.2 Alternative specifications. There are no alternative specifications.

3.5.1.15.3 Standards deficiencies. ISO 5218 does not meet the requirements of specific medical or scientific applications.

3.5.1.15.4 Portability caveats. ISO 5218 does not prescribe file sequences, storage, media, programming languages, or other features of information processing to be used in its implementation.

3.5.1.15.5 Related standards. No related standards have been identified.

3.5.1.15.6 Recommendations. ISO 5218 is recommended for use.

3.5.1.16 Representation of names of languages. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) This BSA presents standards for code to represent the names of languages.

3.5.1.16.1 Standards. Table 3.5-16 presents standards for representation of names of languages.

TABLE 3.5-16 Representation of names of languages standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Code for the Representation of Names of Languages	639:1988	Informational (Approved)
NPC	ANSI/NISO	Codes for Representation of Languages for Information Interchange	Z39.53	Informational (Approved)

3.5.1.16.2 Alternative specifications. Alternative specifications may include abbreviations in common use in entomology.

3.5.1.16.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.1.16.4 Portability caveats. Portability problems in the existing standards are unknown.

3.5.1.16.5 Related standards. The following standards are related to representation of names of languages:

a. ISO 9:1995: Transliteration of Cyrillic Characters into Latin Characters - Slavic and Non-Slavic Languages

b. ISO 233-2:1993: Information and documentation - Transliteration of Arabic Characters into Latin Characters - Part 2: Arabic Language - Simplified Transliteration

c. ISO 3602:1989: Documentation - Romanization of Japanese (kana script)

d. ISO DIS 14962: ASCII encoded English

3.5.1.16.6 Recommendations. ISO 639 is recommended.

3.5.1.17 Numerical value representation. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Numerical value representation deals with the presentation of numerical values as character strings in machine- and human- readable form.

3.5.1.17.1 Standards. Table 3.5-17 presents standards for numerical value representation.

TABLE 3.5-17 Numerical value representation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Representation of Numerical Values in Character Strings for Information Interchange	6093:1985	Informational (Approved)

ISO 6093 specifies three presentations of numerical values as character strings in machine-readable form for data interchange.

3.5.1.17.2 Alternative specifications. There are no alternative specifications.

3.5.1.17.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.1.17.4 Portability caveats. Portability problems in the existing standards are unknown.

3.5.1.17.5 Related standards. The following standards are related to numerical value representation:

a. Representation of currency

b. Representation of date/time

c. Localization

d. ANSI X3.50 1986/R1992: Representation for U.S. Customary, SI, and other Units to be used in Systems with limited character sets

e. ISO 2955:1993 - Representation of SI and other Units in Systems with limited Character Sets

3.5.1.17.6 Recommendations. ISO 6093 is recommended.

3.5.2 Hardware applications. The following base service areas deal with hardware-based data interchange, data storage issues, and hardware design support.

3.5.2.1 Printer data interchange. Printer data interchange is performed by using page description languages to describe a page to be printed so the printer processor can convert the representation directly into a page image for any printer.

3.5.2.1.1 Standards. Table 3.5-18 presents standards for printer data interchange.

TABLE 3.5-18 Printer data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Standard Page Description Language (SPDL)	10180:1992	Informational (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 46: Integrated Generic Resources: Visual Presentation	10303-46:1994	Informational (Approved)
CPN-C	Adobe	Encapsulated PostScript Format (EPSF)	EPSF Level 1	Informational (Approved)
CPN-C	Adobe	Portable Document Format (PDF)	PDF	Informational (Approved)
IPC	ISO/IEC	Information Technology - Text and office systems - Document Printing Application (DPA) - Part 2: Protocol specification	10175-2:1996	Informational (Approved)
IPC	ISO/IEC	Information Technology - Text and office systems - Document Printing Application (DPA), Part 1: Abstract service definition and procedures	10175-1:1996	Informational (Approved)

3.5.2.1.2 Alternative specifications. The following de facto specifications are available:

a. Adobe: PostScript and Display PostScript
b. Hewlett-Packard: Hewlett-Packard Page Description Language (HPDL)
c. Xerox: Interpress

3.5.2.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.2.1.4 Portability caveats. ISO 10180, SPDL, combines the best of Adobe PostScript and Xerox Interpress, along with enhancements and extensions developed by ISO. However, it is not a superset of the PostScript and Interpress page description languages. The inclusion of parts of each vendor's page description, as well as the ISO extensions, render it incompatible with either PostScript or Interpress.

Although it is a proprietary standard, EPSF is widely supported for importation of display text. However, care should be taken to ensure that tools used to deliver titles support importation of EPSF. Many raster image formats are candidates for this purpose.

3.5.2.1.5 Related standards. No standards are related to page description exchange standards.

3.5.2.1.6 Recommendations. If specifying SPDL in a procurement, the specification of a converter box that converts formats such as PostScript, Interpress, or HPDL to SPDL is recommended. SPDL is a standard with no commercial following. The proprietary specifications, such as PostScript and PDF, are dominant. If used, EPSF or PDF should be considered as an interim solution only until a public standard is available. Adobe PDF is being used frequently in DOD for formatting documents where revisions are not required. However, PDF suffers by the fact that it has not been endorsed by an open consensus standards body.

3.5.2.2 Bar coding. Bar code is an array of parallel lines of varying width used to represent data. The bar code is designed to be read optically by a data capturing device. Traditional one-dimensional bar codes use the bar's width as the code, and typically encode just an identification or account number. Two-dimensional systems hold 1,800 characters in an area the size of a postage stamp.

3.5.2.2.1 Standards. Table 3.5-19 presents standards for bar coding.

TABLE 3.5-19 Bar coding standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Standard DOD Bar Code Symbology (Code 39 Adapted for the DOD)	MIL-STD-1189B of 8/10/1989	Approved (Approved)
CPC	UCC	Serial Shipping Container Code Based on Code 128 algorithm	UCC/EAN-128:1989	Informational (Approved)
IPC	NATO	NATO Standard Bar Code Symbology Printing and Applying Bar Code Labels (R) Recommended Practice for Bar-Coded Vehicle Emission Configuration Label, Recommended Practice; October 1993	STANAG 4329 1992	Informational (Approved)
NPC	ANSI	Bar Code Print Quality-Guideline	X3.182-1990	Informational (Approved)
NPC	AIM	Uniform Symbology Specification (USS)-I-2/5 (Interleaved 2 of 5)	X5-1:1993	Informational (Approved)
NPC	AIM	Uniform Symbology Specification (USS)-39 Code 39	X5-2:1993	Informational (Approved)

3.5.2.2.2 Alternative specifications. The only other available specifications are proprietary.

3.5.2.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.2.2.4 Portability caveats. Various bar code standards were developed by one industry organization and adopted by other industry organizations who modified them slightly for specific application areas or market segments. This has led to many different specifications that have incompatibilities.

3.5.2.2.5 Related standards. The following standards are related to bar coding or bar coding standards:

a. ISO 9735:1988-1992, Electronic Data Interchange for Administration, Commerce, and Transport (EDIFACT)

b. ANSI X.12-1986, Parts 1-22: Electronic Data Interchange (EDI)

c. ITU-T Recommendation X.435, and F.435

3.5.2.2.6 Recommendations. The recommended bar coding standard varies with the market sector and the amount of information to be squeezed into the code. For example, Codabar is used extensively in retail price-labeling. Intermec Corp.'s Code 49 is a stacked code of bars and spaces in horizontal rows. One information-squeezing code is Symbol Technologies Inc.'s PDF 417 which is a matrix-style code that compresses up to 1,750 characters per symbol. For code 39 bar coding, MIL-STD-1189B is recommended.

3.5.2.3 Physical interface. Physical interface standards deal with physical I/O connections and storage systems.

3.5.2.3.1 Standards. Table 3.5-20 presents standards for physical interface.

TABLE 3.5-20 Physical interface standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Interface between DTE and DCE for Operations with PSDN, or between Two DTEs by Dedicated Circuit (adopts ANSI X3.100-1989)	FIPS PUB 100-1:1991	Adopted (Approved)
GPC	NIST	4800 and 9600 Bits per Second Two-Wire Duplex Modems for Data Communications Use on Telephone-Type Circuits (adopts CCITT V.32, Supersedes FIPS 134-1)	FIPS PUB 166:1992	Adopted (Approved)
GPC	NIST	9600 bps Four-Wire Duplex Modems for Data Communications Use on Telephone-Type Circuits (adopts CCITT V.29, Supersedes FIPS 135)	FIPS PUB 167:1992	Adopted (Approved)
GPC	NIST	12000 and 14400 bps Four-Wire Duplex Modems for Data Communications Use on Telephone-Type Circuits	FIPS PUB 168:1992	Adopted (Approved)
GPC	NIST	Error Correction in Modems Employing Asynchronous-to-Synchronous Conversion	FIPS PUB 169:1992	Adopted (Approved)
GPC	NIST	Data Compression in Modems Employing CCITT Recommendation V.42 Error Correction	FIPS PUB 170:1992	Adopted (Approved)
GPC	NIST	Synchronous Signaling Rates Between Data Terminal and Data Communication Equipment (adopts ANSI X3.1-1976)	FIPS PUB 22-1:1977	Adopted (Approved)
CPC	PCMCIA	Personal Computer Memory Card Industry Association (PCMCIA) PC Card Standard	PCMCIA Release 2.1 July 1993	Adopted (Approved)
IPC	ITU-T	Facsimile Modem Speed Reductions and Transaction Time - Telephone Network and ISDN - Quality of Service, Network Management and Traffic Engineering	E.452 (1993)	Informational (Approved)
NPC	ANSI/IEEE	Standard Multivalue Logic System for VHDL Model Interoperability	1164:1993	Informational (Approved)
GPC	NIST	2400 Bits per Second Two-Wire Duplex Modems for Data Communications Use on Telephone-Type Circuits (Supersedes FIPS 133/Fed-Std-1005A)	FIPS PUB 163:1992	Informational (Approved)
GPC	NIST	1200 bps 2-Wire Duplex Modems for Data Communications use on Telephone-Type Circuits (adopts CCITT V.22, Supersedes FIPS 136)	FIPS PUB 162:1992	Informational (Approved)
GPC	NIST	2400 Bits per Second Four-Wire Duplex and Two-Wire Half-Duplex Modems for Data Communications Use on Telephone-Type Circuits (adopts CCITT V.22 bis)	FIPS PUB 164:1992	Informational (Approved)
GPC	NIST	4800 Bits per Second Four-Wire Duplex and Two-Wire Half-Duplex Modems for Data Communications Use on Telephone-Type Circuits (Supersedes FIPS 134-1)	FIPS PUB 165:1992	Informational (Approved)
IPC	ITU-T	Telegraph Modem for Subscriber Lines - Telegraph Transmission	R.20 (1989)	Informational (Approved)
IPC	ITU-T	2-Wire Modem for Facsimile Applications with Rates up to 14 400 bit/s	V.17 (1991)	Informational (Approved)
IPC	ITU-T	300 Bits per Second Duplex Modem Standardized for Use in the General Switched Telephone Network - Data Communication over the Telephone Network	V.21 (1989)	Informational (Approved)
IPC	ITU-T	1200 Bits per Second Duplex Modem Standardized for Use in the General Switched Telephone Network and on Point-to-Point 2-Wire Leased Telephone-Type Circuits - Data Communication Over the Telephone Network	V.22 (1989)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ITU-T	2400 Bits per Second Duplex Modem Using the Frequency Division Technique Standardized for Use on the General Switched Telephone Network and on Point-to-Point 2-Wire Leased Telephone-Type Circuits - Data Communication Over the Telephone Network	V.22 BIS (1989)	Informational (Approved)
IPC	ITU-T	600/1200-Baud Modem Standardized for Use in the General Switched Telephone Network - Data Communication over the Telephone Network	V.23 (1989)	Informational (Approved)
IPC	ITU-T	2400 Bits per Second Modem Standardized for Use on 4-Wire Leased Telephone-Type Circuits - Data Communication over the Telephone Network	V.26 (1989)	Informational (Approved)
IPC	ITU-T	2400/1200 Bits per Second Modem Standardized for Use in the General Switched Telephone Network - Data Communication over the Telephone Network	V.26 BIS (1989)	Informational (Approved)
IPC	ITU-T	2400 Bits per Second Duplex Modem Using the Echo Cancellation Technique Standardized for Use on the General Switched Telephone Network and on Point-to-Point 2-Wire Leased Telephone-Type Circuits - Data Communication over the Telephone Network	V.26 TER (1989)	Informational (Approved)
IPC	ITU-T	4800 Bits per Second Modem with Manual Equalizer Standardized for Use on Leased Telephone-Type Circuits - Data Communication over the Telephone	V.27 (1989)	Informational (Approved)
IPC	ITU-T	4800/2400 Bits per Second Modem with Automatic Equalizer Standardized for Use on Leased Telephone-Type Circuits - Data Communication over the Telephone Network	V.27 BIS (1989)	Informational (Approved)
IPC	ITU-T	4800/2400 Bits per Second Modem Standardized for Use in the General Switched Telephone Network - Data Communication over the Telephone Network	V.27 TER (1989)	Informational (Approved)
IPC	ITU-T	9600 Bits per Second Modem Standardized for Use on Point-to-Point 4-Wire Leased Telephone - Type Circuits - Data Communication over the Telephone Network	V.29 (1989)	Informational (Approved)
IPC	ITU-T	Duplex Modem Operating at Data Signaling Rates of up to 14400 bps for Use on the General Switched Telephone Network and on Leased Point-to-Point 2-Wire Telephone-Type Circuits	V.32 BIS (1991)	Informational (Approved)
IPC	ITU-T	14400 Bits per Second Modem Standardized for Use on Point-to-Point 4-Wire Leased Telephone - Type Circuits - Data Communication over the Telephone Network	V.33 (1989)	Informational (Approved)
IPC	ITU-T	Error-Correcting Procedures for DCEs Using Asynchronous-to-Synchronous Conversion - Data Communication over the Telephone Network	V.42 (1989)	Informational (Approved)
IPC	ITU-T	Data Compression Procedures for Data Circuit Terminating Equipment (DCE) Using Error Correction Procedures	V.42 BIS (1990)	Informational (Approved)
IPC	ITU-T	Duplex Modem Operating at Data Signaling Rates of up to 14400 bps for Use on the General Switched Telephone Network and on Leased Point-to-Point 2-Wire Telephone-Type Circuits	V.32 (1993)	Informational (Approved)
IPC	ITU-T	Error-Correcting Procedures for DCEs Using Asynchronous-to-Synchronous Conversion	V.42, Rev. 1 (1993)	Informational (Approved)
IPC	NATO	Supreme High Frequency (SHF) Military Satellite (MILSATCOM) Jam-Resistant Modem	STANAG 4376	Informational (Draft)

3.5.2.3.2 Alternative specifications. No alternative specifications are applicable.

3.5.2.3.3 Standards deficiencies. Deficiencies in the existing standards are not known.

3.5.2.3.4 Portability caveats. Portability problems with the existing standards are not known.

3.5.2.3.5 Related standards. Magnetic tape storage standards are related to physical interface standards.

3.5.2.3.6 Recommendations. For their individual areas of applicability, the adopted FIPS for physical interface are recommended. DOD policy requires all personal computers to include at least one PC Card (formerly Personal Computer Memory Card Industries Association (PCMCIA)) slot to allow the use of security devices.

3.5.3 Optical digital technologies. Optical Digital Technology (ODT) represents technologies that use the reflective properties of light and an optical recording surface to capture, encode, decode, and store data. ODT predominantly encompasses optical media, optical drives, and scanners.

3.5.3.1 Optical digital technology. This optical digital technology base service area concentrates on optical scanning and image quality, excluding optical character recognition.

3.5.3.1.1 Standards. Table 3.5-21 presents standards for optical digital technology.

TABLE 3.5-21 Optical digital technology standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI/AIIM	Recommended Practice for Quality Control of Image Scanners	MS44-1988 (R1993)	Adopted (Approved)
NPC	ANSI/AIIM	Recommended Practice for Monitoring Image Quality of Roll Microfilm and Microfiche Scanners	MS49-1993	Adopted (Approved)
NPC	ANSI/AIIM	Recommended Practice for Monitoring Image Quality of Aperture Card Film Image Scanners with Scanner Test Target Set	MS50-1994	Adopted (Approved)
NPC	ANSI/AIIM	Recommended Practice for the Requirements and Characteristics of Original Documents Intended for Optical Scanning	MS52-1991	Adopted (Approved)
GPC	NIST	Guideline for Quality Control of Image Scanners, IEEE Std 167A-1987	FIPS PUB 157:1989	Adopted (Approved)
NPC	IEEE	IEEE Standard Facsimile Test Chart	167A:1987	Adopted (Approved)
NPC	ANSI/AIIM	Application Programming Interface (API) for Scanners in Document Imaging Systems	MS61	Informational (Draft)

MS44 is used with the IEEE Scanner Test Chart, IEEE 167A.
FIPS 157 adopts MS44.
IEEE 167A is also known as AIIM Scanner Test Chart #2.

3.5.3.1.2 Alternative specifications. No alternative specifications are known.

3.5.3.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.3.1.4 Portability caveats. Portability problems of the existing standards are unknown.

3.5.3.1.5 Related standards. The following standards are related to optical digital technology:

a. ISO/IEC 9316:1995 - Information Technology - Small Computer Systems Interface 2

b. American National Standards Institute (ANSI) X3.131-1994: Small Computer System Interface-2 (SCSI-2)

c. NIST FIPS 131, Change Notice 2: 1990 - Information Systems - Small Computer System Interface-2 (ANSI X3.131-1986), 1987

d. ISO/IEC 12087 Information Technology -- Computer graphics and image processing -- Image Processing and Interchange (IPI) -- Functional Specification -- Part 1:1995: Common Architecture for Imaging; Part 2:1994: Programmer's imaging kernel system application programming interface; Part 3:1995: Image Interchange Facility (IIF)

e. ISO/IEC 13346:1995, Information Technology - Volume and File Structure of Write-Once and Rewritable Media Using Non-Sequential Recording for Information Interchange, Part 1: General, Part 2: Volume and Boot Block Recognition, Part 3: Volume Structure, Part 4: File Structure, Part 5: Record Structure. (ECMA 167-1992)

f. ISO/IEC DIS 12089:1994, Information Technology -- Computer graphics and image processing -- Encoding for the Image Processing and Interchange Standard (IPI) -- Encoding for the IIF

g. ANSI/Association for Information and Image Management (AIIM) MS53-1993: Standard Recommended Practice - File Format for Storage and Exchange of Images - Bi-Level Image File Format: Part 1. (NIST FIPS PUB 194:1995, MIL-STD-188-196)

h. ISO/ANSI 9318-3:1990, Information Technology - Intelligent Peripheral Interface - Part 3: Device Generic Command Set for Magnetic and Optical Disk Drives (Revision and Redesignation of X3.132:1987)

i. ANSI X3.201-1992, Information Systems - Intelligent Peripheral Interface - Enhanced Physical Level

j. MIL-STD-1189A: Standard Department of Defense Bar Code Symbology, 1989

k. ISO/IEC 10646-1:1993 (Amendments 1-5), Information Technology - Universal Multiple Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Place. Standard adopted by The Frankfurt Group to enhance the Orange Book Compact Disc specifications. ISO/IEC 10646 is a standard for using the many character sets of the world

l. ANSI/National Information Standards Organization (NISO) Z39.2-1994: Information Interchange Format

m. ANSI/NISO Z39.18-1995, Scientific and Technical Reports - Elements, Organization, and Design

n. ANSI/NISO Z39.50-1995: Information Retrieval Application Service Definition and Protocol Specification for Open Systems Interconnection

o. ANSI/NISO Z39.58-1992: Common Command Language for Online Interactive Information Retrieval

p. AIIM TR2-1992, Glossary of Imaging Technology

q. ANSI/AIIM TR15, Planning Considerations, Including Preparation of Documents for Image Capture Systems

r. ANSI/AIIM MS59-1996, Media Error Monitoring and Reporting Techniques for Verification of the Stored Data on Optical Digital Data Disks.

s. ANSI/AIIM TR41-Proposed, Technical Report on Optical Storage Standards.

3.5.3.1.6 Recommendations. Evaluate and select the adopted standards appropriate for the organization's application.

3.5.3.2 Optical character recognition. Optical character recognition (OCR) standards define optically scanning a document to identify the text it contains and convert it from bitmaps to characters.

3.5.3.2.1 Standards. Table 3.5-22 presents standards for optical character recognition.

TABLE 3.5-22 Optical character recognition standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Character Sets for Optical Character Recognition (OCR) (adopts ANSI X3.2-1970/R1976, X3.17-1981/R1989, . X3.49-1975/R1982, 1989)	FIPS PUB 32-1:1982	Informational (Approved)
GPC	NIST	Character Set for Handprinting (adopts ANSI X3.45-1982	FIPS PUB 33-1:1984	Informational (Approved)
GPC	NIST	Guideline for Optical Character Recognition Forms	FIPS PUB 40:1976	Informational (Approved)
GPC	NIST	Optical Character Recognition (OCR) Inks (adopts ANSI X3.86-1980)	FIPS PUB 85:1980	Informational (Approved)
GPC	NIST	Optical Character Recognition (OCR) Character Positioning (adopts ANSI X3.93M-1981)	FIPS PUB 89:1981	Informational (Approved)
GPC	NIST	Guideline for Optical Character Recognition Print Quality (adopts ANSI X3.99-1983)	FIPS PUB 90:1983	Informational (Approved)
GPC	NIST	Optical Character Recognition (OCR) - Dot Matrix Character Sets for OCR-MA (adopts ANSI X3.111-1986)	FIPS PUB 129:1987	Informational (Approved)
IPC	ISO	Alphanumeric Character Sets for Optical Recognition - Part 1: Character Set OCR-A - Shapes and Dimensions of the Printed Image; (Amendment Slip-1978)	1073-1:1976	Informational (Approved)
IPC	ISO	Alphanumeric Character Sets for Optical Recognition, Part II: Character Set OCR-B-Shapes and Dimensions of the Printed Image (Amended 1978)	1073-2:1976	Informational (Approved)
IPC	ISO	Coding Machine Readable Characters (MICR and OCR)	2033:1983	Informational (Approved)
NPC	ANSI	Character Set for Optical Character Recognition (OCR-A)	X3. 17-1981 (R1989)	Informational (Approved)
NPC	ANSI	Character Set for Optical Character Recognition (OCR-B)	X3. 49-1975 (R1989)	Informational (Approved)
NPC	ANSI	Optical Character Recognition (OCR) Inks	X3. 86-1980 (R1993)	Informational (Approved)
NPC	ANSI	Optical Character Recognition (OCR) Character Positioning	X3. 93M-1981 (R1989)	Informational (Approved)
NPC	ANSI	Optical Character Recognition (OCR) - Guidelines for OCR Print Quality	X3. 99-1983 (R1991)	Informational (Approved)
NPC	ANSI	Optical Character Recognition (OCR) - Matrix Character Sets for OCR-MA	X3.111-1986 (R1992)	Informational (Approved)
NPC	ANSI	Optical Character Recognition (OCR) - Matrix Character Sets for OCR-MB	X3.209	Informational (Approved)
IPC	ECMA	Alphanumeric Character Set OCR-B for Optical Recognition	11 (1976)	Informational (Approved)
IPC	ECMA	Nominal Character Dimensions of the Numeric OCR-A Font	8 (1977)	Informational (Canceled)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ECMA	Character Positioning on OCR Journal Tape	21 (1969)	Informational (Canceled)
IPC	ECMA	OCR-B Subsets for Numeric Applications	30 (1976)	Informational (Canceled)
IPC	ECMA	Implementation of the Numeric OCR-A Font with 9 X 9 Matrix Printers	51 (1977)	Informational (Canceled)

3.5.3.2.2 Alternative specifications. No other specifications are available.

3.5.3.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.3.2.4 Portability caveats. Portability problems are unknown at this time.

3.5.3.2.5 Related standards. ODT is most beneficial in application of mass storage which is usually necessary with scanned documents. Raster data interchange standards, imaging standards, and compression standards are related to ODT.

3.5.3.2.6 Recommendations. The FIPS for OCR are preferred.

3.5.4 Office automation document interchange. The following base service areas deal with data formatting and exchange standards for different types of documents in an office automation environment.

3.5.4.1 Document interchange. (This BSA appears in part 5, Data Interchange, and part 12, Multimedia.) Document interchange standards allow the transfer of formatted documents across a network so they can be reproduced exactly and worked on at their destinations.

3.5.4.1.1 Standards. Table 3.5-23 presents standards for document interchange.

TABLE 3.5-23 Document interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Standard Generalized Markup Language (SGML) (Amendment 1 - 1988) (Adopted by FIPS PUB 152:1989)	8879:1986	Mandated (Approved)
CPC	IETF	HyperText Markup Language (HTML) v.2.0	RFC 1866:1995	Mandated (Approved)
GPC	DOD	Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of text (based on ISO 8879)	MIL-PRF-28001	Informational (Approved)
IPC	ISO/IEC	Distributed Office Applications Model (DOAM), Part 1: General Model	10031-1:1991	Informational (Approved)
IPC	ISO/IEC	Distributed Office Applications Model (DOAM), Part 2: Distinguished Object Reference and Associated Procedures	10031-2:1991	Informational (Approved)
IPC	ISO/IEC	Document Filing and Retrieval (DFR), Part 1: Abstract Service Definition and Procedures (corrigendum 1-1994, corrigendum 2- 1994, corrigendum 3-1994)	10166-1:1991	Informational (Approved)
IPC	ISO/IEC	Document Filing and Retrieval (DFR), Part 2: Protocol Specification (corrigendum 1-1994)	10166-2:1991	Informational (Approved)
IPC	ISO	Text and Office Systems - Referenced Data Transfer - Part 1: Abstract Service Definition	10740-1	Informational (Approved)
IPC	ISO	Text and Office Systems - Referenced Data Transfer - Part 2: Protocol Specification	10740-2	Informational (Approved)
IPC	ITU-T	Document Transfer and Manipulation (DTAM) - Services and Protocols- Introduction and General Principles	T.431 (1992)	Informational (Approved)
IPC	ITU-T	Document Transfer and Manipulation (DTAM) - Service Definition	T.432 (1993)	Informational (Approved)
IPC	ITU-T	Document Transfer and Manipulation (DTAM) - Protocol Specification	T.433 (1993)	Informational (Approved)
IPC	ITU-T	Document Transfer and Manipulation (DTAM) - Operational Structure	T.441 (1989)	Informational (Approved)
NPC	ANSI	Text Information Interchange in Page Image Format (PIF)	X3. 98-1983	Informational (Approved)
IPC	ISO	Standard Generalized Markup Language (SGML) Document Interchange Format Support Facilities (SDIF)	9069:1988	Informational (Approved)
IPC	ISO/IEC	Documentation Style Semantics and Specification Language (DSSSL)	10179:1995	Informational (Approved)
CPN-C	AT&T	TROFF - Markup Language	Unix BSD 4.3	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPN-C	Microsoft	Rich Text Format (RTF)	RTF Tech. Manuals	Informational (Approved)
CPN-C	Adobe	PostScript Type I - Outlines	PS Tech. Manuals	Informational (Approved)
CPN-C	Adobe	Portable Document Format (PDF)	PDF	Informational (Approved)
CPC	IETF	HyperText Markup Language (HTML)	HTML v.3.2	Emerging (Draft)
GPC	DOD	Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of text (based on ISO 8879)	MIL-M-28001B of 6/26/1993	Informational (Superseded (CALS))

3.5.4.1.2 Alternative specifications. The following specifications are also available:

a. ANSI/NISO Z39.59-1988 (to represent the logical structure of books and articles)

b. The Association of American Publishers (AAP), the Text Encoding Initiative (TEI), and the DOD Continuous Acquisition and Life Cycle Support (CALS) program have designed alternate nonproprietary architectures with SGML encodings

c. Microsoft's Dynamic Data Exchange (DDE)

d. Microsoft's Dynamic Link Libraries

e. ANSI/NISO Z39.2-1994: Information Interchange Format

f. ANSI/NISO Z39.18-1995: Scientific and Technical Reports - Elements, Organization, and Design

g. ANSI/NISO Z39.50-1992: Information Retrieval Application Service Definition and Protocol Specification for Open Systems Interconnection

h. ANSI/NISO Z39.59-1992: Common Command Language for Online Interactive Information Retrieval

3.5.4.1.3 Standards deficiencies. There is very little standardization of font names when handling fonts represented by tagged-text data types. However, many systems are attempting font substitution, that is, replacing a specified font with one that is similar, such as substituting TrueType Arial for PostScript Helvetica. Not all tagged text systems are able to specify colored text.

The following are recognized gaps in the Office Document Architecture (ODA)/ Office Document Interchange Format (ODIF) standards:

a. Revision collection, status, rationale, and author information

b. Document annotations

c. Automatic content generation of listings such as table of contents, lists of figures, indexes, glossaries, and cross-references

d. Business charting, including the ability to derive business graphics from tabular, spreadsheet, or other data in the document or referenced by the document; the ability to derive part of a document from external business graphics, and the ability to include a business graphic in a document in such a way that the processing specific to business graphics can be performed by the recipient of a document

e. Data in documents, such as spreadsheets

f. Exchange of documents based on hypertext

g. Exchange of documents that include voice and audio information (Hyper ODA)

3.5.4.1.4 Portability caveats. At present, portability using ODA/ODIF is limited, because it is not in widespread use or widely available, although SGML is widely available.

3.5.4.1.5 Related standards. The following standards are related to document exchange:

a. ISO 8824:1987 and ISO 8825:1987 - ASN.1/BER

b. SGML for documents that are not predefined

c. TeX by Donald Knuth of MIT and LaTeX macros are widely used for typesetting, especially for documents that include mathematics

3.5.4.1.6 Recommendations. In keeping with the ongoing shift from literal page appearance to electronic transfer of document content (as exemplified by the electronic commerce and CALS programs) we recommend the use of SGML for document interchange. 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. On March 25-26, 1993, the Defense Information Systems Agency (DISA) convened a Document Interchange Symposium. The symposium featured a panel of ODA and SGML experts to deliberate on SGML/ODA issues. The panel reached the following conclusions:

a. SGML has been adopted by a wide range of government and private industry initiatives for document interchange.

b. Few commercially viable ODA products are found in the U.S. marketplace.

c. Distinctions between office and publishing documents are diminishing (making the need for unique office document architectures less acute).

d. SGML has been adopted by the publishing community.

In addition to the panel's conclusions, it should be noted that NIST has decided not to develop a FIPS for ODA. The DOD SGML standard (MIL-PRF-28001) is based on ISO 8879. MIL-HDBK-28001 for SGML is being developed.

For documents intended for distribution on the Internet, particularly the World Wide Web, HTML should be used. HTML is a document type definition (DTD) of SGML for Internet documents.

Adobe PDF is being used frequently in DOD for formatting documents. Revisions are not required. However, PDF suffers by the fact that it has not yet been endorsed by an open consensus standards body. Efforts need to be taken to move PDF from the de facto, proprietary, realm to be an open standard.

3.5.4.2 Spreadsheet data interchange. Spreadsheet data interchange is the exchange of tabular alphanumeric data (i.e., data found in spreadsheets).

3.5.4.2.1 Standards. Table 3.5-24 presents standards for spreadsheet data interchange.

TABLE 3.5-24 Spreadsheet data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Open Document Architecture (ODA) and Interchange Format: Tabular Structures and Tabular Layout	8613-11:1996	Informational (Approved)

3.5.4.2.2 Alternative specifications. The follow de facto specifications are also available:

a. SoftArts, Data Interchange Format (DIF) for exchanging data between tables
b. Microsoft, XLS spreadsheet format
c. Lotus Development, WK4, WK3, WK1, and WKS spreadsheet formats

3.5.4.2.3 Standards deficiencies. The de facto DIF and the WK3, WK1, and WKS formats mostly allow the contents of spreadsheet cells to be imported into a document, separated by tabs. Most major spreadsheet products allow the import and export of XLS and WKx data values and common formulas. Unless the vendor of a document creation product has made a specific custom interface to the spreadsheet package whose data is to be imported, all lines, shading, graphics, and many other spreadsheet features are lost. No standards, de facto or otherwise, exist for arranging, interpreting, or otherwise processing the spreadsheet after it has been imported into a new document.

3.5.4.2.4 Portability caveats. The de facto DIF standard and WK3, WK1, and WKS formats provide limited portability and interoperability. Although they allow a spreadsheet's cell contents to be interchanged and imported into another spreadsheet separated by tabs, depending on the packages or the cell contents, the data may be interchanged as a stream of numbers or strings, without clear beginnings or endings.

3.5.4.2.5 Related standards. The following standards are related to spreadsheet data exchange or spreadsheet data exchange standards:

a. ISO 8613: ODA/ODIF.
b. ISO 8879: SGML.

3.5.4.2.6 Recommendations. If a particular agency has many existing spreadsheet packages, the quest for portability, interoperability, and data interchange will make it advisable to require an open interface to access each of these existing systems, rather than having a common format such as "DIF."

3.5.4.3 Custom definition of document types. These standards provide the ability to custom-define a document type when predefined document types are not applicable.

3.5.4.3.1 Standards. Table 3.5-25 presents standards for custom definition of document types.

TABLE 3.5-25 Custom definition of document types standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Standard Generalized Markup Language (SGML) (Amendment 1 - 1988) (Adopted by FIPS PUB 152:1989)	8879:1986	Mandated (Approved)
IPC	ISO	Standard Generalized Markup Language (SGML) Document Interchange Format Support Facilities (SDIF)	9069:1988	Informational (Approved)
IPC	ISO/IEC	Standard Generalized Markup Language (SGML) Support Facilities: Registration Procedures for Public Text Owner Identifiers	9070:1991	Informational (Approved)
IPC	ISO	SGML Support Facilities - Techniques for Using SGML	TR 9573:1988	Informational (Approved)
IPC	ISO/IEC	SGML Support Facilities - Techniques for Using SGML - Part 13: Public Entity Sets for Mathematics and Science (Replaces ISO 8879 Annex D (in part))	TR 9573-13:1991	Informational (Approved)
IPC	ISO/IEC	SGML and Text-Entry Systems - Guidelines for SGML Syntax-Directed Editing Systems	TR 10037:1991	Informational (Approved)
IPC	ISO/IEC	Hypermedia/Time-Based Structuring Language (HyTime)	10744:1992	Informational (Approved)
NPC	ANSI/NISO	Electronic Manuscript Preparation and Markup	Z39.59:1988	Informational (Approved)
NPC	ANSI	Conformance Testing for Standard Generalized Markup Language (SGML) Systems	X3.190-1992	Informational (Approved)
GPC	DOD	Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of text (based on ISO 8879)	MIL-PRF-28001	Informational (Approved)
IPC	ISO/IEC	Documentation Style Semantics and Specification Language (DSSSL)	10179:1995	Informational (Approved)
GPC	DOD	Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of text (based on ISO 8879)	MIL-M-28001B of 6/26/1993	Informational (Superseded (CALS))
IPC	ISO/IEC	Text and Office Systems - Conformance Testing for Standard Generalized Markup Language (SGML) Systems	13673:1993	Informational (Draft)

3.5.4.3.2 Alternative specifications. The following specifications are also available:

a. ISO 8824:1987: ASN.1

b. The AAP, the TEI, and the DOD CALS program have designed alternate, nonproprietary architectures with SGML encodings.

3.5.4.3.3 Standards deficiencies. SGML does not deal with the meaning of the markup, so additional standards are needed. Markup consists of the common sets of document formatting codes used in classes of document types.

Technical manuals may use a different markup from management guideline documents to accommodate the audience, content, and publishing layout styles commonly used for each document type. Since SGML does not deal with the markup's meaning, it does not specify what to do after the document has been processed by a program that recognizes SGML.

SGML does not deal with hypermedia/time-based document interchange, although standards in that area are being developed.

SGML does not use object-oriented methods, although such work is underway in the Multimedia/Hypermedia Experts Group (MHEG).

3.5.4.3.4 Portability caveats. A lot of disagreement still exists on the particular markup to be employed in document types. This can result in incompatible and misinterpreted markups.

Use SGML in conjunction with selected, stable, draft specifications from the MHEG to handle multimedia objects, as well as other objects.

3.5.4.3.5 Related standards. The following standards are related to custom definition of document types and definition standards:

a. ISO 8613: ODA/ODIF Parts 1-10 and amendments and addenda. ODA Part 5 specifies a method of representation and interchange using the Office Document Language and SDIF. ODL may be used to represent a document structure in accordance with ODA in SGML.

b. ISO DIS 10180: SPDL

c. ISO DIS 10179: DSSSL, an application of SGML; includes a document architecture for typographic presentation style.

d. ISO 10744/ANSI X3V1.8M (Project 749-D): Hypermedia/Time-based Structuring Language (HyTime). HyTime, a notation to describe hypermedia, is an extension of SGML to deal with hypermedia/time-based document interchange.

e. ISO 10031:1990: Distributed Office Applications Model (DOAM), Parts 1-2. ISO 10031 provides guidelines for defining Distributed Office Application objects, such as documents, object attributes, and abstract operations, for use in a client-server environment.

f. MIL-STD-1840B (11/3/1992): Automated Interchange of Technical Information (Life cycle logistics support for weapon systems)

3.5.4.3.6 Recommendations. The following two ISO technical reports include supportive SGML tips and guidelines. Their use in learning about SGML and to achieve portability is valuable.

Use specifications, such as Electronic Manuscript Preparation and Markup (EMPM) or ODA, to determine the markup's meaning in order to decide what to do after the document has been processed by a program that recognizes SGML.

a. ISO Technical Report (TR) 9573: SGML Support Facilities: Techniques for Using SGML

b. ISO TR 10037: SGML and Text-Entry Systems-Guidelines for SGML Syntax-Directed Editing Systems

SGML contains multiple languages and applications, each of which must be specified explicitly in a procurement.

SGML has several advantages. It is used by CALS, more commercial products are available for it than for ODA/ODIF/ODL, it is human-readable, preserves user file divisions, and is extensible to other architectures. Moreover, it transcends ordinary office documents and supports graphics and multimedia now.

However, CALS uses the more restrictive SGML standard (MIL-PRF-28001), minimizes markup, and uses fewer SGML features to provide a "DOD profile" of SGML. MIL-HDBK-28001 for SGML is being developed to aid users of the standard.

3.5.4.4 Bibliographic system text retrieval. Bibliographic system text retrieval standards specify the representation of the logical structure of books, articles, and serial publications and a common command language for managing bibliographic systems.

3.5.4.4.1 Standards. Table 3.5-26 presents standards for bibliographic system text retrieval.

TABLE 3.5-26 Bibliographic system text retrieval standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI/NISO	Information Retrieval Service Definition and Protocol Specification for Open Systems Interconnection	Z39.50:1995	Informational (Approved)
NPC	ANSI/NISO	Common Command Language for On-Line Interactive Information Retrieval	Z39.58:1992	Informational (Approved)
IPC	ISO/IEC	OSI Search and Retrieve Application Service Definition	10162:1993	Informational (Approved)
IPC	ISO/IEC	OSI Search and Retrieve Application Protocol Specification Part 1: Protocol Specification	10163-1:1993	Informational (Approved)
IPC	ISO	Commands for Interactive Text Searching	8777:1993	Informational (Approved)
GPC	Commerce	CD-RDx (A query standard for computer-based retrieval of CD-ROM publication)	CD-RDx	Informational (TBD)
NPC	ANSI	Structured File Query Language (SFQL) (A query language, based on SQL, with extensions to support full text, and using SGML Document Type Definitions to define metainformation about a table or document)	X3H2-Designated number to be assigned	Informational (Draft)
CPC	ATA	Structured File Query Language (SFQL) (A query language, based on SQL, with extensions to support full text, and using SGML Document Type Definitions to define metainformation about a table or document)	SFQL	Informational (Formative)

3.5.4.4.2 Alternative specifications. The following specifications are also available:

a. Thinking Machines, Inc.'s, Wide-Area Information Server (WAIS), a protocol for transmitting query and retrieval information, which has been adopted by a number of major vendors and runs on a wide variety of platforms and networks. (NOTE: WAIS is an extension to the Z39.50 standard to allow discrete portions of documents to be retrieved. WAIS is currently running in about 80 sites.)

b. Information Dimensions Inc.'s OpenAPI, a callable API, which is a low level toolkit interface for developers to use in building Graphical User Interface (GUI)-based text retrieval applications that run on MS Windows, MAC, VMS, and UNIX desktops and connect to servers, over a variety of transports.

3.5.4.4.3 Standards deficiencies. The CD-RDx is considered by many in the government to be less robust and reliable than the Structured File Query Language (SFQL), which is more accepted and will become an IEEE standard.

3.5.4.4.4 Portability caveats. The standards developed by NISO are in widespread use in libraries and bibliographic systems, but are not compatible with the more widely accepted DFR and DTAM standards in the general office and document world.

3.5.4.4.5 Related standards. The following standards are related to bibliographic system text retrieval or retrieval standards:

a. ISO 10166: Document File and Retrieval (DFR)

b. ITU-T T.431, T.432, T.433, and T.441: Document Transfer and Manipulation (DTAM)

3.5.4.4.6 Recommendations. The ISO text/data retrieval protocol is recommended for OSI applications. For library applications in client-server environments ANSI/NISO Z39.50-1988 is recommended in conjunction with the command language in ANSI/NISO Z39.58-1992.

3.5.4.5 Electronic forms. (This BSA appears in part 3, User Interface, part 4, Data Management, and part 5, Data Interchange.) These standards specify the functional interface requirements, transfer of various fields and the interface between programming languages and form filling applications for use on a terminal display.

3.5.4.5.1 Standards. Table 3.5-27 presents standards for electronic forms.

TABLE 3.5-27 Electronic forms standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	DOD Standardized Electronic Forms Requirements	JIEO-E-2300	Adopted (Approved)
IPC	ISO/IEC	Forms Interface Management System (FIMS)	11730:1994	Informational (Approved)
GPC	NIST	Government Open System Interconnection Profile (GOSIP 2): Virtual Terminal Forms Class Profile	FIPS PUB 146-1:1991	Informational (Approved)
CPC	X/Open	Single UNIX Specification (Spec. 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C436 (9/94)	Emerging (Approved)
CPC	X/Open	Single Unix Specification: X/Open Curses, Issue 4 (part of XPG4)	C437 (2/95)	Emerging (Approved)
GPC	DOD	DOD Forms Management Program Procedures Manual	DOD 7750.7-M	Informational (Approved)
CPN-C	Numerous vendors	Query by Forms	Query by Forms	Informational (Approved)
IPC	ISO/IEC	OSI Virtual Terminal Basic Class Service, Amendment 2: Additional Functional Units (forms capability)	9040:1990 DAM 2	Informational (Draft)
IPC	ISO/IEC	OSI Virtual Terminal (VT) Basic Class Protocol, Part 1, Amendment 2: Additional Functional Units (Forms Capability)	9041-1:1990 DAM 2	Informational (Draft)
CPC	X/Open	Internationalized Terminal Interfaces (XCURSES), Issue 4	S422 (4/94)	Informational (Superseded)

3.5.4.5.2 Alternative specifications. The Berkeley Software Distribution (BSD) 4.2/4.3 UUNIX Curses are also available.

3.5.4.5.3 Standards deficiencies. The X/Open Portability Guide 4 (XPG4) Curses is based on the System V Interface Definition (SVID) Issue 2 Curses version, which does not include the SVID's forms and menu libraries.

Forms Class Virtual Terminal has bindings in C only.

DOD has developed a specification for electronic forms (Joint Interoperability and Engineering Organization (JIEO)-E-2300). It defines the minimum operational requirements for electronic forms software and mandates an interchange file format based on Forms Interface Management System (FIMS).

3.5.4.5.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.5.4.5.5 Related standards. The Forms Class Virtual Terminal requires the Synchronous mode (S-mode) of operation and specifies simple delivery control. The following standards are related to forms query and management:

a. ISO 9075: SQL
b. ANSI X3.135-1992: SQL2
c. NIST FIPS 127-2: SQL
d. NIST FIPS 193: SQL Environments

3.5.4.5.6 Recommendations. The recommended standard is JIEO-E-2300. For User Interface, FIMS should be considered. For Data Management, make sure the forms management systems are compatible with FIPS 127-2 SQL. Database forms management systems should be integrated with the SQL database language and formats set forth in FIPS PUB 127-2.

3.5.5 Technical data interchange. The technical data interchange mid-level service area includes vector graphics, product data, and electronic commerce standards areas.

3.5.5.1 Product data interchange. These standards establish data formats for interchanging product description data. These data include not only a graphical depiction, but also manufacturing process information such as materials and surface finishing.

3.5.5.1.1 Standards. Table 3.5-28 presents standards for product data interchange.

TABLE 3.5-28 Product data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI/US PRO	Digital Representation for Communication of Product Definition Data (revision and redesignation of ANSI/ASME Y14.26M-1989) (Formerly IGES)	ANSI/US PRO/ IPO 100-1996	Adopted (Approved)
GPC	NIST	Initial Graphics Exchange Specification (IGES) (adopts ASME/ANSI Y14.26M-1989) (IGES ver. 4)	FIPS PUB 177:1992	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 1: Overview and Fundamental Principles (formerly Product Data Exchange Specification (PDES))	10303-1:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 11: The EXPRESS Language Reference Manual (formerly PDES)	10303-11:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 21: Implementation Methods: Clear Text Encoding of the Exchange Structure	10303-21:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 31: Conformance Testing Methodology/Framework: General Concepts	10303-31:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 41: Integrated Generic Resources: Fundamental of Product Description and Support	10303-41:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 42: Integrated Generic Resources: Geometric and Topological Representation	10303-42:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 43: Integrated Generic Resources: Representation Structures	10303-43:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 44: Integrated Generic Resources: Product Structure Configuration	10303-44:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 101: Integrated Application Resources: Draughting	10303-101:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 201: Application Protocol: Explicit Draughting	10303-201:1994	Adopted (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 203: Application Protocol: Configuration Controlled Design	10303-203:1994	Adopted (Approved)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-PRF-28000	Adopted (Approved)
GPC	DOD	Automated Interchange of Technical Information (Life cycle logistic support of weapon systems)	MIL-STD-1840B of 11/3/1992	Adopted (Approved)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-PRF-28002	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI/US PRO	IGES 5.2, Initial Graphics Exchange Specification (Replaces ANSI/ASME Y14.26M-1989)	US PRO/IPO-100 (Nov 1993)	Informational (Approved)
IPC	ISO/IEC	Part Libraries, About 10 Parts in Progress	13584-XX work in TC184/SC04	Informational (Draft)
GPC	NIST	Initial Graphics Exchange Specification (IGES): v. 5.2 OR 6.0	FIPS PUB 177-1 (future)	Informational (Formative)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-D-28000A(1) of 12/14/92	Informational (Superseded)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-R-28002B(1) of 9/20/1993	Informational (Superseded)
NPC	ANSI/ASME	Digital Representation for Communication of Product Definition Data	Y14.26M:1989	Informational (Superseded)

3.5.5.1.2 Alternative specifications. Standard for the Exchange of Product Model Data (STEP) is being developed as an advanced alternative to Initial Graphics Exchange Specifications (IGES).

3.5.5.1.3 Standards deficiencies. IGES does not cover the complete life cycle of manufactured products. It addresses only the specification of products and not the manufacturing process relationships. The DOD/CALS IGES standard is preferred for engineering drawings, electronics, and numerical control. The standard is optional for technical manual illustrations. Version 5.0 of the NISTIR 4412 does not contain B-rep solids. However, B-Rep solids are contained in Version 5.2.

3.5.5.1.4 Portability caveats. STEP is an international standard that has been a core set of Application Protocols that have been implemented. However, interoperability between these Aps cannot alway be assured. The emerging standard is still unstable and liable to be revised at any time, thereby creating incompatibilities that limit portability and interoperability.

3.5.5.1.5 Related standards. The following standards are related to product data exchange or product data exchange standards:

a. ISO 7942: Graphical Kernel System (GKS)

b. ISO 9592: Programmer's Hierarchical Interactive Graphics System (PHIGS)

c. STEP is related to IGES, but was extended to cover the full life cycle of products from requirements and design through production and installation.

d. MIL-HDBK-1300A, NITFS.

e. MIL-STD-2500A, NITF, Version 2.0 for the NITFS.

f. EIAs Special Report CALS: Harmonizing CALS Product Data Description Standards

3.5.5.1.6 Recommendations. ANSI/US PRO/IPO 100-1996 (Formerly IGES) is Year 2000 compliant and is recommended except for cases where STEP provides additional capabilities that are lacking in IGES and are critical to the accomplishment of the system. STEP includes IGES's functionality, but is more comprehensive. Moreover, CALS specifies five classes of IGES files: Technical Illustration (I), Electrical/Electronic (II), Engineering (III), Numerical Control Manufacturing (IV), and 3D Piping (V).

IGES products are implemented widely and are likely to be proposed by vendors whether or not a procurement specifies it. In contrast, STEP products must be specified explicitly. If STEP is specified in a procurement, then it should conform to the requirements in the ISO 10303 STEP.

The DOD/CALS IGES standard is preferred for engineering drawings, electronics drawings, and numerical control. The standard is optional for technical manual illustrations. It defines subsets for technical illustrations, engineering drawings, electrical/electronic applications, and numerical control manufacturing, and includes an application protocol for three dimensional piping information.

The ISO 10303 STEP standard is a set of interrelated standards that define a vocabulary and syntax for the exchange of product data. The scope of ISO 10303 encompasses all aspects of product data that may be collected and exchanged for any product throughout the life cycle. In its current state, ISO 10303 primarily addresses the exchange of material and shape data. ISO 10303 is a standard designed for expansion. As such, a large part of its initial content lays in the conceptual framework from which any topic area of product data may be standardized to exchange data.

Two specific applications to be included in the initial version of STEP concern the exchange of 2-D drafting data and the exchange of configuration controlled 3-D design data.

3.5.5.2 Business data interchange. Business data interchange, also known as EDI, refers to a family of national and international standards that support the intercompany, computer-to-computer exchange of business documents in standard formats. Examples of common business documents exchanged using EDI are invoices, bills of lading, purchase orders, technical drawings, business graphics, compound documents, catalogs, price lists, electronic funds transfer information, and promotional announcements. EDI is gaining prominence for technical data.

3.5.5.2.1 Standards. Table 3.5-29 presents standards for business data interchange.

TABLE 3.5-29 Business data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Electronic Data Interchange (EDI) (adopts families of standards known as ANSI X12 and EDIFACT)	FIPS PUB 161-1:1993	Adopted (Approved)
IPC	ISO	Trade Data Elements Dictionary (TDED)	7372:1986	Informational (Approved)
IPC	ISO	Electronic Data Interchange for Administration, Commerce, & Transport (EDIFACT) Application Level Syntax Rules	9735:1988	Informational (Approved)
NPC	ANSI	Electronic Data Interchange (EDI)-Many Transaction Sets	X12.1-3, 5-10, 12-16, 20, 22-all 1989	Informational (Approved)
IPC	ITU-T	Message Handling Systems: Electronic Data Interchange (EDI) Messaging System (EDI over X.400-1988 with P.edi)	X.435 (1991)	Informational (Approved)
IPC	UN Econ. Comm. For Europe	United Nations Trade Data Interchange Directory (UNTDID)	TBD-United Nations Trade Data Interchange Directory (UNTDID)	Informational (Approved)
IPC	ISO/IEC	Reconciliation of IEEE 1175 (CDIF) and STEP	JTC1/SC21/WG3	Informational (TBD)
IPC	ISO/IEC	EDIFACT+ (Merged ANSI X.12 & CCITT X.435)	9735 (future)	Informational (Formative)
IPC	ISO/IEC	Proposed EDIFACT/FTAM Document Type	JTC1/SC21, WG5, N6224	Informational (Draft)

3.5.5.2.2 Alternative specifications. The following specifications are also available:

a. EDI II: EDI functionality that surrounds applications, rather than having to be buried within the applications.

b Imaging Technologies that electronically digitize an image of a paper document, such as an invoice or a purchase order, along with subsequent retrieval and document processing capabilities.

3.5.5.2.3 Standards deficiencies. EDI for Administration, Commerce, and Transport (EDIFACT) specifies only an EDI message architecture. X12 specifies transaction sets for several business applications, but does not cover all transaction sets needed by government

agencies. Applicable transaction sets need to be developed. EDIFACT does not currently support the transmission of binary files or technical data. Adoption of a solution is imminent and should be included in version 4 of ISO 9735 in the spring of 1995.

ISO 9735 EDI does not provide security. The 1984 version of X.400 is not adequate for EDI. The 1988 X.400/X.435 version is needed to handle EDI messages. P.edi works only with the 1988 version of X.400. X12 supports the transmission of technical data through transmission set 841.

Up to 85 percent of EDI documents still have to be rekeyed several times by senders and recipients, largely defeating the purpose of EDI, unless users substantially restructure their business processes.

3.5.5.2.4 Portability caveats. The ISO EDIFACT standard is not aligned with ANSI X12, although work is underway to align the two standards. An estimate of when this alignment is likely to take place is difficult to make. EDIFACT and X12 differ in syntax control segments, data segments, and data elements.

3.5.5.2.5 Related standards. The following standards are related to business data interchange or business data interchange standards:

a. ISO 646:1991: 7-Bit Coded Character Set for Information Interchange

b. ISO 8571: FTAM

c. ISO 8632:1987: CGM

d. ISO 8824: ASN.1

e. ISO 8825: BER

f. ISO 8879:1988: SDIF

g. ISO 9069:1988: SGML Support Facilities for SDIF

h. ISO Draft Proposed Standard (DP) 10303: STEP

i. Various ISO standards for coded character sets and graphic characters

j. ITU-T X.400: MHS

k. ITU-T X.435: Messaging protocols used to send EDI messages through an X.400 network

l. ISO/IEC DIS 13208: Electronic data interchange messaging system

m. ISO/IEC DIS 13209: Electronic data interchange messaging service

n. ANSI/ASME Y14.26M-1989: IGES v.4.0

3.5.5.2.6 Recommendations. FIPS PUB 161 recommends the use of X12 standards for domestic applications, and X12 or EDIFACT for international interchanges. Both families of standards may be employed to meet organizational needs.

DOD components that implemented EDI systems after September 30, 1991, are required to conform to FIPS PUB 161. DOD components that implemented EDI systems before September 30, 1991, using industry-specific standards, have until September 30, 1996, to convert to the standards specified in FIPS PUB 161.

Migration to X.435 is recommended as soon as possible, especially for international operations because EDI over X.400 is already in production in Europe.

When specifying EDI services, include compliance CCITT Recommendation X.435 and applicable portions of NIST Special Publication 500-183 (Stable Implementation Agreements).

To maximize portability and interoperability, procurements must specify the ITU-T 1988 X.400 MHS Recommendations or later and avoid the use of products that conform to the 1984 Recommendation. For partially existing systems, FIPS PUB 161 encourages the "interim" use of message handling system implementations built in conformance with the ITU-T 1984 X.400 Recommendation.

3.5.5.3 Computer aided software engineering (CASE) tool data interchange. These standards provide formats for the exchange of data between CASE tools.

3.5.5.3.1 Standards. Table 3.5-30 presents standards for CASE tool data interchange.

TABLE 3.5-30 Computer aided software engineering (CASE) tool data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	Standard Reference Model for Computing System Engineering Tool Interconnections	1175:1992	Informational (Approved)
NPC	IEEE	Trial-Use Standard Reference Model for Computing System Tool Interconnections	TR 1175:1992	Informational (Approved (Trial-Use))
NPC	IEEE	Recommended Practice for the Evaluation and Selection of CASE Tools	1209:1993	Informational (Approved)
NPC	EIA	CASE Data Interchange Format (CDIF), Framework for Modeling and Extensibility; Transfer Format Definition; CASE Interchange Meta-model	IS-81, IS-82, IS-83 of July, '91	Informational (Approved (Interim Std.) (ANSI/EIA Std. Is imminent)
IPC	ISO	Portable Common Tool Environment (PCTE) - Part 2: C Programming Language Binding	13719-2:1995	Informational (Approved)
IPC	ISO	Portable Common Tool Environment (PCTE) - Part 3: Ada Programming Language Binding	13719-3:1995	Informational (Approved)
NPC/IPC	ANSI/ISO	Information Resources Dictionary System 2 (IRDS2) (Repository standard revision will include an interface with CASE tools)	JTC1/21.06.04,5; ANSI X3H4 Project 0754-D (or DT?)	Informational (Formative)

3.5.5.3.2 Alternative specifications. No consortia or de facto specifications are available.

3.5.5.3.3 Standards deficiencies. Deficiencies in the existing standards are unknown. This is a fledgling standardization area, but it is advancing rapidly.

3.5.5.3.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.5.5.3.5 Related standards. The following standards are related to case tool data exchange or exchange standards:

a. ECMA 149 PCTE (Portable Common Tools Environment)

b. ECMA, European regional standards organizations, and the European Defense Community: PCTE+

c. DOD-STD-1838A: Common Ada Programming Support Environment (APSE) Interface Set (CAIS-A)

d. ECMA TR 55 CASE Reference Model

e. ISO Draft International Standardized Profile (DISP) 10609-23:International Standardized Profile TB, TC, TD and TE - Connection-Mode Transport Service over Connection-Mode Network Service - Part 23: Subnetwork-Type Dependent Requirements for Network Layer and Data Link Layer for Data Transfer Concerning a Packet Switched Mode Integrate

f. ISO DISP 10609-24: International Standardized Profile TB, TC, TD and TE - Connection-Mode Transport Service over Connection-Mode Network Service - Part 24: Subnetwork-Type Dependent Requirements for Network Layer and Data Link Layer for Data Transfer Concerning a Packet Switched Mode Integrate

g. ISO DISP 10609-26: International Standardized Profile TB, TC, TD and TE - Connection-Mode Transport Service over Connection-Mode Network Service - Part 26: Subnetwork-Type Dependent Requirements for Network Layer for Call Control Procedures Concerning the Outgoing Call of a Packet Switched Mode

h. ISO DISP 10609-27: International Standardized Profile TB, TC, TD and TE - Connection-Mode Transport Service over Connection-Mode Network Service - Part 27: Subnetwork-Type Dependent Requirements for Network Layer for Call Control Procedures Concerning the Incoming Call of a Packet Switched Mode

3.5.5.3.6 Recommendations. It is recommended that, for those procurements requiring CASE tools and exchange of the associated data, systems migrate to IEEE 1175, CDIF, Product Data Exchange Specification (PDES) or the STEP for CASE tool data exchange.

3.5.5.4 Circuit design data interchange. Circuit data interchange standards provide a format for the interchange of hardware circuit design data.

3.5.5.4.1 Standards. Table 3.5-31 presents standards for circuit design data interchange.

TABLE 3.5-31 Circuit design data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	VHSIC Hardware Description Language (VHDL) (adopts ANSI/IEEE 1076-1987)	FIPS PUB 172:1992	Adopted (Approved)
NPC	IEEE	Standard VHSIC Hardware Description Language (VHDL) Ref Manual Interpretations	1076/INT-91	Informational (Approved)
NPC	ANSI/IEEE	Standard VHSIC Hardware Description Language (VHDL) Reference Manual	1076:1987 (R1993)	Informational (Approved)
NPC	ANSI/IEEE	Standard Multivalue Logic System for VHDL Model Interoperability	1164:1993	Informational (Approved)
NPC	ANSI/EIA	Commercial Component Model Specification	5670000:1991	Informational (Approved)
NPC	EIA	Introduction to Electronic Design Interchange Format (EDIF), Monograph Series Volume 1	EDIF-1 of Sept. 1988	Informational (Approved)
NPC	EIA	Electronic Design Interchange Format (EDIF) Connectivity Monograph Series Volume 2	EDIF-2 of June, 1989	Informational (Approved)
NPC	ANSI/EIA	Electronic Design Interchange Format (EDIF), Version 2n0n0n	548:1988	Informational (Approved (May be superseded))
NPC	EIA	Application Guide Using Electronic Data Interchange Format (EDIF), Ver 2n0n0n for Schematic Transfer	EDIF/AG-1 of July 1989	Informational (Approved (May be superseded))
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-PRF-28000	Informational (Approved)
CPC	CAD Framework Initiative	Procedure Interface (PI) (for circuit connectivity data)	PI	Informational (Approved)
CPN-C	Open Verilog Intl.	Verilog Hardware Description Language (HDL) (IEEE P1364 working on VHDL based Verilog HDL)	Verilog HDL	Informational (Approved)
CPN-C	Vendors	Graphic Design System II (GDSII): CAD Exchange Format	GDSII	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-D-28000A(1) of 12/14/92	Informational (Superseded)
CPC	CAD Framework Initiative	CAD Design Tool Interchange Format (for circuit design) (Planned to be submitted to ANSI)	None assigned yet	Informational (Formative)
NPC	IEEE	Design Management	P1077	Informational (Canceled)
NPC	IEEE	Information Model for Design Language	P1078	Informational (Canceled)
NPC	IEEE	Interface for IEEE VHSIC Hardware Description Language (IEEE Standard 1076-1987) to CAD/CAM Tools	P1163	Informational (Canceled)
NPC	IEEE	Recommended Practice for the Interrelationships between IEEE 1076 and EIA Standard RS-44 EDIF	P1165	Informational (Canceled)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	Standard Delay File Format (SDF)	TBD-Standard Delay File Format (SDF)	Informational (Draft)

3.5.5.4.2 Alternative specifications. The following specifications are also available:

a. Cadence Design Systems' Standard Delay File format (SDF), developed for the Verilog Hardware Design Language (HDL), which has been introduced as the strawman candidate for the Institute of Electrical and Electronics Engineers (IEEE) standard delay file format.

b. Institute for Interconnecting and Packing Electronic Circuits (IPC): IPC-D-350, IPC-D-356.

3.5.5.4.3 Standards deficiencies. VHSIC Hardware Description Language (VHDL) lacks analog design capabilities, high-level predefined types (e.g., queues), and explicit notations for finite state machines. VHDL lacks interfaces with other design and programming languages, such as the Verilog HDL and C. This issue is addressed in the 1992 revision of the standard. VHDL does not support hierarchical path names. This issue is addressed in the 1992 revision of the standard.

No formal standard or industry-accepted standard practice exists for representing timing data (e.g., delay values) in VHDL models and libraries. For VHDL to work effectively with ASIC models, a neutral format for technology-specific data is needed so that data, such as delay information, can be transmitted independent of the simulator. The IEEE has formed a working group to develop a methodology for accomplishing this goal.

3.5.5.4.4 Portability caveats. Specialized synthesis tools based on VHDL are emerging, each requiring a different variation of the input VHDL language. Each tool has its own idiosyncrasies and limitations, some of which stem from these variations.

Although tools based on the Electronic Data Interchange Format (EDIF) are offered by many vendors as a way to import or export design data, the EDIF standard is being supplanted by the Electronic Industries Association's (EIA) CASE Data Interchange Format (CDIF), which is not totally compatible with the original EDIF specifications.

Tools based on VHDL (the formal standard) and tools based on Verilog HDL (the widespread de facto standard) do not interoperate. The use of VHDL and Verilog will require users to maintain incompatible tools for two standards.

3.5.5.4.5 Related standards. The MIT X Consortium's X Window System is related to hardware data exchange.

3.5.5.4.6 Recommendations. National Institute of Standards and Technology (NIST) FIPS 172, VHDL, is recommended. Disregard claims about the level of integration among tools. Focus instead on using VHDL to generate a design at the highest level to gain the benefits of top-down design. Probably, you will have to modify some code for each tool.

In any procurement specifying EDIF, require an upgrade path from EDIF to CDIF. In any procurement specifying the VHDL, specify the full VHDL (e.g., a full VHDL simulator) rather than any subset or superset. This is the only way to be certain that the VHDL will synthesize correctly.

Vendors delivering VHDL most likely will deliver the 1987 version of the standard. This version lacks several important capabilities that are addressed in the standard's revision. Therefore, in any procurement specifying VHDL, require vendors to explain their upgrade paths to the revised VHDL standard.

VHDL synthesis can produce a high productivity level, only if the designers know how to drive it and how to write out VHDL files to get that productivity. Since VHDL is relatively new, in any procurement specifying VHDL, it is advisable to require training from the vendor.

3.5.5.5 Military logistics and document support. These are standards for creating documentation of military systems in support of life cycle logistics support.

3.5.5.5.1 Standards. Table 3.5-32 presents standards for military logistics and document support.

TABLE 3.5-32 Military logistics and document support standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Logistic Support Analysis (LSA) Record	MIL-STD-1388-2B	Adopted (Approved)
GPC	DOD	Automated Interchange of Technical Information (Life cycle logistic support of weapon systems)	MIL-STD-1840B of 11/3/1992	Adopted (Approved)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
GPC	DOD	Manuals, Technical: General Style and Format Requirements	MIL-M-38784C(3) of 12/9/1992	Informational (Approved)
GPC	DOD	Manuals, Interactive Electronic Technical: General Content, Style, Format and User Interaction Requirements	MIL-M-87268 of 11/20/1992	Informational (Approved)
GPC	DOD	Database Revisable:Interactive Electronic Technical Manuals for the Support of	MIL-D-87269 of 11/20/1992	Informational (Approved)
GPC	DOD	Quality Assurance Program Interactive Electronic Technical Manuals (IETM) and Associated Technical Information, Requirements for	MIL-Q-87270 of 11/20/1992	Informational (Approved)
GPC	DOD	Defense System Software Development	DOD-STD-2167A	Informational (Superseded)
GPC	DOD	DOD Automated Information Systems (AIS) Documentation Standards	DOD-STD-7935A	Informational (Superseded)
GPC	DOD	DOD Requirements for a Logistic Support Analysis Record (LSAR)	MIL-STD-1388-2B of 3/28/1991	Informational (Canceled)

3.5.5.5.2 Alternative specifications. The following specifications are also available:

a. Association European des Constructeurs de Material Aerospatial (AECMA) 1000D: Specification for Production of Technical Publications, Utilizing a Common Source Data Base.

b. AECMA 2000M: Specification for Material Management, and Integrated Data Processing for Military Equipment.

3.5.5.5.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.5.5.4 Portability caveats. Europe has its own versions of military logistics support document interchange, and has stated that it will adapt the CALS versions of the logistics support standards (MIL-STD-1388), rather than adopt them without change. Although Europe will seek compatibility, its failure to seek compliance can lead to incompatible areas. North Atlantic Treaty Organization (NATO) is looking into harmonizing DOD and AECMA logistics standards.

If hard copies of documents are required, it should be noted that the ISO A4 paper size commonly used in Europe for international communication on text and facsimile equipment is longer and narrower than that used in the United States, and does not necessarily work with standard office equipment.

MIL-STDs and DOD-STDs 2167A, 7935A, and 1703 have been revised and consolidated (aka 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 standardization process.

3.5.5.5.5 Related standards. The following standards are related to military logistics and document support or support standards:

a. ISO 8571: FTAM
b. ISO 8649: Association Control Service Element (ACSE)
c. ISO 9066: Reliable Transfer Service Element (RTSE)
d. ISO 9072: ROSE

3.5.5.5.6 Recommendations. The adopted standards are recommended.

3.5.5.6 Geospatial data interchange. (This BSA appears in part 5, Data Interchange, and part 6, Graphics.) These standards provide formats and facilities for machine-readable graphics-based mapping, charting, and geodesy data.

3.5.5.6.1 Standards. Table 3.5-33 presents standards for geospatial data interchange.

TABLE 3.5-33 Geospatial data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD (NIMA)	World Geodetic System (WGS 84)	MIL-STD-2401 of 21 March 1994	Mandated (Approved)
GPC	DOD (NIMA)	Raster Product Format (RPF)	MIL-STD-2411:1994	Mandated (Approved)
GPC	DOD (NIMA)	Interface Standard for Vector Product Format (VPF)	MIL-STD-2407	Mandated (Approved)
IPC	NATO	Digital Geographic Information Exchange Standard (DIGEST) Part 1 - Generic Standard Part 2 - Minimum Standards Specifications Part 3 - Matrix (Exchange of elevation of data) Part 4 - Spaghetti Vector	STANAG 7074	Informational (Approved)
GPC	NIST	Spatial Data Transfer Standard (SDTS)	FIPS PUB 173-1:1994	Informational (Approved)
IPC	NATO	Digital Terrain Elevation Data, (DTED)	STANAG 3809	Informational (Approved)
GPC	NIST	Representation of Geographic Point Locations for Information Interchange (adopts ANSI X3.61-1986)	FIPS PUB 70-1:1986	Informational (Approved)
GPC	NIST	Codes for Identification of Hydrologic Units in the United States and the Caribbean Outlying Areas (adopts USGS Circular 878-A and ANSI X3.145-1986)	FIPS PUB 103:1983	Informational (Approved)
GPC	DOD (NIMA)	NIMA GGI&S List of Products and Services	NIMAL 805-1A, Jan 1997	Informational (Approved)
GPC	DOD (NIMA)	Arc Digitized Raster Graphics Worldwide Map Images on CD-ROM, 1:5,000 through 1:2,000,000	MIL-A-89007 of 2/22/1990	Informational (Approved)
GPC	DOD (NIMA)	DTED (Machine readable terrain/elevation data for the U.S., the former USSR, Europe, Central Asia, Mideast, Parts of Southern Asia, Northern Canada, 3-Arc-Sec)	MIL-D-89000 of 2/26/90 MIL-D-89001 of 2/26/90 MIL-D-89020 of 5/28/93	Informational (Approved)
GPC	DOD (NIMA)	Digital Chart of the World (DCW) (A comprehensive 1:1,000,000-scale digital base map of the world)	MIL-D-89009 of 4/13/92	Informational (Approved)
GPC	DOD (NIMA)	Digital Cities Data Base (DCDB)	MIL-D-89011 of 7/2/90	Informational (Approved)
GPC	DOD (NIMA)	Firefinder Elevation Data (FED)	MIL-D-89018 of 10/1/92	Informational (Approved)
GPC	DOD (NIMA)	Digital Landmass Blanking (DLMB)	MIL-D-89021 of 6/15/91	Informational (Approved)
GPC	DOD (NIMA)	Interim Terrain Data/Planning Interim Terrain Data (ITD/PITD)	MIL-I-89014 of 11/30/90	Informational (Approved)
GPC	DOD (NIMA)	Video Disc for Mapping, Charting and Geodesy (Worldwide Map Images on 12 inch Video Disk, 1:50,000 through 1:1,000,000)	MIL-V-89300(1) of 11/30/92	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD (NIMA)	World Vector Shoreline (showing Worldwide Coastlines and International Boundaries, 1:250,000 scale)	MIL-W-89012(2) of 11/30/92	Informational (Approved)
GPC	DOD (NIMA)	World Magnetic Model (WMM)	MIL-W-89500 of 6/18/93	Informational (Approved)
GPC	DARPA	SIMNET Geographic Data Model and Database Interchange Specification	BBN DARPA Report 7108:July 1989	Informational (Approved)
GPC	NGDC	Worldwide Coverage for 5 Mini Grid maps: Bathymetric/Elevation Data	ETOPO 5	Informational (Approved)
GPC	USGS	LANDSAT: Worldwide Coverage for 1:1,000,000 Scale Maps: Feature/Terrain Data	LANDSAT	Informational (Approved)
IPC	NATO	Scope and Presentation of Military Geographic Information and Documentation	STANAG 2251	Informational (Approved)
IPC	NATO	Roads and Road Structures	STANAG 2253	Informational (Approved)
IPC	NATO	MGD-Ports	STANAG 2255	Informational (Approved)
IPC	NATO	Indexes to series of Land Maps and Aeronautical Charts and Indexes to Military Geographic Information and Documentation (MGID)	STANAG 3672	Informational (Approved)
IPC	NATO	Preferred Magnetic Tape Standards for the Exchange of Digital Geographic Information	STANAG 3985	Informational (Approved)
IPC	NATO	Digital Data File Transmittal Form for Geographic Information	STANAG 3986	Informational (Approved)
GPC	USGS	Specification for Representation of Geographic Point Locations for Information Interchange (adopts ANSI X3.61-1986)	USGS Circular 878-B of 1983	Informational (Approved)
GPC	USGS	Digital Elevation Models	USGS Circular 895-B of 1983	Informational (Approved)
GPC	USGS	Digital Line Graphs from 1:24,000 Scale Maps	USGS Circular 895-C of 1983	Informational (Approved)
GPC	USGS	Digital Line Graphs from 1:2,000,000 Scale Maps	USGS Circular 895-D of 1983	Informational (Approved)
GPC	USGS	Land Use and Land Cover Digital Data	USGS Circular 895-E of 1983	Informational (Approved)
GPC	USGS	Geographic Names Information System	USGS Circular 895-F of 1983	Informational (Approved)
GPC	CIA	World Data Bank II: Worldwide Coverage for 1:2,000,000 Scale Maps (Lines of Communication, Coastlines, Waterways, International/Political Boundaries)	World Data Bank II	Informational (Approved)
GPC	DOD (USAF)	Arc Digital Raster Imagery (ADRI) Format	MIL-STD-2406	Informational (Final)
GPC	DOD (NIMA)	Standard Linear Format (SLF) Digital Cartographic Feature	MIL-HDBK-854	Informational (Final)
GPC	DOD (AFMC)	Registered Data Values for Raster/Gridded Product Format	MIL-HDBK-856	Informational (Final)
GPC	DOD (NIMA)	Text Product Form (TPF)	MIL-STD-2400	Informational (Final)
GPC	DOD (NIMA)	Mapping Charting and Geodesy Symbology Graphics	MIL-STD-600002	Informational (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	NATO	Header Record Format for Exchange of Digital Geographic Information	STANAG 3984	Informational (Draft)
IPC	NATO	Digital Geographic Information Data Sets Series Numbering	STANAG 7070	Informational (Draft)
GPC	DOD (NIMA)	DFAD (Machine-readable feature data of the U.S., Europe, the former Western USSR, Limited Areas of Far East and Western Asia, 1:250,000 scale)	MIL-D-89005	Informational (Draft)
GPC	DOD (NIMA)	Tactical Terrain Data: Digital Database for 1:50,000 Scale Maps	TBD-Tactical Terrain Data: Digital Database for 1:50,000 Scale Maps	Informational (Formative)

3.5.5.6.2 Alternative specifications. Many existing proprietary map graphics applications vary in complexity to meet users' needs. These applications serve as the cornerstone of the mapping, charting, and geodesy areas requiring further investigation for standardization consideration.

3.5.5.6.3 Standards deficiencies. Many of the standards listed in the table accompanying this section are old. They do not accommodate new sophisticated computerized techniques, and probably will be replaced in the next several years. The standards available pertain almost exclusively to the data rather than the functionality of an application.

3.5.5.6.4 Portability caveats. Portability will be reduced if a Geographic Information System (GIS) does not allow users to associate their cartographic data independently with relational database management systems based on SQL.

The use of different file formats by a GIS reduces portability. However, in the production world several file formats specified by v· 'ors are used so widely that they are considered neutral file formats (e.g., Intergraph's Standard Interchange Format (SIF), Autodesk's Drawing Exchange Format (DXF), and Map Overlay Statistical System (MOSS)).

Traditionally, standards governing exchanges among field systems have been the responsibility of the military system development organization. This leads to substantial interoperability problems, particularly international. To maximize interoperability, Digital Geographic Information Exchange Standard (DIGEST) and other map producing data should be exchanged between map-producing agencies, such as the National Imagery and Mapping Agency (NIMA) and not between operational units, and the systems development organizations should use the standards set by such agencies as the NIMA.

Portability difficulties may exist between the Vector Product Format (VPF) and the Spatial Transfer Specification (SDTS).

Because too many standards exist, the situation is equivalent to having no standards.

3.5.5.6.5 Related standards. The following standards are related to map graphics exchange or exchange standards:

a. ISO 646: 7-bit Coded Character Set for Information Interchange

b. ISO 1001: File Structure and Labeling of Magnetic Tapes for Information Interchange

c. ISO 2375: Non-Latin Alphabets

d. ISO 6937: Supplementary Characters (for accents to the text)

e. ISO 8211:1985 Specification for a Data Descriptive File for Information Exchange

f. ISO 8824/8825: ASN.1

g. ISO 9292: Picture Coding

h. ISO 9660:1988 Volume and File Structure of CD ROM for Information Exchange

i. ANSI/ASME Y14.26M-1989: IGES (Neutral file format)

j. Intergraph Corporation, Huntsville, AL: SIF

k. Autodesk, Inc., Sausalito, CA: DXF

l. Autometric, Inc., Lakewood, CO: MOSS

m. The various data compression standards listed earlier in the section on data compression

3.5.5.6.6 Recommendations. GIS specifications in a procurement should require SQL compatibility so that cartographic data can be associated independently with relational database management systems based on SQL. In each case, consideration of the scale of data and geographic region needed will be a primary determinant in selection. The standards in the table above labeled mandated are recommended. The VPF is preferred.

If a packaged GIS is to be purchased, if possible, it should be standardized around a single GIS file format. If a GIS is to be used on workstations and PCs, this may not be possible. Then the agency's focus will have to be on the use of interoperability protocols and designing applications for portability. GIS specifications should require SQL compatibility so that cartographic data can be associated independently with relational database management systems based on SQL.

3.5.5.7 Symbology graphics. (This BSA appears in part 5, Data Interchange, and part 6, Graphics.) These are standards for the symbology to be used in geospatial applications such as hardcopy mapping products and computer-generated displays. DoD standards provide definitions for the representation of military and intelligence information.

3.5.5.7.1 Standards. Table 3.5-34 presents standards for symbology graphics.

TABLE 3.5-34 Symbology graphics standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD (US Army)	Human Factors Engineering Design Criteria for Helicopter Cockpit Electro-Optical Display Symbology	MIL-STD-1295A of 6/26/1984	Adopted (Approved)
GPC	DOD (USAF)	Aircraft Display Symbology	MIL-STD-1787B of 6/93	Adopted (Approved)
GPC	DOD (NIMA)	Mapping, Charting and Geodesy (MC&G) Symbology for Graphic Products	MIL-STD-2402 of 2/95	Adopted (Approved)
GPC	DOD (DISA)	Common Warfighting Symbology, Version 1	MIL-STD-2525	Adopted (Approved)
GPC	WMO	Technical Regulation Vol II, Meteorological Services for International Air Navigation	WMO Document #49 of 1988	Adopted (Approved)
GPC	DOD	Military Symbols	Q-STAG 509 of 3/5/1979	Informational (Approved)
NPC	ANSI/SAE	Human Interface Design Methodology for Integrated Display Symbology	ARP 4155 (1990)	Informational (Approved)
GPC	DOD (US Army)	Symbols for Army Air Defense System Displays	MIL-STD-1477B of 2/1/1993	Informational (Approved)
GPC	DOD (DISA)	Common Warfighting Symbology, Version 2	MIL-STD-2525A	Informational (Approved)
GPC	DOD (US Army)	Army Field Manual (FM): Operational Terms and Symbols	FM 101-5-1 SMIGS (Symbols of Oct. 1985)	Informational (Approved)
NPC	ANSI/ISA	Instrumentation Symbols and Identification	S5.1-1984 (R1992)	Informational (Approved)
NPC	ANSI/ISA	Graphic Symbols for Process Displays	S5.5-1985	Informational (Approved)
IPC	NATO	NATO Experimental Tactics and Amplifying Tactical Instructions - AXP-5(B) (Navy/Air)	STANAG 1125	Informational (Approved)
IPC	NATO	Military Symbols for Land Based Systems (APP-6, Ed 3)	STANAG 2019(1) of 11/26/1990	Informational (Approved)
IPC	NATO	Electronically and/or Optically Generated Aircraft Displays for Fixed Wing Aircraft	STANAG 3648 of 6/29/1990	Informational (Approved)
IPC	NATO	Symbols on Land Maps, Aeronautical Charts and Special Naval Charts	STANAG 3675	Informational (Approved)
IPC	NATO	Symbols for Use on Maps of Training Areas for Land Forces	STANAG 3833	Informational (Approved)
GPC	CJCS	Joint Symbols and Graphics	Joint Pub 1-06	Informational (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD (US Army)	Army Field Manual (FM): Operational Terms and Symbols	FM 101-5-1A SMIGS	Informational (Draft)
GPC	DOD (NIMA)	Vector Product Format Symbology	MIL-PRF-89045	Informational (Draft)
GPC	DOD (ASPO)	Symbol Automation	MIL-STD-2526	Informational (Draft)
GPC	DIA	Standard Military Graphics Symbols (SMIGS)	DIAM 65-xx	Informational (Draft)
IPC	NATO	Display Symbology and Colors for NATO Maritime Units	STANAG 4420	Informational (Formative)

3.5.5.7.2 Alternative specifications. No other consortia or de facto specifications are available.

3.5.5.7.3 Standards deficiencies. Draft MIL-STD-2525A does not currently contain weather, geospatial (mapping/charting), cockpit display, and engineering design symbology. Therefore NIMA MIL-STD-2402, 2412 should be used for geospatial symbology until such time as a decision is made to modify MIL-STD-2525A to accomodate these symbols.

3.5.5.7.4 Portability caveats. Portability will be reduced if a GIS does not allow users to associate their cartographic data independently with relational database management systems based on SQL. Only government standards are available. Most commercial products will not comply with these standards.

3.5.5.7.5 Related standards. The following standards are related to symbology graphics or symbology graphics standards:

a. ISO 6937: Supplementary Characters (for accents to the text)
b. ISO 9292: Picture Coding
c. Autometric, Inc., Lakewood, CO: MOSS
d. Map graphics standards.

3.5.5.7.6 Recommendations. The adopted symbology standards are recommended, as applicable; MIL-STD 2525 is the recommended standard for warrior symbology.

3.5.5.8 Continuous Acquisition and Life-Cycle Support. Continuous Acquisition and Life-Cycle Support (CALS) standards specify the digital exchange of documents. CALS is one part of a broad Electronic Commerce (EC) initiative within the DOD that has the potential for converging CALS standards and enabling technologies within the Open Systems Environment (OSE). CALS has begun to emerge from its legacy as support for weapon systems technical documents. Current and projected CALS standards will rationalize their native standards and emphasize the use of external Open Systems standards for their products, permitting format conversion and extensions to deal with complex documents.

3.5.5.8.1 Standards. Table 3.5-35 presents standards for continuous acquisition and life-cycle support.

TABLE 3.5-35 Continuous Acquisition and Life-Cycle Support standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Automated Interchange of Technical Information (Life cycle logistic support of weapon systems)	MIL-STD-1840B of 11/3/1992	Adopted (Approved)
GPC	DOD	Contractor Integrated Technical Information Service (CITIS)	MIL-STD-974	Adopted (Approved)
GPC	DOD	Department of Defense Continuous Acquisition and Life-Cycle Support (CALS) Program Implementation Guide	MIL-HDBK-59B	Adopted (Approved)
GPC	DOD	Manuals, Interactive Electronic Technical: General Content, Style, Format and User Interaction Requirements	MIL-M-87268 11/20/1992	Adopted (Approved)
GPC	DOD	Database Revisable:Interactive Electronic Technical Manuals for the Support of	MIL-D-87269 of 11/20/1992	Adopted (Approved)
GPC	DOD	Quality Assurance Program Interactive Electronic Technical Manuals (IETM) and Associated Technical Information, Requirements for	MIL-Q-87270 of 11/20/1992	Adopted (Approved)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-PRF-28000	Informational (Approved)
GPC	DOD	Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of text (based on ISO 8879)	MIL-PRF-28001	Informational (Approved)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-PRF-28002	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Illustration Data : CGM Application Profile (based on FIPS 128)	MIL-PRF-28003	Informational (Approved)
GPC	DOD	Handbook for use of MIL-M-28001B	MIL-HDBK-28001	Informational (Formative)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-D-28000A(1) of 12/14/92	Informational (Superseded)
GPC	DOD	Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of text (based on ISO 8879)	MIL-M-28001B of 6/26/1993	Informational (Superseded (CALS))
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-R-28002B of 12/14/1992	Informational (Superseded (CALS))
GPC	DOD	Digital Representation for Communication of Illustration Data : CGM Application Profile (based on FIPS 128)	MIL-D-28003A(1) of 8/14/1992	Informational (Superseded)

3.5.5.8.2 Alternative specifications. The AAP TEI has designed an alternative nonproprietary architecture with SGML encodings.

3.5.5.8.3 Standards deficiencies. Markup consists of the common sets of document formatting codes used in classes of document types. Each document type commonly uses a particular publishing style. Technical manuals may use a different makeup from management guideline documents to accommodate the audience, content, and publishing layout styles. Since SGML does not deal with the markup's meaning, it does not specify what to do after the document has been processed by a program that recognizes SGML.

SGML does not use object-oriented methods or deal with hypermedia/time-based document interchange. Standards in both areas are under development.

MIL-PRF-28001 uses relatively few SGML features and, therefore, restricts and minimizes the effectiveness of the markup. However, the standards can be used to transfer revisable documents. However, the DOD/CALS standard mainly is used for weapon system technical support documents, with limited application to business office environments.

3.5.5.8.4 Portability caveats. The DOD CALS have limited functionality when compared with ODA/ODIF and other standards used in support of business operations. Users should treat complex and/or compound documents with care to ensure upward compatibility with evolving standards.

European decisions to adapt rather than fully adopt CALS standards may lead to incompatibilities.

3.5.5.8.5 Related standards. The following standards are related to CALS standards.

a. ISO 8879: SGML
b. ISO 8632: CGM
c. IGES Version 4.0, 5.2
d. ISO 8879:1988: SDIF
e. ISO 9069:1988: SGML Support Facilities for SDIF
f. MIL-STD 974: Contractor Integrated Technical Information Service (CITIS)
g. MIL-HDBK-59: CALS Program Implementation Guide

3.5.5.8.6 Recommendations. The CALS standards are recommended where they apply. The DOD SGML standard (MIL-PRF-28001) is based on ISO 8879. In the meantime, use DOD SGML in conjunction with other specifications that determine the markup's meaning (such as the EMPM of the ODA (ISO 8613). Refer to the document exchange BSA for further SGML recommendations.

IGES is recommended when multivendor product data exchange capabilities are needed. The DOD/CALS IGES standard is preferred for engineering drawings, electronics, and numerical control. The standard is optional for technical manual illustration, and the CGM standard is more

appropriate. The more comprehensive STEP will provide more comprehensive functionality than IGES.

3.5.6 Graphics data interchange. Graphics data interchange is a collection of service areas that form the basis for creating graphics. Special graphics applications such as found in Technical Data Interchange are not included.

3.5.6.1 Raster data interchange. (This BSA appears in part 3, part 5, and part 6.) Raster data interchange MIL SPEC identifies the requirements to be met when raster graphics data represented in digital, binary format are delivered to the government. Raster graphics standards are standards for pixel-by-pixel representation of images. (See still image compression, section 3.5.8.2, for more facsimile standards suitable for raster data interchange.)

3.5.6.1.1 Standards. Table 3.5-36 presents standards for raster data interchange.

TABLE 3.5-36 Raster data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	User Interface Component of the Applications Portability Profile (Adopts the X Protocol, Xlib Interface, Xt Intrinsics, and Bitmap Distribution Format of X11R5)	FIPS PUB 158-1:1993	Mandated (Approved)
NPC/IPC	ANSI/ISO/IEC	Interfacing Techniques for Dialogues with Graphical Devices (CGI) - Functional Specification - Part 6: Raster	9636-6:1991	Mandated (Approved)
GPC	DOD (NIMA)	Raster Product Format (RPF)	MIL-STD-2411:1994	Mandated (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 1: Overview and Fundamental Principles (formerly Product Data Exchange Specification (PDES))	10303-1:1994	Informational (Approved)
CPC	X/Open	X Window System File Formats and Application Conventions (Bitmap Distribution Format (BDF))	C170 (7/91)	Informational (Approved)
GPC	NIST	General Aspects of Group 4 Facsimile Apparatus (Adopts EIA-536-1988)	FIPS PUB 149:1988	Informational (Approved)
GPC	NIST	Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus (Adopts EIA 538-1988)	FIPS PUB 150:1988	Informational (Approved)
GPC	NIST	Initial Graphics Exchange Specification (IGES) (adopts ASME/ANSI Y14.26M-1989) (IGES ver. 4)	FIPS PUB 177:1992	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-PRF-28000	Informational (Approved)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-PRF-28002	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Illustration Data : CGM Application Profile (based on FIPS 128)	MIL-PRF-28003	Informational (Approved)
NPC	ANSI/AIIM	Recommended Practice; File Format for Storage and Exchange of Images; Bi-Level Image File Format: Part 1	MS53-1993	Informational (Approved)
GPC	NIST	Standard for the Interchange of Large Format Tiled Documents	NISTIR 88-4017	Informational (Approved)
IPC	NATO	Analogue Video Standard for Aircraft System Applications	STANAG 3350	Informational (Approved)
IPC	NATO	Exchange Specifications for ARC Standardized Raster Graphics (ASRG)	STANAG 4387:1996	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	NATO	Specifications for UTM/UPS Standardized Raster Products (USRP)	STANAG 7077	Informational (Approved)
IPC	ITU-T	Document Application Profile for the Interchange of Formatted Mixed Mode Document - Terminal Equipment and Protocols for Telematic Services	T.501 (1989)	Informational (Approved)
IPC	ITU-T	Document Application Profile for the Interchange of Group 4 Facsimile Documents	T.503 (1991)	Informational (Approved)
NPC	AIIM	Interchange of Tiled Raster Documents	TR14:1988	Informational (Approved)
IPC	NATO	Exchange Specifications for ARC Digitized Raster Graphics (ADRG)	STANAG 7108	Informational (Draft)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-D-28000A(1) of 12/14/92	Informational (Superseded)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-R-28002B(1) of 9/20/1993	Informational (Superseded)

3.5.6.1.2 Alternative specifications. Currently IGES is the most mature and widely implemented standard for conveying product data information. Other bitmap formats include proprietary formats such as GIF, PCX, TIFF, RLE, and TGA. Except for support of legacy products, these formats are not recommended.

3.5.6.1.3 Standards deficiencies. Raster graphics files require enormous amounts of storage and must be supplemented by compression standards.

3.5.6.1.4 Portability caveats. A standard technique for raster data interchange should be selected for use throughout the DOD and applied wherever possible.

3.5.6.1.5 Related standards. The following standards are related to raster data interchange or raster data interchange standards:

a. ASME/ANSI Y14.28M-1989, which describes product design and manufacturing information.

b. ITU-T, facsimile transmission standards.

c. Raster compression standards.

3.5.6.1.6 Recommendations. The mandated standards are recommended for raster data interchange.

MIL PRF-28002 (Raster) can be used in a Computer-Aided Acquisition and Logistic Support (CALS) environment, and, when needed, supplemented by National Institute of Standards and Technology Interim Report (NISTIR) 88-4017 (tiling). FIPS Pub 150 can also be used. With only the CALS Raster standard available, no real tailoring guidance is possible. This version

(MIL-PRF-28002) supports engineering drawings and technical manual illustrations. The previous CALS Raster standard (MIL-R-28002B) can be used for in-place and unrevised legacy data. Tiling (as in NISTIR 88-4017) and compression are desirable for very large raster graphics files. (See the Still image compression BSA, part 3.5.8.2 of the ITSG.) MIL-PRF-28003 (CGM) offers the capability for having raster and vector graphics in the same file. The approved BDF provides conventions for font conversion/interchange between external and internal X Windows fonts and can be used in procurements using a client-server computing architecture with a graphical user interface in a networked environment. BDF can be compiled in Server Normal Format to be optimized for a particular server.

3.5.6.2 Image data interchange. Image data interchange is the exchange of imagery data, metadata, and attachments to the images. (See still image compression and raster data interchange for more standards suitable for image data interchange.)

3.5.6.2.1 Standards. Table 3.5-37 presents standards for image data interchange.

TABLE 3.5-37 Image data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Metafile for Storage/Transfer of Pictorial Description Information (CGM) (as profiled by FIPS PUB 128-1 and MIL-STD-2301)	8632-1,2,3,4:1992 (w/Amd 1&2)	Mandated (Approved)
IPC	ISO/IEC	Digital Compression and Coding of Continuous - Tone Still Images, Part 1: Requirements and Guidelines (as profiled by MIL-STD-188-198A - JPEG)	10918-1:1994	Mandated (Approved)
GPC	DOD	Bi-Level Image Compression	MIL-STD-188-196	Mandated (Approved)
GPC	DOD	Vector Quantization (VQ) Decompression for the NITFS	MIL-STD-188-199 of 6/27/1994	Mandated (Approved)
GPC	DOD	National Imagery Transmission Format version 2.0	MIL-STD-2500A	Mandated (Approved)
TBD	TBD	JPEG File Interchange Format (JFIF), Version 1.02, C-Cube Microsystems for raster graphics data	JFIF	Mandated (Approved)
GPC	DOD	National Imagery Transmission Format Standard	MIL-HDBK-1300A	Informational (Approved)

3.5.6.2.2 Alternative specifications. No alternative specifications exist.

3.5.6.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.6.2.4 Portability caveats. Portability problems with the existing standards are not known.

3.5.6.2.5 Related standards. The remaining National Imagery Transmission Format Standard (NITFS) documents are related.

3.5.6.2.6 Recommendations. The mandated standards are recommended.

3.5.6.3 Vector graphics data interchange. (This BSA appears in part 5, Data Interchange, and part 6, Graphics.) These standards provide file formats for the storage, exchange, and import/export of raster or vector graphical drawings and images.

3.5.6.3.1 Standards. Table 3.5-38 presents standards for vector graphics data interchange.

TABLE 3.5-38 Vector graphics data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Metafile for Storage/Transfer of Pictorial Description Information (CGM) (as profiled by FIPS PUB 128-1 and MIL-STD-2301)	8632-1,2,3,4:1992 (w/Amd 1&2)	Mandated (Approved)
NPC/IPC	ANSI/ISO/IEC	Programmers' Hierarchical Interactive Graphics System (PHIGS and PHIGS PLUS) (as profiled by FIPS PUB 153-1)	9592-1,2,3,4:1989 with AMD1:1992	Mandated (Approved)
GPC	NIST	Initial Graphics Exchange Specification (IGES) (adopts ASME/ANSI Y14.26M-1989) (IGES ver. 4)	FIPS PUB 177:1992	Informational (Approved)
NPC	ANSI/US PRO	IGES 5.2, Initial Graphics Exchange Specification (Replaces ANSI/ASME Y14.26M-1989)	US PRO/IPO-100 (Nov 1993)	Informational (Approved)
IPC	ANSI/NPESA	Prepress Digital Data Exchange - Tag Image File Format for Image Technology (TIFF/IT)	IT8.8	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-PRF-28000	Informational (Approved)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-PRF-28002	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Illustration Data : CGM Application Profile (based on FIPS 128)	MIL-PRF-28003	Informational (Approved)
GPC	DOD	Computer Graphics Metafile (CGM) Implementation Standard for National Imagery Transfer Format Standard (NITFS) (based on FIPS 128)	MIL-STD-2301A	Informational (Approved)
NPC	ANSI/AIIM	Recommended Practice; File Format for Storage and Exchange of Images; Bi-Level Image File Format: Part 1	MS53-1993	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-D-28000A(1) of 12/14/92	Informational (Superseded)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-R-28002B(1) of 9/20/1993	Informational (Superseded)
GPC	DOD	Digital Representation for Communication of Illustration Data : CGM Application Profile (based on FIPS 128)	MIL-D-28003A(1) of 8/14/1992	Informational (Superseded)
NPC	ANSI/ASME	Digital Representation for Communication of Product Definition Data	Y14.26M:1989	Informational (Superseded)

3.5.6.3.2 Alternative specifications. The following specifications are also available:

a. BMP (Windows Bitmap) - Proprietary.
b. CGI (Computer Graphics Interface)
c. GIF (Graphics Interchange Format) (Used by CompuServe)
d. NAPLPS (North American Presentation Level Protocol Syntax)
e. PDL (Page Description Language) - Proprietary

f. TIFF (Tagged Image File Format) - Proprietary
g. VDM (Virtual Device Metafile)
h. VDI (Virtual Device Interface)

3.5.6.3.3 Standards deficiencies. The CGM standards have limited capabilities for handling 3-D geometries, providing fine control over line drawing details, and using font resource references enabling reasonably accurate font substitution (the latter is an understatement), and describing color. Several addenda and amendments are being developed. The addenda would add a global symbol capability, 3-dimensional geometry extensions, and improved engineering drawing capabilities (such as better control over fine details of line drawings). The amendments listed in table 3.5-20 are concerned with fonts and color. These CGM changes are intended to be upwardly compatible with existing versions of the specification.

3.5.6.3.4 Portability caveats. Portability problems for existing versions of the CGM standard are unknown. Potential portability problems exist for the CGM addenda and amendments, as with any new version of a specification or product, even though the standards groups are developing their specifications with upward compatibility in mind.

3.5.6.3.5 Related standards. The following standards are related to graphics data exchange or graphics data exchange standards:

a. ISO 9281: Identification of Picture Coding Methods.

b. ISO 10918-1: Digital Compression and Coding of Continuous Tone Still Images, Part 1: Requirements and Guidelines.

c. ISO 10918-2: Digital Compression and Coding of Continuous Tone Still Images, Part 2: Compliance Testing.

d. ISO CD 11172: Coding of Moving Pictures and Associated Audio.

e. ISO SC21/WG5, N4192: Proposed FTAM Document Type to Support CGM.

f. ISO SC21/WG5, N5165: FTAM Constraint Set and Document Types for CGM.

g. MIL-HDBK-1300A, NITFS

h. MIL-STD-2500A, National Imagery Transmission Format (NITF) Version 2.0 for the NITFS.

3.5.6.3.6 Recommendations. The mandated standards are recommended.

The following wording from the APP is recommended for specifying data interchange standards:

"All computer graphics metafiles acquired to describe, store, and/or communicate graphical (pictorial) information in vector format among different devices, systems, and installations should comply with the requirements set forth in FIPS PUB 128-1, Computer Graphics Metafile (CGM)."

The use of CGM is widespread, and many (most) off-the-shelf products for graphics data interchange are compatible with it.

It is important to consider the specification of CGM conformance in procurements because CGM is important to the integration of PC applications with the enterprise. Most PC graphics, word processing and desktop publishing programs support the importing and exporting of pictures, bidirectionally to other PC programs and between PC and server/minicomputer/ workstation applications.

3.5.6.4 Color definition. (This BSA appears in part 5, Data Interchange, part 12, Multimedia, and part 13, Human Factors.) Color definition deals with establishing a reference base for identifying colors to aid in the matching and exchange of color. Color definition standards apply to defining color in general, and not only to color definition for information technology systems.

3.5.6.4.1 Standards. Table 3.5-39 presents standards for color definition.

TABLE 3.5-39 Color definition standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ASTM	Standard Test Method for Computing the Colors of Objects by Using the CIE System	E308 (1990)	Informational (Approved)
NPC	EIA	1976 CIE-UCS Chromaticity Diagram with Color Boundaries	TEB26 (1988)	Informational (Approved)
IPC	ISO	CIE Standard Colorimetric Illuminants	CIE 10526 (1991)	Informational (Approved)
IPC	ISO	CIE Standard Colorimetric Observers	CIE 10527 (1991)	Informational (Approved)
IPC	CIE	Recommendations on Uniform Color Spaces, Color-Difference Equations, and Psychrometric Color Terms	CIE Pub. 15, Suppl. 2 (1986)	Informational (Approved)
NPC	NPESA	Graphic Technology - Input Data for Characterization of 4-Color Process Printing	IT8.7/3 (1993)	Informational (Approved)
NPC	NPESA	Graphic Arts Prepress Definition of Default RGB Data for Use in the Graphic Arts Industry	IT8.7/4	Informational (Approved)
N/A	SMPTE/EIA/VESA/ISO	Unreferenced 24-bit RGB	Technical Reports	Informational (Approved)
IPC	ISO/IEC	Text and Office Systems Colour Architecture (TOSCA)	JTC1/SC18/WG5	Informational (Draft)
CPC	ICC	Definition of Named Color	TBD	Informational (Formative)
NPC	ANSI IT8 and CGATS	Specifications for Web Offset Publications (SWOP)	TBD	Informational (Formative)

The CIE (International Commission on Illumination) is the principal international standards writing body for agreements for color, vision, and illumination. Under ANSI, four bodies work on color-related standards. ANSI X3 works on office document automation and information systems. ANSI IT8/CGATS is concerned with graphic arts. ASTM deals with color metrology and standard practices, and SMPTE handles standards for color television and color monitors.

ANSI's Committee for Graphic Arts Technology Standards (CGATS) has eight subcommittees working on topics such as materials handling, process control, and color data definition. NPESA is the National Printing Equipment and Supply Association.

3.5.6.4.2 Alternative specifications. The following alternative specifications are also available:

a. Pantone Matching System

b. RGB (Red, Green, Blue) - the method directly used by color video display terminals

c. CMYK (Cyan, Magenta, Yellow, Black) - used in four color printing

d. HSV (Hue, Saturation, V.)

e. HSL (Hue, Saturation, Luminescence)

f. HVC

g. SWOP (Specifications for Web Offset Publications)

h. HSB (Hue, Saturation, Brightness)

i. TIFF (Tag Image File Format)

3.5.6.4.3 Standards deficiencies. Comparison of color defined by the existing standards assumes identical viewing conditions. There are no standards directly addressing comparisons across viewing environments, although models are being worked on. Strict adherence to correct presentation and output standards will require color calibration equipment.

3.5.6.4.4 Portability caveats. Translation of color from one color definition system to another can be difficult and is only an approximation at best. There are three different color definitions from the CIE. They are the CIEXYZ tristimulus values, and the CIELAB and CIELUV color spaces. These standards have existed for a long time and are seen as the common basis for any future unifying definitions. There are also the problems of color matching. For example, of 1012 Pantone colors for coated paper, 70 cannot be reproduced in the CMYK definition. CIEXYZ is useful in comparing colors under identical viewing conditions. CIEXYZ has a rigorous definition and by itself does not necessarily constitute a complete color specification. CIEXYZ is a standardized set of primaries which are not physically realizable but can match all possible colors with entirely positive tristimulus values. A new form of color definition is emerging, known as high-fidelity color. The idea behind high-fidelity color is the use of five to seven different colors in the printing process to widen the range of colors that can be printed. Two such models that have appeared are the Kupper set which increases the number of printed colors in the blue region by 80%, and the VSF model which provides better performance in deep red and green colors. These processes are very non-standard and should be avoided at present.

Common systems typically do not support colorimetric calibration.

3.5.6.4.5 Related standards. The following types of standards are related to standards for the definition of color:

a. color matching standards
b. color data exchange standards

c. color use standards
d. style guide standards

3.5.6.4.6 Recommendations. The approved standards in this section are recommended where they are applicable. Maintain original copies of source material so that revisions can be produced for next generation systems that will allow the inclusion of calibration information.

3.5.6.5 Color data interchange. (This BSA appears in part 5, Data Interchange, and part 13, Human Factors.) This BSA deals with the specific problems of interchanging data about color in computer graphics.

3.5.6.5.1 Standards. Table 3.5-40 presents standards for color data interchange.

TABLE 3.5-40 Color data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Graphic Technology - Prepress Digital Data Exchange - Colour Picture Data on Magnetic Tape (ANSI IT8.1-1988)	10755:1992	Informational (Approved)
IPC	ISO	Graphic Technology - Prepress Digital Data Exchange - Colour Line Art Data on Magnetic Tape	10756:1994	Informational (Approved)
IPC	ISO	Graphic Technology - Prepress Digital Data Exchange - Online Transfer from Electronic Prepress Systems to Colour Hardcopy Devices	10758:1994	Informational (Approved)
NPC	NPESA	Graphic Technology - Input Data for Characterization of 4-Color Process Printing	IT8.7/3 (1993)	Informational (Approved)
NPC	NPESA	Graphic Arts Prepress Definition of Default RGB Data for Use in the Graphic Arts Industry	IT8.7/4	Informational (Approved)
IPC	ISO/IEC	Generic Architecture for Colour Data Interchange (GACDI)	JTC1/SC18/WG5	Informational (Draft)

The Generic Architecture for Colour Data Interchange (GACDI) standard is a color architecture standard that will provide a consistent color framework across document-related standards. This standard will enable users to interchange color information in an open systems environment through the use of color data and transform representations.

3.5.6.5.2 Alternative specifications. No alternative specifications are available.

3.5.6.5.3 Standards deficiencies. There are no standards directly addressing comparison across viewing environments, although models are being worked on.

3.5.6.5.4 Portability caveats. Portability problems with the existing standards are unknown.

3.5.6.5.5 Related standards. Data interchange standards are related to standards for color data exchange.

3.5.6.5.6 Recommendations. The approved standards in this section are recommended where they are applicable.

3.5.6.6 Color matching. (This BSA appears in part 5, Data Interchange, and part 13, Human Factors.) This BSA deals with the problem of matching displayed and printed colors in computer systems.

3.5.6.6.1 Standards. Table 3.5-41 presents standards for color matching.

TABLE 3.5-41 Color matching standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Graphic Technology - Prepress Digital Data Exchange - Online Transfer from Electronic Prepress Systems to Colour Hardcopy Devices	10758:1994	Informational (Approved)
NPC	ASTM	Standard Test Method for Computing the Colors of Objects by Using the CIE System	E308 (1990)	Informational (Approved)
IPC	CIE	Recommendations on Uniform Color Spaces, Color-Difference Equations, and Psychrometric Color Terms	CIE Pub. 15, Suppl. 2 (1986)	Informational (Approved)
NPC	NPESA	Graphic Technology - Input Data for Characterization of 4-Color Process Printing	IT8.7/3 (1993)	Informational (Approved)
NPC	NPESA	Graphic Arts Prepress Definition of Default RGB Data for Use in the Graphic Arts Industry	IT8.7/4	Informational (Approved)
CPC	ICC	ICC Profile Format	ICC Profile Format ver. 3, 1994	Informational (Approved)
IPC	ISO/IEC	Text and Office Systems Colour Architecture (TOSCA)	JTC1/SC18/WG5	Informational (Draft)

The ICC was formed in March, 1994, by Apple, Adobe, Silicon Graphics, Taligent, Agfa, Kodak, Microsoft, and Sun for the purpose of defining profiles for color handling. The ICC Profile format has no preferred color space, and provides for more than four input colors.

ColorSync Profile Consortium has adopted the CGATS.5 specification as its definition of colorimetry and color measurement.

The Open System Color Association (OSCA) has taken on the role of providing industry with a centralized, stable, reliable, and common source of certified color-calibration data. OSCA consists of Agfa, DuPont, Fujifilm, Kodak, Radius, 3M, and 24 other non-founding member companies. OSCA's work is in harmony with the ICC Profile format.

3.5.6.6.2 Alternative specifications. The following alternative specifications are also available:

a. Pantone Matching System (PMS)

b. RGB (Red, Green, Blue) - the method directly used by color video display terminals

c. CMYK (Cyan, Magenta, Yellow, Black) - used in four color printing

d. Apple ColorSync 2.0 (supports ICC and CMYK)

e. Kodak Precision Color Management System (CMS)

f. Electronics for Imaging (EFI) Inc., EFIColor

g. Hewlett-Packard ColorSmart

h. Microsoft Independent Color Matching (ICM) in future versions of WindowsNT and Windows 95. (accepts ICC Profile Format).

i. Pantone Open Color Environment (POCE) (overshadowed by CMS and ColorSync)

j. Pantone ColorDrive (to standardize color palettes)

k. Trumatch SwatchPrinter

l. Tektronix TekColor

m. Agfa-Gevaert FotoFlow

3.5.6.6.3 Standards deficiencies. Comparison of color defined by the existing standards assumes identical viewing conditions. There are no standards directly addressing comparisons across viewing environments, although models are being worked on. the issue of where and how to correct color remains unresolved.

3.5.6.6.4 Portability caveats. Translation of color from one color definition system to another can be difficult and is only an approximation at best. There are three different color definitions from the CIE. They are CIEXYZ, CIELAB, and CIELUV. These standards have existed for a long time and are seen as the common basis for any future unifying definitions

Because of their display orientation, all standards that are defining computer generated graphics color, use RGB models. Most programmers assume that the RGB values they are using are linear with display intensity and that may be approximately true depending on the response of the graphics system. The actual colors produced vary according to the graphics system used.

3.5.6.6.5 Related standards. Color definition standards are related to human factors standards for color matching.

3.5.6.6.6 Recommendations. The approved standards in this section are recommended where they are applicable.

3.5.7 DOD messaging. The following base service areas deal with specialized topics of message exchange in real time tactical systems.

3.5.7.1 Interchange of formatted military messages. These standards specify military fixed and variable format messages used in the exchange of tactical information. Most of the standards for formatted military messages are not open systems standards and, therefore, do not conform to the design requirements for open systems.

3.5.7.1.1 Standards. The following table presents the major DOD joint standards for the exchange of preformatted tactical military messages. Not all the standards listed below are open systems compliant and, therefore, fall outside the purview of this document. They have been included for completeness.

Table 3.5-42 presents standards for interchange of formatted military messages.

TABLE 3.5-42 Interchange of formatted military messages standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Message Text Formats (MTF) (NOTE 1)	Interim MIL-STD-6040 and CJCSM 6120.05	Mandated (Approved)
GPC	DOD	Joint Tactical Information Distribution System (JTIDS) Technical Interface Design Plan - Test Edition (TIDP-TE) (TADIL J Message Standard)	JIEO (TIDP-TE)	Mandated (Approved)
GPC	DOD	National Imagery Transmission Format version 2.0	MIL-STD-2500A	Mandated (Approved)
IPC	NATO ADSIA	Interoperability Standards and Allied Operating Procedures for NATO Link 16	STANAG 5516 & ADATP-16	Mandated (Approved)
GPC	DOD	Tactical Digital Information Link (TADIL) Message Standards (TADIL A, B, and C) (NOTES 3 and 4)	MIL-STD-6011	Informational (Approved)
IPC	NATO ADSIA	Interim Joint Tactical Information Distribution System (JTIDS) Message Specification (IJMS)	IJMS Decision Paper 4 and 5	Informational (Approved)
IPC	NATO ADSIA	Interim Joint Tactical Information Distribution System (JTIDS) Message Specification (IJMS) Standing Operating Procedures (SOP)	IJMS Decision Paper 6	Informational (Approved)
GPC	DOD (JIEO)	Multi-TADIL Data Extraction and Reduction Guide (DERG)	JIEO DERG-Guide	Informational (Approved)
GPC	CJCS	Joint Multi-TADIL Operating Procedures (NOTE 8)	Joint Pub 3-56.20 thru 23	Informational (Approved)
GPC	DOD	Army Tactical DATA Link-1 (ATDL-1) Message Standard (Note 6)	MIL-STD-6013	Informational (Approved)
IPC	NATO ADSIA	NATO Performance Standards and Allied Operating Procedures for Ship-Shore-Ship Buffer	STANAG 5601 & ADATP-12	Informational (Approved)
IPC	NATO ADSIA	NATO Message Text Format (MTF) and Allied Operating Procedures	STANAG 5500 & ADATP-3	Informational (Approved)
IPC	NATO ADSIA	Interoperability Standards and Allied Operating Procedures for NATO Link 11	STANAG 5501 & ADATP-31	Informational (Approved)
IPC	NATO ADSIA	Interoperability Standards and Allied Operating Procedures for NATO Link 4	STANAG 5504 & ADATP-4	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	NATO ADSIA	Interoperability Standards and Allied Operating Procedures for NATO Link 11 and 11B	STANAG 5511 & ADATP-11	Informational (Approved)
IPC	NATO ADSIA	Data Forwarding Standards for NATO Data Link	STANAG 5616	Informational (Draft)
IPC	NATO ADSIA	Interoperability Standards for NATO Link 22	STANAG 5522	Emerging (Draft)
GPC	DOD	Variable Message Format (VMF) Interface Operating Procedures (IOP)	VMF (IOP)	Emerging (Partial Draft)
GPC	DOD	Tactical Digital Information Link (TADIL C) Message Standard (NOTE 5)	Interim MIL-STD-6004	Informational (Draft)

Notes:

(1) United States Message Text Formats (USMTF) provide a structured format for use by the military services and other government agencies. It is a character-oriented message (COM) and can be transmitted in record or voice formats. It is used to transmit down-channel, lateral, and up-channel information.

(2) Variable Message Format (VMF) messages are bit-oriented messages (BOM) that are used to exchange information that is time sensitive (but not real-time), requires a response or action, and are machine readable. The structure of VMF messages are designed to provide specific information consisting of specific fields. The VMF standard continues to expand under configuration control. This expansion is expected to continue through FY96.

(3) Tactical Data Information Link (TADIL) A is a secure, netted data link using parallel transmission frame characteristics and standard message formats at either 2[illegible] 1364 bits per second. TADIL A operates in the high frequency (HF) and ultra-high frequency (UHF) frequency range. TADIL A is interoperable with NATO Link 11.

(4) TADIL B is a secure point-to-point data link utilizing serial transmission frame characteristics and standard message formats at a basic speed of 600 or 1200 bits per second. This data link interconnects tactical air defense and air control units. Message formats are the same for TADIL B and TADIL A. TADIL B is interoperable with NATO Link 11B.

(5) TADIL C is a time division data link between control station and controlled aircraft. It provides the capability for automatic transmission of orders, status, and other information. Data exchange is accomplished on a fully automatic link at 5000 bits per second, using serial transmission. TADIL C uses the UHF frequency range. TADIL C will be updated and republished in a separate MIL STD in FY96. TADIL C is interoperable with NATO Link 4.

(6) The Army Tactical Data Link (ATDL-1) is a point-to-point digital data link using serial transmission frame characteristics and standard message formats at a basic speed of 600 or 1200 bits per second. This data link connects tactical air control and defense-oriented systems.

(7) TADIL J is a high capacity, secure, jam-resistant, nodeless broadcast-type RF data link that uses a time division multiple access (TDMA) protocol. It provides information distribution, position location, and identification capabilities in an integrated form for tactical military operations. TADIL J uses the Joint Tactical Information Distribution System (JTIDS), and the protocols, conventions, and fixed word message formats defined by the JTIDS Technical Interface Design Plan - Test Edition (TIDP-TE). JTIDS operates in the upper ultrahigh frequency Lx band. TADIL J is interoperable with NATO Link 16.

(8) Joint Multi TADIL Operating Procedures are currently undergoing a rewrite. The existing four Joint Publications will be replaced by CJCSM 6120.01 with anticipated distribution in late FY96.

3.5.7.1.2 Alternative specifications. No other specifications are available.

3.5.7.1.3 Standards deficiencies. These standards have no known deficiencies. Since these standards are configuration managed, any desired or required changes to them must be approved through a formal configuration process and approved by a configuration control board (CCB).

3.5.7.1.4 Portability caveats. Portability caveats are not applicable to these systems.

3.5.7.1.5 Related standards. No standards are related to these tactical, preformatted military messages.

3.5.7.1.6 Recommendations. Any program manager considering using one of the above standards should contact JIEO, Code JEBC, for additional information. These standards are not subject to tailoring.

3.5.7.2 Tactical communications. Tactical communication is a method or means of conveying information of any kind, especially orders and decisions from one command, person, or place to another within the tactical forces, normally by means of electronic equipment (including communications security equipment).

A tactical communication system is a system configured by various types of fixed-size, self-contained assemblages; switching, transmission, and terminal equipment; and interconnect and control facilities used within or in support of tactical military forces. The system provides securable voice and data communications among mobile users to facilitate command and control.

3.5.7.2.1 Standards. Table 3.5-43 presents standards for tactical communications.

TABLE 3.5-43 Tactical communications standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Tactical Communication Protocol 2 (TACO2) for the National Imagery Transmission Format Standard (NITFS)	MIL-STD-2045-44500 of 6/18/1993	Mandated (Approved)
GPC	DOD	Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, July 27, 1995	MIL-STD-188-220A	Mandated (Approved)
GPC	DOD	Interoperability and Performance Standards for Tactical Digital Information Link (TADIL) C (NOTE 5)	MIL-STD-188-203-3 of 10/5/88	Informational (Approved)
GPC	DOD	Interoperability and Performance Standards for Tactical Digital Information Link (TADIL) A (NOTE 3)	MIL-STD-188-203A-1 of 1/8/1988	Informational (Approved)
GPC	DOD	Interoperability and Performance Standards for Tactical Digital Information Link (TADIL) B (NOTE 4)	MIL-STD-188-212 of 10/17/1992	Informational (Approved)
GPC	DOD	Transport Profile: Reliable End System Transport for DOD Communications	MIL-STD-2045-14500 Part 1:March 1994	Informational (Approved)
GPC	DOD	SIMPLEX Transport Profile: CLTS over CLNS	MIL-STD-2045-14501	Informational (Approved)
GPC	DOD	Common Messaging	MIL-STD-2045-17501	Informational (Approved)
GPC	DOD	Military Messaging	MIL-STD-2045-17502	Informational (Approved)
GPC	DOD	DoD Standardized Profiles - File Transfer, Access and Management (FTAM) - Parts 1,4, and 5 (References ISO 8571 parts 1-5)	MIL-STD-2045-17508 - Parts 1,4, and 5; 7/94	Informational (Approved)
GPC	DOD	National Imagery Transmission Format Standard (NITFS)	NITFS V.1.1	Informational (Superseded)

NITF standards are mandatory for secondary imagery systems.

3.5.7.2.2 Alternative specifications. The following specifications are also available:

a. ISO 8802/3 (same as IEEE 802.3)

b. ITU-T I.441: Integrated Services Digital Network (ISDN) User Network Interface, LAP-D Data Link Layer specification

3.5.7.2.3 Standards deficiencies. The Tactical Communication Protocol-2 (TACO2) protocols perform well in half-duplex mode using low-speed and/or dedicated resources and circuits that have long turnaround times. This limits them to tactical environments that often have these features. But the TACO2 protocols are not a substitute for high-level packet switching protocols typically found in networked environments. FED-STD-1037B defines point-to-point transmission (i.e., transmission between two designated stations). X.25 also supports point-to-point transmission.

3.5.7.2.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.5.7.2.5 Related standards. The following standards are related to tactical communications or tactical communications standards:

a. ISO/IEC International Standardized Profile (ISP) 10607: Information Technology - ISP - FTAM Protocol

b. ISO 8571-5: FTAM Protocol Implementation Conformance Statement (PICS)

c. ISO/IEC ISP 10611 (Draft): Information Technology ISP - Message Handling System Comm Messaging

d. MIL-HDBK-1300A, NITFS

e. MIL-STD-2500A, NITF Version 2.0 for the NITFS

3.5.7.2.6 Recommendations. MIL-STD-2045-44500 is recommended. When specifying communication products to be used in the tactical environment, procurements should require products that support a commercially available communication protocol that performs file transfers and/or message transfers with a variety of systems, rather than developing a unique capability specific to a site.

3.5.8 Compression. These standards specify algorithms for compressing data for storage and exchange over a network. Data compression can reduce communications loading by as much as 80 percent without affecting the form of transmitted data. Compression requires application of the same algorithms at the sending and receiving locations. Compression algorithms for data must be "lossless" so that the expanded output exactly matches the original input. Compression algorithms for images and audio may be "lossy," where some data may be lost, but the expanded output is not noticeably different from the original input.

3.5.8.1 Text and data compression. This service supports general purpose compression of any data, including text files, data files, and executable programs. For these applications, the compression must be "lossless."

3.5.8.1.1 Standards. Table 3.5-44 presents standards for text and data compression.

TABLE 3.5-44 Text and data compression standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Single UNIX Specification (Spec. 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C436 (9/94)	Adopted (Approved)
IPC	ISO/IEC	Data Compression for Information Interchange - Adaptive Coding with Embedded Dictionary - DCLZ Algorithm	11558:1992	Informational (Approved)
IPC	ISO/IEC	Procedure for the Registration of Algorithms for the Lossless Compression of Data	11576:1994	Informational (Approved)
IPC	ISO/IEC	Data Compression for Information Interchange - Binary Arithmetic Coding Algorithm	12042:1993	Informational (Approved)
NPC	ANSI	Compaction Algorithm - Binary Arithmetic Coding	X3.225	Informational (Approved)
IPC	ECMA	Data Compression for Information Interchange - Adaptive Coding with Embedded Dictionary - DCLZ Algorithm	151 (1991)	Informational (Approved)
IPC	ECMA	Data Compression for Information Interchange - Binary Arithmetic Coding Algorithm	159 (1991)	Informational (Approved)
IPC	ECMA	Adaptive Lossless Data Compression Algorithm	222 (1995)	Informational (Approved)

Huffman coding is a statistical data compression technique that substitutes bit strings for character strings based on the frequency distribution of their occurrence. Strings that occur more frequently are replaced by shorter strings. Huffman coding is optimal when all symbol probabilities are an integral power of 1/2, which rarely occurs.

Arithmetic coding uses a similar technique for coding character strings based on their frequency of occurrence, and can achieve very close to the theoretical maximum reduction in message size. However, it can consume large amounts of computing resources in terms of CPU power and memory.

Substitutional compressors replace an occurrence of a particular phrase or group of bytes in a piece of data with a reference to a previous occurrence of that phrase. There are two main classes of schemes, named after Jakob Ziv and Abraham Lempel, who first proposed them in 1977 and 1978. The LZ78 based schemes work by entering phrases into a dictionary, and replacing repeat occurrences with an index into the dictionary. The most well known of the Lempel-Ziv algorithms is Terry Welch's LZW scheme, which he designed in 1984.

A second Lempel-Ziv compression scheme, called LZ77, keeps track of the last N bytes of data seen, and when a repeated phrase is encountered they output a pair of values corresponding to the position of the phrase in the buffer and the length of the phrase. In effect, the compressor moves a fixed-size "window" over the data.

(Note: Much of the material in this section was derived form the Frequently Asked Questions (FAQ) in the Usenet newsgroup comp.compression. This file can be found on the World Wide Web at http://www.cis.ohio-state.edu/hypertext/faq/usenet/compression-faq/top.html.)

ISO 11558 describes an LZ78 algorithm, while ISO 12042 and ANSI X3.225 describe arithmetic coding algorithms. The "compress" utility uses the LZW algorithm. The "pack" utility uses static Huffman coding. The "zip" utility and the compatible MS-DOS product PKZIP use LZ77 compression followed by static Huffman coding of the result. The "gzip" utility uses a similar scheme. In addition, the "gunzip" utility can uncompress files created by "gzip", "zip" "compress", or "pack."

3.5.8.1.2 Alternative specifications. The following specifications are also available:

a. Utah Run Length Encoding (RLE): University of Utah.
b. IFF : Electronic Arts.
c. Sun Rasterfile: Sun Microsystems.
d. Other proprietary specifications such as ARC, AR7, ARJ, LZH, PAK, and ZOO.
e. GNU data compression utilities: (gzip) Free Software Foundation.
f. ZIP, version 2.0.1

3.5.8.1.3 Standards deficiencies. None of the ISO standards have been implemented in products.

The Arithmetic algorithms use excessive amounts of computer resources, and therefore have not been implemented in any widely-used products or utilities.

The LZ78 schemes can require more memory than LZ77 schemes, which require only a fixed buffer.

Huffman coding schemes, such as used in "pack," are not as efficient as Lempel-Ziv coding. Huffman coding requires that a substitution table be transferred before the compressed data so that the receiving end can do the decompression. This adds overhead, particularly for short files. An alternative is to use a fixed substitution table, perhaps based on the frequency of English letters, but this is inefficient for non-text files. In contrast, the Lempel-Ziv substitution algorithms

allow the receiver to decompress the output without receiving any advance overhead tables. The dictionary, if used, can be constructed "on the fly" from the received data stream.

Several Arithmetic and Lempel-Ziv schemes are covered by multiple, overlapping patents. Of note, the LZW scheme, used in UNIX "compress," CompuServe GIF graphics compression, and the V.42bis modem standard, is covered by patents owned by IBM and Unisys. The developer of the PKZIP product owns the patent for one LZ77 scheme. Several Arithmetic schemes are covered by IBM patents, including the scheme used in JPEG image compression. Most of these patents cover algorithm implementations rather than the output format.

3.5.8.1.4 Portability caveats. Although many compression utilities use the same basic algorithms, individual manufacturers, software developers, and computer services have adopted their own options and internal storage formats. This has led to many different specifications that have incompatibilities. A unifying standard is needed.

3.5.8.1.5 Related standards. The following standards are related to text and data compression:

a. ITU-T T.81, Joint Photographic Expert Group (JPEG) standard

b. FIPS 170:1992, Data Compression in Modems Employing CCITT Recommendation V.42 Error Correction.

3.5.8.1.6 Recommendations. X/Open C436 "compress" and "uncompress" are recommended. These utilities are provided with almost all UNIX implementations, and are readily available for other platforms. The "pack" and "unpack" utilities were recommended, and are still included in the X/Open C436 specification, but X/Open plans to remove them in a future version. Systems using "pack" should migrate to "compress."

The Free Software Foundation "gzip" is also recommended. It is widely available without charge for a variety of platforms. It has been specified for use as a standard for software distribution by several DOD software programs.

The zip file format is widely used, especially in MS-DOS environments. Only properly licensed copies of the PKZIP utility or the compatible "zip" utility should be used. Creators of compressed files to be exchanged between MS-DOS systems are encouraged to create "self-extracting" files that can be distributed and automatically decompressed on other MS-DOS systems without license restrictions.

3.5.8.2 Still image compression. (This BSA appears in part 5, Data Interchange, and part 6, Graphics.) Still image compression standards provide the capability of reducing storage needed for raster graphics files. This compression can be either exact (loss-less) or approximate (lossy) upon reversal, depending upon the algorithm. The JPEG is interested in developing standards covering compression and decompression of still-frame, continuous tone, photographic (gray scale or color) digitized images by facsimile.

3.5.8.2.1 Standards. Table 3.5-45 presents standards for still image compression.

TABLE 3.5-45 Still image compression standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Digital Compression and Coding of Continuous - Tone Still Images, Part 1: Requirements and Guidelines (as profiled by MIL-STD-188-198A - JPEG)	10918-1:1994	Mandated (Approved)
GPC	DOD	Bi-Level Image Compression for the National Imagery Transmission Format Standards (NITFS)	MIL-STD-188-196 of 6/18/1993	Mandated (Approved)
GPC	DOD	Vector Quantization (VQ) Decompression for the NITFS	MIL-STD-188-199 of 6/27/1994	Mandated (Approved)
GPC	NIST	Group 3 Facsimile Apparatus for Document Transmission	FIPS PUB 147:1981	Informational (Approved)
GPC	NIST	Procedures for Document Facsimile Transmission (Adopts EIA-RS-466)	FIPS PUB 148:1982	Informational (Approved)
GPC	NIST	General Aspects of Group 4 Facsimile Apparatus (Adopts EIA-536-1988)	FIPS PUB 149:1988	Informational (Approved)
GPC	NIST	Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus (Adopts EIA 538-1988)	FIPS PUB 150:1988	Informational (Approved)
IPC	ITU-T	Standardization of Group 3 Facsimile Apparatus for Document Transmission: Terminal Equipment and Protocols for Telematic Services	T.4 (1993)	Informational (Approved)
IPC	ITU-T	Fax Coding Schemes & Coding Control Functions for Group 4 Fax Apparatus - Terminal Equipment & Protocols for Telematic Services	T.6 (1989)	Informational (Approved)
IPC	ITU-T	Digital Compression and Coding of Continuous - Tone Still Images - Requirements and Guidelines - Terminal Equipment and Protocols for Telematic Services	T.81 (1993)	Informational (Approved)
IPC	ISO/IEC	Digital Compression and Coding of Continuous-Tone Still Images - Part 2: Compliance Testing	10918-2:1993	Informational (Approved)
IPC	ISO/IEC	Progressive Bi-Level Image Compression (JBIG) Compression Algorithm for Black-and-White Images	11544 (Corrigendum 1):1995	Informational (Approved)
IPC	ISO/IEC	Data Compression for Information Interchange - Adaptive Coding with Embedded Dictionary - DCLZ Algorithm	11558:1992	Informational (Approved)
IPC	ISO/IEC	Procedure for the Registration of Algorithms for the Lossless Compression of Data	11576:1994	Informational (Approved)
IPC	ISO/IEC	Data Compression for Information Interchange - Binary Arithmetic Coding Algorithm	12042:1993	Informational (Approved)
IPC	ITU-T	Common Components for Image Compression and Communication - Basic Principles - Terminal Equipment and Protocols for Telematic Services	T.80 (1992)	Informational (Approved)
IPC	ITU-T	Coded Representation of Picture and Audio Information - Progressive Bi-Level Image Compression - Terminal Equipment and Protocols for Telematic Services	T.82 (1993)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-PRF-28002	Informational (Approved)
GPC	DOD	Adaptive Recursive Interpolated Differential Pulse Code Modulation (ARIDPCM) for the National Imagery Transmission Format Standards (NITFS)	MIL-STD-188-197A of 10/12/1994	Informational (Approved)
NPC	ANSI	Compaction Algorithm - Binary Arithmetic Coding	X3.225	Informational (Approved)
IPC	ISO/IEC	Digital Compression and Coding of Continuous-Tone Still Images - Part 3: Extensions	10918-3:1995	Informational (Draft)
IPC	ISO/IEC	Digital Compression and Coding of Continuous-Tone Still Images - Registration Procedures for JPEG profile, APPn marker, and SPIFF profile ID marker	10918-4:1996	Informational (Draft)
IPC	ISO/IEC	Coding of Moving Pictures and Associated Audio for Digital Storage Media up to about 1.5 Mbit/sec (MPEG 1), Part 5: Technical Report on Software for ISO/IEC 11172:1993	11172-5	Informational (Draft)
IPC	ISO/IEC	Generic Moding of Moving Pictures and Associated Audio Information (MPEG2) Part 4: Compliance Testing	13818-4	Emerging (Draft)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-R-28002B(1) of 9/20/1993	Informational (Superseded)

NITF standards are mandatory for Secondary Imaging Systems.

3.5.8.2.2 Alternative specifications. The following compression methods are also available:

a. LZW compression algorithm.
b. Fractal transforms.

3.5.8.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.8.2.4 Portability caveats. The DOD NITFS Adaptive Recursive Interpolated Differential Pulse Code Modulation (ARIDPCM) compression scheme for eight-bit gray scale images eventually will be replaced by the ISO/JPEG standard in the broader community, thereby providing the potential for incompatibilities with existing ARIDPCM-based systems. Fractal transforms are still in a preliminary stage and continue to present many problems.

Motion Pictures Expert Group (MPEG) is a joint development project of ISO and ITU-T. The same organization is responsible for the JPEG standard. Coordination of the standards in this area, ITU-T H.261, JPEG, and MPEG will depend on ISO and ITU-T.

3.5.8.2.5 Related standards. The following standards are related to non-text data compression standards:

a. MIL-HDBK-1300A, NITFS
b. MIL-STD-2500A, NITF Version 2.0 for the NITFS
c. Various multimedia standards

d. Raster graphics standards
e. ISO/IEC 11172, MPEG1
f. ISO/IEC 13818, MPEG2

3.5.8.2.6 Recommendations. The standards listed as mandated are recommended. If the DOD ARIDPCM compression scheme defined in the NITFS is specified in a procurement, a migration strategy to the ISO/ITU-T/JPEG standard also should be required. NITFS only supports ITU-T Group III compression, while CALS only supports Group IV.

Use the NITFS compression standards or CALS compression standard, as applicable. The MPEG and Joint Bi-Level Imaging Group (JBIG) standards should be considered for their specialized areas of use. The NIST and ITU-T standards for facsimile are recommended also. Lossless versus lossy compression: Group 4 facsimile is compatible with Group 3, but Group 3 facsimile is not necessarily compatible with Group 4. NITFS supports group 3, and CALS MIL-PRF-28002 supports group 4. If a file is compressed using group 4 facsimile, it will not be readable by a group 3 facsimile system, but a file compressed using group 3 facsimile will be readable by a group 4 facsimile system.

The JPEG standard can be implemented in hardware or software, and is already available in commercial products. However, sites purchasing JPEG products based on the draft versions of the standard should require vendor assurance that the products will comply with the international standard.

ITU-T H.261 is recommended for applications that require a 64-Kbit/second line rate. JPEG is recommended for still image applications when its data loss does not impact on the system function. MPEG is recommended for moving image applications when its elimination of redundant information between frames does not impact on the system function.

3.5.8.3 Motion image compression. Motion image compression standards deal with moving pictures coding and associated audio for digital storage media.

3.5.8.3.1 Standards. Table 3.5-46 presents standards for motion image compression.

TABLE 3.5-46 Motion image compression standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Coding of Moving Pictures and Associated Audio for Digital Storage Media up to about 1.5 Mbit/sec (MPEG 1), Part 1: Systems, Part 2: Video, Part 3: Audio (with Technical Corrigendum 1:1996)	11172-1,2,3:1993	Mandated (Approved)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG2), Part 1: Systems	13818-1:1996	Mandated (Approved)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG2), Part 2: Video	13818-2:1996	Mandated (Approved)
IPC	ISO/IEC	Coding of Moving Pictures and Associated Audio for Digital Storage Media up to about 1.5 Mbit/sec (MPEG 1), Part 4: Conformance Testing	11172-4: 1995	Informational (Approved)
IPC	ISO/IEC	Progressive Bi-Level Image Compression (JBIG) Compression Algorithm for Black-and-White Images	11544 (Corrigendum 1):1995	Informational (Approved)
IPC	ISO/IEC	Data Compression for Information Interchange - Adaptive Coding with Embedded Dictionary - DCLZ Algorithm	11558:1992	Informational (Approved)
IPC	ISO/IEC	Procedure for the Registration of Algorithms for the Lossless Compression of Data	11576:1994	Informational (Approved)
IPC	ISO/IEC	Data Compression for Information Interchange - Binary Arithmetic Coding Algorithm	12042:1993	Informational (Approved)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 9: Extension for Real Time Interface for Systems Decoders	13818-9:1996	Informational (Approved)
GPC	NIST	Video Teleconferencing Services at 56 to 1, 920 KB/s (adopts CCITT H.221, H.230, H.242, H.261, and H.320 (all 1990))	FIPS PUB 178:1992	Informational (Approved)
IPC	ITU-T	Frame Structure for a 64 to 1920 kbit/s Channel in Audiovisual Teleservices - Line Transmission of Non-Telephone Signals	H.221 (1993)	Informational (Approved)
IPC	ITU-T	Frame-Synchronous Control and Indication Services for Audiovisual Systems - Line Transmission of Non-Telephone Signals	H.230, Rev. 1 (1990)	Informational (Approved)
IPC	ITU-T	System for Establishing Communication between Audiovisual Terminals Using Digital Channels up to 2 Mbit/s	H.242 (1993)	Informational (Approved)
IPC	ITU-T	Video Codec for Audiovisual Services at p x 64 kbit/s - Line Transmission on Non-Telephone Signals (known as PX64)	H.261 (1993)	Informational (Approved)
IPC	ITU-T	Narrow-Band Visual Telephone Systems and Terminal Equipment - Line Transmission of Non-Telephone Signals	H.320 (1993)	Informational (Approved)
IPC	ITU-T	Common Components for Image Compression and Communication - Basic Principles - Terminal Equipment and Protocols for Telematic Services	T.80 (1992)	Informational (Approved)
IPC	ITU-T	Digital Compression and Coding of Continuous - Tone Still Images - Requirements and Guidelines - Terminal Equipment and Protocols for Telematic Services	T.81 (1993)	Informational (Approved)
IPC	ITU-T	Coded Representation of Picture and Audio Information - Progressive Bi-Level Image Compression - Terminal Equipment and Protocols for Telematic Services	T.82 (1993)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI	Compaction Algorithm - Binary Arithmetic Coding	X3.225	Informational (Approved)
IPC	ISO/IEC	Coded Representation of Multimedia and Hypermedia Information Objects (MHEG), Multimedia Synchronized and Hypermedia Objects	JTC1/Projects 29.06.01, 29.06.02 & 29.07 (SC29/WG12)	Informational (Formative)
NPC	ANSI	Digital Processing of Video Signals - Video Coder/Decoder for Audiovisual Services at 56 to 1,536 kbits	T1. 64	Informational (Draft)
IPC	ISO/IEC	Coding of Moving Pictures and Associated Audio for Digital Storage Media up to about 1.5 Mbit/sec (MPEG 1), Part 5: Technical Report on Software for ISO/IEC 11172:1993	11172-5	Informational (Draft)
IPC	ISO/IEC	Generic Moding of Moving Pictures and Associated Audio Information (MPEG2) Part 4: Compliance Testing	13818-4	Emerging (Draft)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 5: Software Simulation	13818-5	Informational (Draft)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 6: Extensions for DSM-CC	13818-6	Informational (Draft)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 7: Audio Extensions	13818-7:1993	Informational (Draft)

3.5.8.3.2 Alternative specifications. The following specifications are also available:

a. Microsoft and Aldus: TIFF.
b. Apple: PICT Version 2.
c. Truevision, Inc.: TGA.
d. Sun Microsystems: Sun Rasterfile.
e. Intel, IBM, and AT&T: Digital Video Interactive (DVI).

3.5.8.3.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.8.3.4 Portability caveats. MPEG is a joint development project of ISO and ITU-T. The same organization is responsible for the JPEG standard. Coordination of the standards in this area, ITU-T H.261, JPEG, and MPEG will depend on ISO and ITU-T.

ISO/IEC 11172-1 addresses synchronization and multiplexing of multiple compressed audio and video bit streams. ISO/IEC 11172-2 addresses compression of video signals at 1.5 Mbits. ISO/IEC 11172-3 addresses compression of digital audio signals at rates of 64, 128, and 192 kbit/s per channel.

3.5.8.3.5 Related standards. The following specifications are related to motion image compression standards:

a. Other compression and graphics format standards.

3.5.8.3.6 Recommendations. MPEG is recommended for moving image applications when its elimination of redundant information between frames does not impact on the system function. Selection of the standard will depend on the type of video-still frames or full motion and the line rate for transmission. ITU-T H.261 is the international standard for video encoding and decoding at a 64-Kbit/second line rate. It is designed primarily for use in the ISDN and can operate over existing digital networks. MPEG compresses video using a process called intraframe encoding, and it loses some of the video during the encode-decode cycle. Compression ratios of up to 25 to 1 can be used without a noticeable loss of image quality. MPEG is designed specifically for video and takes an asymmetrical approach to compression, dividing the world of compressed videos into publishers-producers and consumers-viewers. MPEG uses interframe encoding to eliminate redundant information between frames. ITU-T H.261 is recommended for applications that a require a 64-Kbit/second line rate.

3.5.8.4 Audio compression. Audio compression standards deal with the special needs of audio data in compression.

3.5.8.4.1 Standards. Table 3.5-47 presents standards for audio compression.

TABLE 3.5-47 Audio compression standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part3:Audio	11172-3:1993	Mandated (Approved)
IPC	ISO/IEC	Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 3: Audio Technical Corrigendum	11172-3:1993/Cor.1:1995	Mandated (Approved)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 3: Audio	13818-3:1995 with Amd 1	Mandated (Approved)
IPC	ISO/IEC	Progressive Bi-Level Image Compression (JBIG) Compression Algorithm for Black-and-White Images	11544 (Corrigendum 1):1995	Informational (Approved)
IPC	ITU-T	Characteristics of Compandors for Telephony - General Characteristics of International Telephone Connections and Circuits	G.162 (1989)	Informational (Approved)
IPC	ITU-T	Characteristics of Syllabic Compandors for Telephony on High Capacity Long Distance Systems - General Characteristics of International Telephone Connections and Circuits	G.166 (1989)	Informational (Approved)
IPC	ISO/IEC	Generic Moding of Moving Pictures and Associated Audio Information (MPEG2) Part 4: Compliance Testing	13818-4	Emerging (Draft)

3.5.8.4.2 Alternative specifications. Refer to other compression BSAs for alternatives.

3.5.8.4.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.8.4.4 Portability caveats. Portability problems with the existing standards are unknown.

3.5.8.4.5 Related standards. Other compression standards are related.

3.5.8.4.6 Recommendations. The mandated standards are recommended.

3.5.9 Data interchange media. Data interchange media is a collection of service areas for physical media used for data interchange.

3.5.9.1 Read-only optical disks. These standards are for optical disks used for read-only data storage. Read-only disks are a growing means of distributing software.

3.5.9.1.1 Standards. Table 3.5-48 presents standards for read-only optical disks.

TABLE 3.5-48 Read-only optical disks standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Volume and File structure of CD-ROM for Information Interchange (same as ECMA 119)	9660:1988	Adopted (Approved)
IPC	ISO/IEC	90 mm Optical Disk Cartridges, Rewritable and Read Only, for Data Interchange (128MB) (see ECMA 154-1994)	10090:1992	Adopted (Approved)
IPC	ISO/IEC	Data Interchange on Read-Only 120mm Optical Data Disks (CD-ROM) (see ECMA 130-1988)	10149:1995	Adopted (Approved)
IPC	ISO/IEC	Data interchange on 130 mm optical disk cartridges - capacity 1,3 Gbytes per cartridge, CC Servo Format. (ECMA-184 and X3B11 Project 1001-L)	13549:1993	Adopted (Approved)
IPC	ISO/IEC	Information Technology 130 mm Optical Disk Cartridges Capacity: 2 Gbytes per Cartridge For Information Interchange. (ECMA 195-1993)	13842:1995	Adopted (Approved)
IPC	ECMA	Volume and File Structure of CD-ROM for Information Interchange	119 (1987)	Informational (Approved)
IPC	ECMA	Data Interchange on Read-Only 120 mm Optical Data Disks (CD-ROM)	130 (1988)	Informational (Approved)
IPC	ECMA	Data Interchange on 90 mm Optical Disk Cartridges, Read Only and Rewritable, M.O.	154 (1991)	Informational (Approved)
IPC	ECMA	Volume and File Structure of Read-Only and Write-Once Compact Disk Media for Information Interchange	168 (1994)	Informational (Approved)
IPC	ECMA	Data Interchange on 130 mm Optical Disk Cartridges - Capacity: 1,3 Gigabytes per Cartridge	184 (1992)	Informational (Approved)
IPC	ECMA	Data Interchange on 130mm Optical Disk Cartridges - Capacity: 2 GigaBytes per Cartridge	195 (1995)	Informational (Approved)
IPC	ECMA	Data Interchange on 90mm Optical Disk Cartridge - HS-1 Format - Capacity: 650 Megabytes per Cartridge (ISO/IEC DIS 15498)	239 (1996)	Informational (Approved)
IPC	ECMA	Data Interchange on 120mm Optical Disk Cartridges using Phase Change PD Format - Capacity:650 Mbytes per Cartridge	240 (1996)	Informational (Approved)
NPC	ANSI	86mm, 90mm case, Rewritable and Read Only Optical Disk Cartridge Using the Discrete Block Format (DBF) Method for Digital Information Interchange (113MB)	X3.213-1994	Informational (Approved)
NPC	ANSI	Test Methods for Media Characteristics of 90mm (3.5") Rewritable/Read-Only Optical Digital Data Disks with Continuous Composite Servo (CCS)	X3.244-1995	Informational (Approved)
NPC	ANSI	Test Methods for Media Characteristics of 90 mm Read Only and Rewritable M.O. Optical Disk Data Storage Cartridges with Discrete Block Format (DBF)	X3.246-1994	Informational (Approved)
CPC	Various	Digital Video Disk (DVD)	DVD	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Volume and File Structure of Read-Only and Write-Once Compact Disc Media for Information Interchange (This is ECMA-168.)	13490:1995	Informational (Draft (DIS))
IPC	ISO/IEC	Procedures for the Registration of Identifiers and Attributes for Volume and File Structure	13800:1994	Informational (Draft)
IPC	ISO/IEC	Information Interchange for 130mm Optical Disk Cartridges, Capacity: 2.6 Gigabytes Per Cartridge, Rewritable and Read-Only, MO, 1,7 Modulation ZCAV (mixed mode media)	14517	Informational (Draft)
IPC	ISO/IEC	Data Interchange on 90 mm Optical Disk Cartridges (640 MB, MO, includes DOW)	15041	Informational (Draft)
IPC	ISO/IEC	Information Interchange on 90mm Overwritable and Read Only Optical Disk Cartridges Using Phase Change, Capacity:1,3 Gbytes per Cartridge (ANSI X3B11 Project 1159-D)	14760	Informational (Formative)
NPC	ANSI	130mm Optical Disk Cartridges, Rewritable and WORM Using Phase Change Technology and Embossed Read-Only for Information Interchange (2GB)	X3.281	Informational (Draft (Work Suspended))

3.5.9.1.2 Alternative specifications. No other consortia or de facto specifications are available.

3.5.9.1.3 Standards deficiencies. It is doubtful there will be support for discrete Block Format (ANSI X3.213-1994 and ANSI X3.246-1994) in the future. Other deficiencies in the existing standards are unknown.

3.5.9.1.4 Portability caveats. The following portability problems have been identified:

a. ISO/IEC 9660 covers the logical format that makes a Compact Disc readable (see also the "Yellow Book"). ISO/IEC 9660 is being revised by Japan's National Body. ISO/IEC 10149 covers the physical characteristics of a Compact Disc (see also the "Red Book").

b. ISO/IEC DIS 13490 (also known as The Frankfurt Proposal) removes many ISO/IEC 9660 restrictions, but is compatible with ISO/IEC 9660 at the directory and file structure level. DIS 13490 includes directory information required to support Unix, supports ISO 10646 (a new standard supporting all the character sets of the world), and is extendible to support future file systems, like Windows NT. It also addresses the logical structure of data on a Compact Disc - Write Once (CD-WO, Orange Book - Part 2) disc, and is designed to support both the CD-ROM (Yellow Book) and CD-WO conforming media. DIS 13490 has been accepted by ECMA, under ECMA 168 CD-WO. (Note: ECMA 168 will be used for the future CD-E (Compact Disc-Erasable)).

c. ISO/IEC 13549:1993 introduced the concept of "mixed mode" media; i.e., can combine read-only, write once, and rewrite functionality on the same disk.

d. ISO/IEC 13842:1994 allows for a reverse spiral on Side B; allowing for both sides to be read or written to simultaneously.

e. ISO/IEC DIS 13800 is being designed to be used with ISO DIS 13490.

f. ANSI is recommending cancellation of X3.281. There is little or no industry interest in continuing work on this standard. Products conforming to an approved 2GB Magneto-optic cartridge already exist in the marketplace, and the active work being done by X3B11 is for higher capacity.

g. Trends in read-only optical disk standards are for higher capacities and performance, and alternate technologies. The read-only version of high density CDs (Digital Video Disc-Read Only (DVD-RO)) have a capacity of 4.7 GB. DVDs store information in data sectors, instead of along a spiral as in the original Red Book audio. All versions of DVD (read-only, rewrite, erasable, video and games) will share a common file format, a subset of the Optical Storage Technology Association (OSTA) Universal Disk Format (UDF).

3.5.9.1.5 Related standards. The following standards are related to read-only optical disks:

a. Red Book - The standards for CD-Digital Audio, developed by Philips and Sony, are defined in the "Red Book."

b. Yellow Book - The standards for CD-ROM, developed by Philips and Sony and the standards for CD-ROM/ Extended Architecture (XA) developed by Sony, Philips, and Microsoft are defined in the "Yellow Book." This document defines the physical properties of the disc, how data is stored and indexed, and how errors are corrected.

c. Orange Book - The standards for CD-Recordable (CD-R), developed by Philips and Sony, are defined in the "Orange Book." This document standardizes the physical media into two modes: Part 1 describes CD-Magneto-Optical (MO) and part 2 describes CD-WO. The Orange Book specifications refer to the physical standard, while ISO/IEC DIS 13490 refers to the logical structure of data on a CD-WO disk.

d. Green Book - The standards for CD-Interactive (CD-I), developed by Philips and Sony, are defined in the "Green Book." The Green Book not only covers the CD-I disc format, it also defines the hardware specifics of the player as well, including the CPU memory, operating system (CD-RTOS-Compact Disc Real-Time Operating System, based on OS-9, the official disk operating system of the Tandy Color Computer). The CD-I format synchronizes sound, video, graphics, and text so that they play together in a smooth, realistic way.

e. ISO/IEC 10646-1:1993 (amendments 1-5), Information Technology - Universal Multiple Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane. Standard adopted by The Frankfurt Group to enhance the Orange Book specifications. ISO/IEC 10646 is a standard for using the many character sets of the world.

3.5.9.1.6 Recommendations. ISO 9660 (Volume and file structure of CD-ROM) is the standard recommended for compact disc.

3.5.9.2 Write-once optical disks. These standards are for optical disks that a user uses to write data to disks, and allows read-only access to the recorded data.

3.5.9.2.1 Standards. Table 3.5-49 presents standards for write-once optical disks.

TABLE 3.5-49 Write-once optical disks standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	130mm (5.25') Optical Disk Cartridge - Write-Once, for Information Interchange - Part 1: Unrecorded Optical Disk Cartridge	9171-1:1990	Adopted (Approved)
IPC	ISO/IEC	130mm Optical Disk Cartridge, Write Once, for Information Interchange - Part 2: Recording format. Format A - Continuous Composite (CC) (ISO/IEC version of ANSI X3.211) Format B - Sampled Servo (SS) (ISO/IEC version of ANSI X3.214)	9171-2:1990	Adopted (Approved)
IPC	ISO/IEC	356mm Optical Disk Cartridge for information interchange - Write Once (ISO/IEC version of ANSI X3.200-1992.)	10885:1993	Adopted (Approved)
IPC	ISO/IEC	Digital Information Interchange on 130mm Optical Disk Cartridges of the Write Once, Read Multiple (WORM) Type, Using the Magneto-Optical Effect. (ECMA-153 JUN 1991, ISO/IEC version of ANSI X3.220.)	11560:1992	Adopted (Approved)
IPC	ISO/IEC	Volume and File Structure of Write-Once and Rewritable Media Using Non-Sequential Recording for Information Interchange. (ECMA 167)	13346:1995	Adopted (Approved)
IPC	ISO/IEC	Information Technology - Information Interchange on 300 mm Optical Disk Cartridges of the Write Once, Read Multiple (WORM) Type using the CCS Method. (ECMA 190)	13403:1995	Adopted (Approved)
IPC	ISO/IEC	Data interchange on 130 mm optical disk cartridges - capacity 1 Gbytes per cartridge, CC Servo Format. (ECMA-183 and X3B11 Project 1000-L.)	13481:1993	Adopted (Approved)
IPC	ISO/IEC	Data interchange on 130 mm optical disk cartridges - capacity 1.3 Gbytes per cartridge, CC Servo Format. (ECMA-184 and X3B11 Project 1001-L)	13549:1993	Adopted (Approved)
IPC	ISO/IEC	Information Technology - Information Interchange on 300 mm Optical Disk Cartridges of the Write Once, Read Multiple (WORM) Type using the SSF Method. (ECMA 189)	13614:1995	Adopted (Approved)
NPC	ANSI	356mm (14.00 inch) WORM Optical Disk Cartridge, Parts 1 and 2	X3.200-1992	Adopted (Approved)
NPC	ANSI	130mm (5.25') Write-Once Optical Disk Cartridge Using Continuous Servo RLL 2,7 Encoding and LCD	X3.211-1992	Adopted (Approved)
NPC	ANSI	130mm Write-Once Optical Disk Cartridge Using Sampled Servo and 4/15 Encoding	X3.214-1992	Adopted (Approved)
NPC	ANSI	130mm Optical Disk Cartridge of the Write-Once Read Multiple (WORM) type Using the Magneto-Optical Effect	X3.220-1992	Adopted (Approved)
NPC	ANSI	Recorded Optical Media Unit for Digital Information Interchange -130mm (5.25') Write Once Sampled Servo RZ Selectable Pitch Optical Disk Cartridge	X3.191-1991	Informational (Approved (Declining))
NPC	ANSI	356 mm (14") Optical Disk Cartridge (Write-Once) Test Methods for Media Characteristics	X3.199-1991	Informational (Approved)
IPC	ECMA	Volume and File Structure of Read-Only and Write-Once Compact Disk Media for Information Interchange	168 (1994)	Informational (Approved)
IPC	ECMA	Data Interchange on 130mm Optical Disk Cartridges of Type WORM (Write Once Read Many) using irreversible effects - Capacity: 2,6 Gbytes per cartridge (ISO/IEC DIS	238 (1996)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
		15486)		
IPC	ECMA	Data Interchange on 120mm Optical Disk Cartridges using Phase Change PD Format - Capacity:650 Mbytes per Cartridge	240 (1996)	Informational (Approved)
IPC	ISO/IEC	Volume and File Structure of Read-Only and Write-Once Compact Disc Media for Information Interchange (This is ECMA-168.)	13490:1995	Informational (Draft (DIS))
IPC	ISO/IEC	Procedures for the Registration of Identifiers and Attributes for Volume and File Structure	13800:1994	Informational (Draft)
IPC	ISO/IEC	Information Interchange for 130mm Optical Disk Cartridges, Capacity: 2.6 Gigabytes Per Cartridge, Rewritable and Read-Only, MO, 1,7 Modulation ZCAV (mixed mode media)	14517	Informational (Draft)
NPC	ANSI	130mm Optical Disk Cartridges, Rewritable and WORM Using Phase Change Technology and Embossed Read-Only for Information Interchange (2GB)	X3.281	Informational (Draft (Work Suspended))
NPC	ANSI	356 mm Optical Disk Cartridge, Extended Capacity, Using Phase Change Technology, For Information Interchange (Phase Change - Write Once Read Many, PC-WORM)	X3B11 Project 1029-D	Informational (Formative)
CPN-C	Toshiba	Digital Video Disk-Recordable (DVD-R) (3.9GB)	DVD-R	Informational (Formative)

3.5.9.2.2 Alternative specifications. No other consortia or de facto specifications are available.

3.5.9.2.3 Standards deficiencies. Data interchange through physical distribution of optical disks cannot be assured with write-once technology. ISO/IEC 9171 (130mm) allows for two incompatible format types, continuous composite servo (CCS-Format A), and sampled servo format (SS or SSF-Format B). A CCS disk cannot be exchanged with an SS disk nor can it be read by an SS optical drive. Because of this ANSI established two separate standards; X3.211 for Format A, and X3.214 for Format B. If system requirements demand the interchangeability of the physical disk, specify the appropriate ANSI standard. There are currently no commercial manufacturers producing 300mm (12") write-once optical disks that conform to either of the two newly ISO adopted standards, ISO 13403:1995 or ISO 13614:1995.

ANSI X3B11 recommended reaffirmation of X3.199:1991 during its five-year review; however, drives are no longer being manufactured, and this standard should be considered declining.

3.5.9.2.4 Portability caveats. The following portability problems have been identified:

a. A standard technique for write-once optical disks should be selected for use throughout the DOD and applied wherever possible.

b. ISO/IEC 13346:1995 is a new file system standard developed through ANSI, ECMA, and ISO. It supports both write-once and rewritable functionality and allows for unlimited file and volume sizes. It is also operating system independent.

c. ISO/IEC 13403:1995 and ISO/IEC 13614:1995 (300mm, 12") both have the potential for a 12GB total capacity.

d. Standards for 130mm optical cartridges, ANSI X3.211, ANSI X3.214, ISO/IEC 9171, and ISO/IEC 11560, all specify a storage capacity of 325MB per side (650MB total).

e. A new ANSI project has been approved (Project 1158-D) to develop the standards for 130mm Rewritable and Read-Only Optical Disk Cartridge, Capacity: 5.2 GB per Cartridge (8X), for Information Interchange. An "I" status (International) is being requested so that ANSI and ISO efforts will work in parallel. The new standard will likely provide backward read and write compatibility with ISO/IEC DIS 14517 (2.6GB), and read compatibility (at a minimum) with ISO/IEC 13549 (1.3GB), and ISO/IEC 10089 (650MB). Backward compatibility to ISO/IEC 13842 (2GB) is not expected to be included in the proposed standard. Project 1158-D also allows for three sector sizes, 512, 1024, and 2048 bytes per sector.

f. ANSI X3.191 specifies a storage capacity of 1.28GB for a double sided disk. The cartridge dimensions of ANSI X3.191 are different from those of other 130mm Write-Once Read Many (WORM) standards, and optical drives are no longer being produced. Although this standard has been reaffirmed during its five-year review, optical drives are no longer being produced, and it should be considered declining.

g. ANSI X3B11 Project 1029-D, second generation 356mm (14") media standard, will include both 14.8 and 25GB capacities and will include backward read compatibility to ISO/IEC 10885 (6.8GB). ISO 10885 is expected to be reaffirmed at its upcoming five-year review.

h. ANSI X3.281 (X3B11 Project 985-D) uses zone bit recording (ZBR) to achieve its capacity of 2.0GB per double sided cartridge. Due to lack of industry interest, ANSI is recommending cancellation of this standard.

i. There are two ISO write-once standards for the 12" (300mm) optical disk; ISO 13403:1995 specifies the CCS format method and ISO 13614:1995 specifies the SS.

j. ECMA has approved its own version of a 130mm write-once media type based on that described in ISO/IEC DIS 14517 (ECMA 238 (1996)) and has submitted it through the Fast Track procedures as ISO/IEC DIS 15486.

3.5.9.2.5 Related standards. The following standards, proposed standards, and technical reports are related to write-once optical disk standards:

a. ISO/IEC TR 13841:1995 - Information Technology - Guidance on Measurement Techniques for 90mm Optical Disk Cartridges.

b. ISO/IEC TR 10091: Information Technology - Technical aspects of 130mm Optical disk cartridges - Write-once Recording Formats. (Technical Report, complement to ISO/IEC 9171-2 for the Type A and B formats.)

c. AIIM TR 21-1991 - Recommendations for the Identifying Information to be Placed on Write-Once-Read-Many (WORM) and Rewritable Optical Disk (OD) Cartridge Label(s) and Optical Disk Cartridge Packaging (Shipping Containers)

d. AIIM TR 28-1991 - Expungement of Information Recorded on Optical WORM Systems.

e. A new ANSI project has been approved (Project 1158-D) to develop the standards for 130mm Rewritable and Read-Only Optical Disk Cartridge, Capacity: 5.2 GB per Cartridge (8X), for Information Interchange. An "I" status (International) is being requested so that ANSI and ISO efforts will work in parallel. This standard will likely provide backward read and write compatibility with ISO/IEC DIS 14517 (2.6GB), and read compatibility (at a minimum) with ISO/IEC 13549 (1.3GB), and ISO/IEC 10089 (650MB). Backward compatibility to ISO/IEC 13842 (2GB) is not expected to be included in the proposed standard.

3.5.9.2.6 Recommendations. The recommendation is to apply the standards shown above as "adopted" that may suit to the circumstances of data communication in the system.

3.5.9.3 Rewritable optical disks. These standards are for optical disks that allow the user to read, write, and change data.

3.5.9.3.1 Standards. Table 3.5-50 presents standards for rewritable optical disks.

TABLE 3.5-50 Rewritable optical disks standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	130mm Rewritable Optical Disk Cartridge for Information Interchange. (ISO/IEC version of ANSI X3.212)	10089:1991	Adopted (Approved)
IPC	ISO/IEC	90mm optical disk cartridges, rewritable and read only, for data interchange. (Same as ECMA-154)	10090:1992	Adopted (Approved)
IPC	ISO/IEC	Volume and File Structure of Write-Once and Rewritable Media Using Non-Sequential Recording for Information Interchange. (ECMA 167)	13346:1995	Adopted (Approved)
IPC	ISO/IEC	Data interchange on 130 mm optical disk cartridges - capacity 1 Gbytes per cartridge, CC Servo Format. (ECMA-183 and X3B11 Project 1000-L.)	13481:1993	Adopted (Approved)
IPC	ISO/IEC	Data interchange on 130 mm optical disk cartridges - capacity 1.3 Gbytes per cartridge, CC Servo Format. (ECMA-184 and X3B11 Project 1001-L)	13549:1993	Adopted (Approved)
IPC	ISO/IEC	Information Technology 130 mm Optical Disk Cartridgee Capacity: 2 Gbytes per Cartridge For Information Interchange. (ECMA 195-1993)	13842:1995	Adopted (Approved)
IPC	ISO/IEC	Data Interchange on 90 mm Optical Disk Cartridges - Capacity: 230 MB per cartridge (ECMA 201)	13963:1995	Adopted (Approved)
NPC	ANSI	130mm Rewritable Optical Disk Cartridge Using Magneto-Optical Effect and Continuous Composite Servo Format	X3.212-1992	Adopted (Approved)
IPC	ECMA	Data Interchange on 90 mm Optical Disk Cartridges - Capacity: 385 MBytes per Cartridge	223 (1995)	Informational (Approved)
IPC	ECMA	Data Interchange on 90mm Optical Disk Cartridge - HS-1 Format - Capacity: 650 Megabytes per Cartridge (ISO/IEC DIS 15498)	239 (1996)	Informational (Approved)
IPC	ECMA	Data Interchange on 120mm Optical Disk Cartridges using Phase Change PD Format - Capacity:650 Mbytes per Cartridge	240 (1996)	Informational (Approved)
NPC	ANSI	86mm, 90mm case, Rewritable and Read Only Optical Disk Cartridge Using the Discrete Block Format (DBF) Method for Digital Information Interchange (113MB)	X3.213-1994	Informational (Approved)
NPC	ANSI	Test Methods for Media Characteristics of 130 mm Rewritable Optical Disk Data Storage Cartridges with Continuous Composite Servo (CCS)	X3.234-1993	Informational (Approved)
NPC	ANSI	Test Methods for Media Characteristics of 90mm (3.5") Rewritable/Read-Only Optical Digital Data Disks with Continuous Composite Servo (CCS)	X3.244-1995	Informational (Approved)
NPC	ANSI	Test Methods for Media Characteristics of 90 mm Read Only and Rewritable M.O. Optical Disk Data Storage Cartridges with Discrete Block Format (DBF)	X3.246-1994	Informational (Approved)
IPC	ISO/IEC	Data Interchange on 90 mm Optical Disk Cartridges (640 MB, MO, includes DOW)	15041	Informational (Draft)
IPC	ISO/IEC	Information Interchange for 130mm Optical Disk Cartridges, Capacity: 2.6 Gigabytes Per Cartridge, Rewritable and Read-Only, MO, 1,7 Modulation ZCAV (mixed mode media)	14517	Informational (Draft)
IPC	ISO/IEC	Information Interchange on 90mm Overwritable and Read Only Optical Disk Cartridges Using Phase Change, Capacity:1,3 Gbytes per Cartridge (ANSI X3B11 Project 1159-I)	14760	Informational (Formative)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI	130mm Optical Disk Cartridges, Rewritable and WORM Using Phase Change Technology and Embossed Read-Only for Information Interchange (2GB)	X3.281	Informational (Draft (Work Suspended))
CPN-C	Toshiba	Digital Video Disc-Rewritable (DVD-RAM) (2.6GB)	DVD-RAM	Informational (Formative)

3.5.9.3.2 Alternative specifications. No other consortia or de facto specifications are available.

3.5.9.3.3 Standards deficiencies. It is doubtful there will be support for Discrete Block Format (X3.246-1994) in the future. ANSI is recommending cancellation of X3.281. There is little or no industry interest in continuing work on this standard. Products conforming to an approved 2GB magneto-optic cartridge already exist in the marketplace, and the active work being done by X3.B11 is for higher capacity.

3.5.9.3.4 Portability caveats. The following portability problems have been identified:

a. Data interchange through physical distribution of rewriteable optical disks is more standardized than with write-once, but still cannot be assured.

b. All single-sided 90mm (3.5 inch) rewritable optical disks use the CCS (Continuous Composite Servo) formatting. However, there are two methods for rewritability, magneto-optic (MO) which requires a separate erase pass before rewriting, and phase-change rewrite (PCR) which allows for direct overwrite. Two draft international standards, ISO/IEC DIS 14517 and ISO/IEC DIS 15041 both allow for Direct Overwrite (DOW).

c. ISO/IEC 10089:1991 has been reaffirmed by ANSI X3B11 technical committee as a valid standard during its five-year review.

d. ISO/IEC 13549:1993 introduced the concept of "mixed mode" media, i.e., read-only, write once, and rewrite functionality can be combined on the same disk.

e. A new ANSI project has been approved (Project 1158-D) to develop the standards for 130mm Rewritable and Read-Only Optical Disk Cartridge, Capacity: 5.2 GB per Cartridge (8X), for Information Interchange. An "I" status (International) is being requested so that ANSI and ISO efforts will work in parallel. This standard will likely provide backward read and write compatibility with ISO/IEC DIS 14517 (2.6GB), and read compatibility (at a minimum) with ISO/IEC 13549 (1.3GB), and ISO/IEC 10089 (650MB). Backward compatibility to ISO/IEC 13842 (2GB) is not expected to be included in the proposed standard.

f. ANSI X3 Project 915-I (ISO/IEC DIS 15041), Extended Capacity 90mm Rewritable Optical Media (640MB, 5X), should be able to read and write to 230MB (2X) disks (ISO/IEC 13963:1995).

g. Japanese manufacturers state they can produce a "bridge drive" which can accommodate both the 230MB 90mm Magneto-Optic and Phase Change Rewrite (PCR) optical disk cartridges; however, the 1.3GB PCR drive will not accommodate 230MB M disks.

h. A request has been made to make ECMA 195 compatible with ISO/IEC 13842:1995.

i. ANSI X3.213 and ISO/IEC 10090 specify a capacity of 128MB per side. ANSI X3.212,ISO/IEC 10089, and ISO/IEC DIS 15498 specify a capacity of 325 MB per side. ANSI X3B11 Project 915-I will specify a capacity of 640MB per cartridge.

j. A standard for a phase change multifunction dual drive (PD), which combines phase change rewritability (650MB capacity) with quad-speed CD-ROM read funtionality in a single unit has been approved through ECMA (ECMA 240 (1996).

k. Double sided 90mm optical disks are being proposed by industry, which will have capacities of 1.3GB and 2.6GB.

l. ISO/IEC 10089 allows for both CCS and SSF formats, which are incompatible with each other. An organization may have to use ANSI X3.212 to specify CCS only.

3.5.9.3.5 Related standards. The following standards, proposed standards, and technical reports are related to rewritable optical disks:

a. ISO/IEC TR13561:1994 Information Technology - Guidelines for Effective Use of ODCs Conforming to ISO/IEC 10090 First Edition.

b. ISO/IEC TR13841:1995 Information Technology - Guidance on Measurement Techniques for 90mm ODCs.

c. A new ANSI project has been approved (Project 1158-D) to develop the standards for 130mm Rewritable and Read-Only Optical Disk Cartridge, Capacity: 5.2GB per Cartridge (8X), for Information Interchange. An "I" status (International) is being requested so that ANSI and ISO efforts will work in parallel. This standard will likely provide backward read and write compatibility with ISO/IEC DIS 14517 (2.6GB), and read compatibility (at a minimum) with ISO/IEC 13549 (1.3GB),

and ISO/IEC 10089 (650MB). Backward compatibility to ISO/IEC 13842 (2GB) is not expected to be included in the proposed standard.

d. X3B11 Paper 95-096. Planning Guide for Third Working Draft for 90mm Phase Change Optical Disk Cartridge, Capacity: 1,3GB per Cartridge. An "I" (International) Project is being requested.

e. AIIM TR 21-1991 - Recommendations for Identifying Information to be Placed on WORM and Rewritable Optical Disk (OD) Cartridge Label(s) and OD Cartridge Packaging (Shipping Containers)

3.5.9.3.6 Recommendations. The recommendation is to apply the standards shown above as "adopted" that may suit the circumstances of the system. ISO/IEC 10090 and 10089 and ANSI X3.212 are recommended for rewritable optical disk cartridges; however, future trends for higher capacity and performance, as well as new technologies, will soon cause lower capacity/performance disks to be outmoded. Reaffirmation of ISO/IEC 10089 has been recommended by ANSI X3B11 technical committee during the standard's five year review.

3.5.9.4 Support for software distributed on CD-ROM. These standards provide the formats for data on CD-ROM and the specifications for drivers to read them. these formats are designed to deliver finished software products to a broad range of platforms.

3.5.9.4.1 Standards. Table 3.5-51 presents standards for support for software distribution on CD-ROM.

TABLE 3.5-51 Support for software distributed on CD-ROM standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Volume and File structure of CD-ROM for Information Interchange (same as ECMA 119)	9660:1988	Adopted (Approved)
IPC	ISO/IEC	Data Interchange on Read-Only 120mm Optical Data Disks (CD-ROM) (see ECMA 130-1998)	10149:1995	Adopted (Approved)
CPC	X/Open	CD-ROM (XCDR)	C519 (12/95)	Informational (Approved)
CPC	IMA	Recommended Practice for Data Exchange (adopts Bento and an OMFI subset)	IMA-RP, 950701.1	Informational (Approved)
GPC	DOD (DISA)	Department of Defense Handbook, DOD-Produced CD-ROM Products, 1st Revision	MIL-HDBK-9660A (1996)	Informational (Approved)
CPC	Various	UNIPACK (format interface)	P18.01-DO.141 (5/93)	Informational (Approved)
CPN-C	Apple	Bento (Format and API)	1.0d5, 1992	Informational (Approved)
CPN-C	Avid	Open Media Framework Interchange (OMFI) format and API	OMFI, V. 1.0, 1993	Informational (Approved)
IPC	ISO/IEC	Coding of Multimedia and Hypermedia Information - Part 1: MHEG objects representation - base notation (ASN.1), Part 4: Registration procedure for MHEG format identifier	13522-1,4:1995	Informational (Approved)
CPN-C	Apple	CD-WO (Write Once) (media interface for interchange)	Orange Book, 1993	Informational (Approved)
CPN-C	Microsoft	CD-XA (Extended Architecture) (media interface for interchange)	CD-XA, 1986	Informational (Approved)
CPC	Various	CD-Rom standard	Yellow Book, 1984	Informational (Approved)
CPC	Various	Digital Video Disk (DVD)	DVD	Informational (Approved)
CPC	X/Open	CD-ROM Support Component (XCDR)	P120:5/91	Informational (Superseded)

3.5.9.4.2 Alternative specifications. No other specifications are available.

3.5.9.4.3 Standards deficiencies. ISO 9660 does not support long filenames such as those used on UNIX systems.

3.5.9.4.4 Portability caveats. The IMA's Recommended Practice for Data Exchange has only recently been published. Therefore, it is not broadly supported. It is designed to be a platform and

content-neutral recommendation for the exchange of multimedia data for content and title developers.

Digital Video Disc (DVD also known as Digital Versatile Disc) will come in read-only, recordable, and rewritable forms. DVD-RO will have a 4.7GB capacity in the single layer version (a second layer will allow for ISO 9660 files). DVD-R will have 3.9 GB and DVD-RAM will be 2.6GB. DVD will not use the ISO 9660 file format, will support packet writing and will write in sectors instead of a spiral. Transfer rates for DVD will be about 1.4MBps.

3.5.9.4.5 Related standards. The following standards are related to CD-ROM:

a. CD-R is a standard and technology that allows a user to write to and read from a Compact Disc.

b. CD-ROM is a compact disc format used to hold text, graphics, and stereo sound.

c. CD-ROM/XA is a CD-ROM enhancement that allows audio to be interleaved with data. It also functions as a bridge between CD-ROM and CD-I, since CD-ROM/XA discs will play on a CD-I player. CD-ROM/XA uses a standard CD-ROM player, but requires a CD-ROM/XA controller card in the computer. Although it is not a video specification limited video can be included on disc. To use it, you must have a drive that reads the audio portions of the disc and an audio card in your computer that translates the digital data into sound. Not all drives can recognize the extensions.

d. CD-Video (CD-V) is a format for putting five minutes of video on a three-inch disc.

e. CD-WO is a CD-ROM version of the WORM technology. CD-WO discs conform to ISO 9660 standards and can be played in CD-ROM drives.

3.5.9.4.6 Recommendations. ISO 9660 and 10149 should be used for all CD-ROM applications. ISO 9660 describes the logical structure of information on a CD. ISO 10149 describes the physical structure of the CD. In addition, MIL-HDBK-9660A, Department of Defense Handbook, DOD-Produced CD-ROM Products, 1st Revision, 30 September 1996, which gives DOD labeling and security requirements along with other information, should be followed.

MHEG (ISO 13522) will define an interchange format for real-time multimedia information interchange. Its goals are platform independent interchange of interactive multimedia content, robust time-space composition and synchronization, real-time interchange, and incorporation of arbitrary monomedia formats.

3.5.10 Data interchange security. Securing the storage, access, and transmission of data to ensure confidentiality employs a variety of techniques. These techniques encompass encryption, data security labeling, and electronic signatures which provide non-repudiation services.

3.5.10.1 Systems confidentiality. (This BSA appears in part 5 and part 10.) These standards provide the high-level framework with which to view the security service of confidentiality in systems.

3.5.10.1.1 Standards. Table 3.5-52 presents standards for systems confidentiality.

TABLE 3.5-52 Systems confidentiality standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Computer Security Guidelines for Implementing the Privacy Act of 1974	FIPS PUB 41:1975	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 5: Confidentiality	10181-5	Informational (Draft)

3.5.10.1.2 Alternative specifications. There are no alternative specifications.

3.5.10.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.10.1.4 Portability caveats. Portability problems in the existing standards are unknown.

3.5.10.1.5 Related standards. DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information. DDS-2600-6243-92, Compartmented Mode Workstation Evaluation Criteria, Version 1 (final), defines minimum security requirements for workstations to be accredited in the Compartmented Mode under the policy set forth in DCID 1/16. Public Law (PL) 93-579, Privacy Act of 1974, and PL 100-235, Computer Security Act of 1987, contain confidentiality requirements. FIPS PUB 41 provides guidance for conformance with PL 93-579.

3.5.10.1.6 Recommendations. The mandated standard is recommended. The DGSA, Volume 6 of the TAFIM, provides security principles and target security capabilities to guide system security architects in creating specific security architectures consistent with the DGSA. The

DGSA should be used by system security architects to develop logical and specific security architectures.

3.5.10.2 Data encryption security. (This BSA appears in part 5, part 7, part 10, and part 11.) Encryption is the cryptographic transformation of data to produce cipher text. Standards for data encryption security services describe services such as definitions/algorithms, modes of operation, and guidelines for use for those systems that require their data to be encrypted using data encryption security services. None of these standards are for systems processing classified information.

3.5.10.2.1 Standards. Table 3.5-53 presents standards for data encryption security.

TABLE 3.5-53 Data encryption security standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Escrowed Encryption Standard (EES)	FIPS PUB 185: 1994	Mandated (Approved)
GPC	NIST	Data Encryption Standard (DES) (related to ANSI X3.92-1981/R1987/R1993)	FIPS PUB 46-2:1993 (Reaffirmed until 1998)	Informational (Approved)
GPC	NIST	Guidelines for Implementation and using the NBS Data Encryption Standard	FIPS PUB 74:1981	Informational (Approved)
GPC	NIST	Data Encryption Standard (DES) Modes of Operation (related to ANSI X3.106-1983)	FIPS PUB 81:1980	Informational (Approved)
GPC	NIST	Security Requirements for Cryptographic Modules	FIPS PUB 140-1:1994	Informational (Approved)
IPC	ISO	Modes of Operation for a 64-Bit Block Cipher Algorithm (Related to ANSI X3.106)	8372:1987	Informational (Approved)
NPC	ANSI	Data Encryption Algorithm	X3. 92-1981 (R1993)	Informational (Approved)
NPC	ANSI	Digital Encryption Algorithm - Modes of Operation	X3.106-1983 (R1990)	Informational (Approved)
GPC	NIST	Advanced Encryption Standard	FIPS PUB JJJ	Informational (Formative)

3.5.10.2.2 Alternative specifications. The only other available specifications are proprietary, for example, RSA.

3.5.10.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.10.2.4 Portability caveats. DES applications are not portable to non-DES systems. Portability problems related to EES are unknown. The U.S. controls export of cryptographic technologies, products, and related technologies as munitions. On October 1, 1996, a new federal policy allowing U.S. vendors to export products using up to 56-bit encryption, provided the vendors sign an agreement to make their 56-bit encryption technologies key-recovery-compliant within 24 months.

3.5.10.2.5 Related standards. FIPS PUB 113, Computer Data Authentication, is related to DES security mechanisms and their standards.

3.5.10 2.6 Recommendations. The mandated standard is recommended. FIPS PUB 185, EES, supports lawful authorized access to the keys required to decipher enciphered information for systems requiring strong encryption protection of sensitive but unclassified information. EES provides stronger protection than DES against unauthorized access. Devices conforming to EES may be used when replacing Type II and Type III (DES) encryption devices owned by the Government. Implementations requiring use of EES should require conformance with FIPS PUB 140-1.

On 2 January 1997, NIST announced plans to develop a FIPS, Advanced Encryption Standard, incorporating an advanced encryption algorithm to replace DES (FIPS PUB 46-2).

3.5.10.3 Data interchange security labeling. (This BSA appears in part 5 and part 10.) Data interchange security labeling provides a security service to define the format and correctly parse a security label into the security attributes used by other security services.

3.5.10.3.1 Standards. Table 3.5-54 presents standards for data interchange security labeling.

TABLE 3.5-54 Data interchange security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Common Security Label (CSL)	MIL-STD-2045-48501: 1995	Mandated (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Informational (Approved)
GPC	NIST	Standard Security Label (SSL) for Information Transfer	FIPS PUB 188:1994	Informational (Approved)
IPC	ITU-T	Message Handling Systems: Message Transfer System: Abstract Service Definition and Procedures	X.411: 1992	Informational (Approved)
CPC	TSIG	Trusted Security Information Exchange for Restricted Environments	TSIX (RE) 1.1	Emerging (Draft)

3.5.10.3.2 Alternative specifications. There are no alternative specifications.

3.5.10.3.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.10.3.4 Portability caveats. Portability problems with the existing standards are unknown.

3.5.10.3.5 Related standards. DOD 5200.28-STD is a related standard.

DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

3.5.10.3.6 Recommendations. The mandated standard is recommended. TSIG TSIX(RE) 1.1 includes options compatible with MIL-STD-2045-48501.

3.5.10.4 Systems non-repudiation. (This BSA appears in part 5, part 7, part 10, and part 11.) These standards provide the security services for non-repudiation in systems.

3.5.10.4.1 Standards. Table 3.5-55 presents standards for open systems non-repudiation.

TABLE 3.5-55 Systems non-repudiation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Digital Signature Standard (DSS)	FIPS PUB 186:1994	Mandated (Approved)
GPC	DOD	Information Technology - Defense Standardized Profiles AMHDx(D)- Message Handling Systems - Message Security Protocol (MSP) Parts 1-5	MIL-STD-2045-18500: 1993	Mandated (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, Rev. 3.0: 1994	Legacy (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, v. 4.0, Rev. A: 1997	Emerging (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 4: Protecting Transfer Syntax Specification	11586-4:1994	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
CPC	IETF	IP Authentication Header (AH)	RFC 1826: 1995	Emerging (Draft)
CPC	OMG	Common Object Request Broker Architecture (CORBA) Security	OMG 95-12-1: 1995	Emerging (Draft)
CPC	IETF	S/MIME Message Specification: PKCS Security Services for MIME	draft-dussc-mime-msg-spec-00.txt, September 1996	Informational (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 4: Non-Repudiation (same as ITU-TS X.813)	10181-4	Informational (Draft)
IPC	ISO	Non-Repudiation Mechanisms Part 1: General Model	13888-1:1992 (SC27 N868 (Project 1.27.06.01))	informational (Draft)
IPC	ISO	Non-Repudiation Mechanisms Part 2: Using Symmetric Encipherment Algorithms	13888-2:1994 (SC27 N864 (Project 1.27.06.02))	Informational (Draft)
IPC	ISO	Non-Repudiation Mechanisms Part 3: Using Asymmetric Techniques	13888-3:1992 (SC27 N869 (Project 1.27.06.03))	Informational (Draft)
IPC	ISO	OSI Distributed Transaction Processing (DTP) - Draft Amendments to Parts 1 to 3: Transaction Processing Security	WDAMs (SC21 N 5232 to ISO 10026-1,2,3) 1991	Informational (Draft)

3.5.10.4.2 Alternative specifications. There are no alternative specifications.

3.5.10.4.3 Standards deficiencies. FIPS 186 is for electronic signatures for unclassified but sensitive information. It cannot be used for classified information.

3.5.10.4.4 Portability caveats. The Secure Hash Algorithm (SHA-1) in FIPS 180-1 supersedes the SHA in FIPS 180. SHA-1 and SHA are not interoperable; therefore, implementations of FIPS 186 using SHA-1 and SHA are not interoperable.

3.5.10.4.5 Related standards. FIPS PUB 180-1, Secure Hash Standard, must be used with FIPS PUB 186. FIPS PUB 180-1 provides the Secure Hash Algorithm used in generating and verifying electronic signatures.

3.5.10.4.6 Recommendations. The mandated standards are recommended for non-repudiation.

MIL-STD-2045-18500 describes the security provided by MSP. It should be used for DOD message systems that are required to exchange classified and sensitive but unclassified information. It is based on Version 3.0 of the MSP documented in SDN.701, "Secure Data Network System (SDNS) Message Security Protocol," Revision 1.5, 1 August 1989. MSP is under revision to Version 4.0 to accommodate, in part, Allied requirements. This DSP standard will be replaced by a portion of the U.S. Supplement to ACP 123 or ACP 120, Common Security Protocol, when the revision to MSP is complete.

MSP provides for signed receipts. S/MIME, an Internet Draft specification, does not provide for signed receipts.

3.5.10.5 Electronic signature. (This BSA appears in part 5, part 7, and part 10.) Electronic signature is the process that operates on a message to ensure message source authenticity and integrity, and source non-repudiation. Electronic signatures are composed so that the identity of a signatory and integrity of the data can be verified.

3.5.10.5.1 Standards. Table 3.5-56 presents standards for electronic signature.

TABLE 3.5-56 Electronic signature standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Digital Signature Standard (DSS)	FIPS PUB 186:1994	Mandated (Approved)
IPC	ISO	Digital Signature Scheme Giving Message Recovery	9796:1991	Informational (Approved)
CPC	IETF	Privacy Enhancement for Internet Electronic Mail	RFC 1421-1424:1993	Informational (Draft)
IPC	ISO	Digital Signature with Appendix - Part 1: General	SC27/WG2 N294 (Project 1.27.08.01)	Informational (Formative)
IPC	ISO	Digital Signature with Appendix - Part 2: Identity-Based Mechanisms	SC27/WG2 N295 (Project 1.27.08.02)	Inform- onal (Form ve)
IPC	ISO	Digital Signature with Appendix - Part 3: Certificate-Based Mechanisms	SC27/WG2 N296 (Project 1.27.08.03)	Informational (Formative)

3.5.10.5.2 Alternative specifications. Rivest-Shamir-Adelman (RSA) Public Key Algorithm RC-5 was developed and published in 1994. It is proprietary, but RSA Data Security is working to have it included in numerous Internet standards. At present, RC-5 is not recommended for DOD use because it is proprietary.

3.5.10.5.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.10.5.4 Portability caveats. DSS applications are not interoperable with non-DSS systems.

3.5.10.5.5 Related standards. FIPS PUB 180-1, Secure Hash Standard, must be used with FIPS PUB 186. FIPS PUB 180-1 provides the Secure Hash Algorithm used in generating and verifying electronic signatures.

3.5.10.5.6 Recommendations. The mandated standard is recommended. FIPS PUB 186 is implemented in the FORTEZZA cryptographic card, a PC card (formerly called a Personal Computer Memory Card International Association (PCMCIA) standard card) that can be integrated into personal computers and workstations to provide security in commercial applications. FORTEZZA is being used in the Defense Message System. FIPS PUB 186 is the government-wide key cryptographic signature system.

3.5.10.6 Electronic hashing. (This BSA appears in part 5, part 7, part 8, and part 10.) Electronic hashing services compute a condensed representation of a message or a data file, often used as a measure of data integrity checking.

3.5.10.6.1 Standards. Table 3.5-57 presents standards for electronic hashing.

TABLE 3.5-57 Electronic hashing standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180-1:1995	Mandated (Approved)
IPC	ISO	Hash Functions, Part 1: General Model	10118-1:1994	Informational (Approved)
IPC	ISO	Hash Functions, Part 2: Hash Functions Using an N-Bit Block Cipher Algorithm	10118-2:1994	Informational (Approved)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180:1993	Informational (Superseded)
IPC	ISO	Hash Functions, Part 3: Dedicated Hash Functions	WD 10118-3, JTC1/SC27 N883 (Project 1.27.09.03)	Informational (Draft)
IPC	ISO	Hash Functions, Part 4: Hash Functions Using Modular Arithmetic	WD 10118-4, JTC1/SC27 N884 (Project 1.27.09.04)	Informational (Draft)

3.5.10.6.2 Alternative specifications. There are no alternative specifications.

3.5.10.6.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.5.10.6.4 Portability caveats. Portability problems with the existing specifications are unknown.

3.5.10.6.5 Related standards. FIPS PUB 180-1 supersedes FIPS PUB 180 and is required for use with FIPS PUB 186, Digital Signature Standard.

3.5.10.6.6 Recommendations. The mandated standard is recommended. FIPS PUB 180-1 specifies SHA, which can be used to generate a message digest. SHA is required for use with the DSA as specified in FIPS PUB 186 and whenever an SHA is required for federal applications.

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 6 of 14 parts)

GRAPHICS SERVICES

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

TABLE OF CONTENTS

LIST OF TABLES

3.6 Graphics services. Graphics services provide functions required for creating pictures and importing them by scanning or photography. These services include definition and management of display element and graphical object attributes. This includes defining multidimensional graphics objects in a form that is independent of output devices and managing database structures, including hierarchical and object-oriented structures containing graphics data.

NOTE: Throughout Part 6, all tables shall have abbreviations listed under the column (Standard Type) as follows:

a. National Public Consensus = NPC
b. International Public Consensus = IPC
c. Government Public Consensus = GPC
d. Consortia Public Consensus = CPC
e. Corporate Private Non-Consensus = CPN-C

3.6.1 Raster graphics. Raster graphics is a technique for representing a picture image as a matrix of dots. Raster graphics images are created by scanners and cameras and are generated by paint packages. The simplest monochrome bitmap uses one bit (on/off) for each dot. Gray scale bitmaps (monochrome shades) represent each dot with a number large enough to hold all the gray levels. Color bitmaps require sufficient storage to hold the intensity of red, green, and blue as would a grey scale equivalent.

3.6.1.1 Raster data interchange. (This BSA appears in part 3, part 5, and part 6.) Raster data interchange MIL SPEC identifies the requirements to be met when raster graphics data represented in digital, binary format are delivered to the government. Raster graphics standards are standards for pixel-by-pixel representation of images. (See still image compression, section 3.5.8.2, for more facsimile standards suitable for raster data interchange.)

3.6.1.1.1 Standards. Table 3.6-1 presents standards for raster data interchange.

TABLE 3.6-1 Raster data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	User Interface Component of the Applications Portability Profile (Adopts the X Protocol, Xlib Interface, Xt Intrinsics, and Bitmap Distribution Format of X11R5)	FIPS PUB 158-1:1993	Mandated (Approved)
NPC/IPC	ANSI/ISO/IEC	Interfacing Techniques for Dialogues with Graphical Devices (CGI) - Functional Specification - Part 6: Raster	9636-6:1991	Mandated (Approved)
GPC	DOD (NIMA)	Raster Product Format (RPF)	MIL-STD-2411:1994	Mandated (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 1: Overview and Fundamental Principles (formerly Product Data Exchange Specification (PDES))	10303-1:1994	Informational (Approved)
CPC	X/Open	X Window System File Formats and Application Conventions (Bitmap Distribution Format (BDF))	C170 (7/91)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	General Aspects of Group 4 Facsimile Apparatus (Adopts EIA-536-1988)	FIPS PUB 149:1988	Informational (Approved)
GPC	NIST	Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus (Adopts EIA 538-1988)	FIPS PUB 150:1988	Informational (Approved)
GPC	NIST	Initial Graphics Exchange Specification (IGES) (adopts ASME/ANSI Y14.26M-1989) (IGES ver. 4)	FIPS PUB 177:1992	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-PRF-28000	Informational (Approved)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-PRF-28002	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Illustration Data : CGM Application Profile (based on FIPS 128)	MIL-PRF-28003	Informational (Approved)
NPC	ANSI/AIIM	Recommended Practice; File Format for Storage and Exchange of Images; Bi-Level Image File Format: Part 1	MS53-1993	Informational (Approved)
GPC	NIST	Standard for the Interchange of Large Format Tiled Documents	NISTIR 88-4017	Informational (Approved)
IPC	NATO	Analogue Video Standard for Aircraft System Applications	STANAG 3350	Informational (Approved)
IPC	NATO	Exchange Specifications for ARC Standardized Raster Graphics (ASRG)	STANAG 4387:1996	Informational (Approved)
IPC	NATO	Specifications for UTM/UPS Standardized Raster Products (USRP)	STANAG 7077	Informational (Approved)
IPC	ITU-T	Document Application Profile for the Interchange of Formatted Mixed Mode Document - Terminal Equipment and Protocols for Telematic Services	T.501 (1989)	Informational (Approved)
IPC	ITU-T	Document Application Profile for the Interchange of Group 4 Facsimile Documents	T.503 (1991)	Informational (Approved)
NPC	AIIM	Interchange of Tiled Raster Documents	TR14:1988	Informational (Approved)
IPC	NATO	Exchange Specifications for ARC Digitized Raster Graphics (ADRG)	STANAG 7108	Informational (Draft)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-D-28000A(1) of 12/14/92	Informational (Superseded)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-R-28002B(1) of 9/20/1993	Informational (Superseded)

3.6.1.1.2 Alternative specifications. Currently IGES is the most mature and widely implemented standard for conveying product data information. Other bitmap formats include proprietary formats such as GIF, PCX, TIFF, RLE, and TGA. Except for support of legacy products, these formats are not recommended.

3.6.1.1.3 Standards deficiencies. Raster graphics files require enormous amounts of storage and must be supplemented by compression standards.

3.6.1.1.4 Portability caveats. A standard technique for raster data interchange should be selected for use throughout the Department of Defense (DOD) and applied wherever possible.

3.6.1.1.5 Related standards. The following standards are related to raster data interchange or raster data interchange standards:

a. ASME/ANSI Y14.28M-1989, which describes product design and manufacturing information.

b. ITU-T, facsimile transmission standards.

c. Raster compression standards.

3.6.1.1.6 Recommendations. The mandated standards are recommended for raster data interchange.

MIL PRF-28002 (Raster) can be used in a Computer-Aided Acquisition and Logistic Support (CALS) environment, and, when needed, supplemented by National Institute of Standards and Technology Interim Report (NISTIR) 88-4017 (tiling). FIPS Pub 150 can also be used. With only the CALS Raster standard available, no real tailoring guidance is possible. This version (MIL-PRF-28002) supports engineering drawings and technical manual illustrations. The previous CALS Raster standard (MIL-R-28002B) can be used for in-place and unrevised legacy data. Tiling (as in NISTIR 88-4017) and compression are desirable for very large raster graphics files. (See the Still image compression BSA, part 3.5.8.2 of the ITSG.) MIL-PRF-28003 (CGM) offers the capability for having raster and vector graphics in the same file. The approved BDF provides conventions for font conversion/interchange between external and internal X Windows fonts and can be used in procurements using a client-server computing architecture with a graphical user interface in a networked environment. BDF can be compiled in Server Normal Format to be optimized for a particular server.

3.6.1.2 Still image compression. (This BSA appears in part 5, Data Interchange, and part 6, Graphics.) Still image compression standards provide the capability of reducing storage needed for raster graphics files. This compression can be either exact (loss-less) or approximate (lossy) upon reversal, depending upon the algorithm. The JPEG is interested in developing standards covering compression and decompression of still-frame, continuous tone, photographic (gray scale or color) digitized images by facsimile.

3.6.1.2.1 Standards. Table 3.6-2 presents standards for still image compression.

TABLE 3.6-2 Still image compression standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Digital Compression and Coding of Continuous - Tone Still Images, Part 1: Requirements and Guidelines (as profiled by MIL-STD-188-198A - JPEG)	10918-1:1994	Mandated (Approved)
GPC	DOD	Bi-Level Image Compression for the National Imagery Transmission Format Standards (NITFS)	MIL-STD-188-196 of 6/18/1993	Mandated (Approved)
GPC	DOD	Vector Quantization (VQ) Decompression for the NITFS	MIL-STD-188-199 of 6/27/1994	Mandated (Approved)
GPC	NIST	Group 3 Facsimile Apparatus for Document Transmission	FIPS PUB 147:1981	Informational (Approved)
GPC	NIST	Procedures for Document Facsimile Transmission (Adopts EIA-RS-466)	FIPS PUB 148:1982	Informational (Approved)
GPC	NIST	General Aspects of Group 4 Facsimile Apparatus (Adopts EIA-536-1988)	FIPS PUB 149:1988	Informational (Approved)
GPC	NIST	Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus (Adopts EIA 538-1988)	FIPS PUB 150:1988	Informational (Approved)
IPC	ITU-T	Standardization of Group 3 Facsimile Apparatus for Document Transmission: Terminal Equipment and Protocols for Telematic Services	T.4 (1993)	Informational (Approved)
IPC	ITU-T	Fax Coding Schemes & Coding Control Functions for Group 4 Fax Apparatus - Terminal Equipment & Protocols for Telematic Services	T.6 (1989)	Informational (Approved)
IPC	ITU-T	Digital Compression and Coding of Continuous - Tone Still Images - Requirements and Guidelines - Terminal Equipment and Protocols for Telematic Services	T.81 (1993)	Informational (Approved)
IPC	ISO/IEC	Digital Compression and Coding of Continuous-Tone Still Images - Part 2: Compliance Testing	10918-2:1993	Informational (Approved)
IPC	ISO/IEC	Progressive Bi-Level Image Compression (JBIG) Compression Algorithm for Black-and-White Images	11544 (Corrigendum 1):1995	Informational (Approved)
IPC	ISO/IEC	Data Compression for Information Interchange - Adaptive Coding with Embedded Dictionary - DCLZ Algorithm	11558:1992	Informational (Approved)
IPC	ISO/IEC	Procedure for the Registration of Algorithms for the Lossless Compression of Data	11576:1994	Informational (Approved)
IPC	ISO/IEC	Data Compression for Information Interchange - Binary Arithmetic Coding Algorithm	12042:1993	Informational (Approved)
IPC	ITU-T	Common Components for Image Compression and Communication - Basic Principles - Terminal Equipment and Protocols for Telematic Services	T.80 (1992)	Informational (Approved)
IPC	ITU-T	Coded Representation of Picture and Audio Information - Progressive Bi-Level Image Compression - Terminal Equipment and Protocols for Telematic Services	T.82 (1993)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-PRF-28002	Informational (Approved)
GPC	DOD	Adaptive Recursive Interpolated Differential Pulse Code Modulation (ARIDPCM) for the National Imagery Transmission Format Standards (NITFS)	MIL-STD-188-197A of 10/12/1994	Informational (Approved)
NPC	ANSI	Compaction Algorithm - Binary Arithmetic Coding	X3.225	Informational (Approved)
IPC	ISO/IEC	Digital Compression and Coding of Continuous-Tone Still Images - Part 3: Extensions	10918-3:1995	Informational (Draft)
IPC	ISO/IEC	Digital Compression and Coding of Continuous-Tone Still Images - Registration Procedures for JPEG profile, APPn marker, and SPIFF profile ID marker	10918-4:1996	Informational (Draft)
IPC	ISO/IEC	Coding of Moving Pictures and Associated Audio for Digital Storage Media up to about 1.5 Mbit/sec (MPEG 1), Part 5: Technical Report on Software for ISO/IEC 11172:1993	11172-5	Informational (Draft)
IPC	ISO/IEC	Generic Moding of Moving Pictures and Associated Audio Information (MPEG2) Part 4: Compliance Testing	13818-4	Emerging (Draft)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-R-28002B(1) of 9/20/1993	Informational (Superseded)

3.6.1.2.2 Alternative specifications. The following compression methods are also available:

a. LZW compression algorithm.
b. Fractal transforms.

3.6.1.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.6.1.2.4 Portability caveats. The DOD National Imagery Transfer Format Standards (NITFS) Adaptive Recursive Interpolated Differential Pulse Code Modulation (ARIDPCM) compression scheme for eight-bit gray scale images eventually will be replaced by the International Organization for Standardization (ISO)/JPEG standard in the broader community, thereby providing the potential for incompatibilities with existing ARIDPCM-based systems. Fractal transforms are still in a preliminary stage and continue to present many problems.

Motion Pictures Expert Group (MPEG) is a joint development project of ISO and ITU-T. The same organization is responsible for the JPEG standard. Coordination of the standards in this area, ITU-T H.261, JPEG, and MPEG will depend on ISO and ITU-T.

3.6.1.2.5 Related standards. The following standards are related to non-text data compression standards:

a. MIL-HDBK-1300A, NITFS
b. MIL-STD-2500A, NITF Version 2.0 for the NITFS
c. Various multimedia standards
d. Raster graphics standards

e. ISO/IEC 11172, MPEG1
f. ISO/IEC 13818, MPEG2

3.6.1.2.6 Recommendations. The standards listed as mandated are recommended. If the DOD ARIDPCM compression scheme defined in the NITFS is specified in a procurement, a migration strategy to the ISO/ITU-T/JPEG standard also should be required. NITFS only supports ITU-T Group III compression, while CALS only supports Group IV.

Use the NITFS compression standards or CALS compression standard, as applicable. The MPEG and Joint Bi-Level Imaging Group (JBIG) standards should be considered for their specialized areas of use. The NIST and ITU-T standards for facsimile are recommended also. Lossless versus lossy compression: Group 4 facsimile is compatible with Group 3, but Group 3 facsimile is not necessarily compatible with Group 4. NITFS supports group 3, and CALS MIL-PRF-28002 supports group 4. If a file is compressed using group 4 facsimile, it will not be readable by a group 3 facsimile system, but a file compressed using group 3 facsimile will be readable by a group 4 facsimile system.

The JPEG standard can be implemented in hardware or software, and is already available in commercial products. However, sites purchasing JPEG products based on the draft versions of the standard should require vendor assurance that the products will comply with the international standard.

ITU-T H.261 is recommended for applications that require a 64-Kbit/second line rate. JPEG is recommended for still image applications when its data loss does not impact on the system function. MPEG is recommended for moving image applications when its elimination of redundant information between frames does not impact on the system function.

3.6.2 Vector graphics. Vector graphics are a method of representing graphical objects as sets of endpoints for lines, curves, and other geometric shapes with data about width, color, and spaces bounded by lines and curves. The entire image commonly is stored in the computer as a list of vectors called a display list. Vector graphics are used when you need geometric knowledge about the object created. Geometric shapes keep their integrity: a line always can be picked, extended, or erased. Today, most screens are raster graphics displays (composed of dots), and the vectors are put into the required dot patterns (rasters) by hardware or software. Vector graphics systems must be supplemented by data interchange standards such as Initial Graphics Exchange Specification (IGES), CGM, and the Standard for the Exchange of Product Model Data (STEP).

3.6.2.1 Vector graphics APIs. The Programmer's Hierarchical Interactive Graphics System (PHIGS) is a graphics system and language allowing programming of two-dimensional and three-dimensional graphical objects to be displayed or plotted on appropriate devices in interactive, high performance environments, and managing hierarchical database structures containing graphics data. PHIGS is a device-independent interface between the application program and the graphics subsystem. PHIGS manages graphics objects in a hierarchical manner so that a complete assembly can be specified with all of its subassemblies. The Graphical Kernel System (GKS) is a graphics system that is independent of the operating system and provides basic primitives and constructs for drawing two-dimensional objects to be displayed or plotted on appropriate devices (raster graphics and vector graphics devices). The GKS extensions add three-dimensional abilities. The application programming interfaces (APIs) allow graphics applications to be developed on one system and easily moved to another with minimal or no change.

3.6.2.1.1 Standards. Table 3.6-3 presents standards for vector graphics APIs.

TABLE 3.6-3 Vector graphics APIs standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC/IPC	ANSI/ISO/IEC	Programmers' Hierarchical Interactive Graphics System (PHIGS and PHIGS PLUS) (as profiled by FIPS PUB 153-1)	9592-1,2,3,4:1989 with AMD1:1992	Mandated (Approved)
IPC	ISO/IEC	Information Technology-Computer Graphics-Interfacing (CGI) Techniques for Dialogue with Graphics Devices	9636:1991	Mandated (Approved)
IPC	ISO/IEC	Graphical Kernel System (GKS) functional description API (ANSI X3.124:1985 as profiled by FIPS PUB 120-1:1991)	7942:1985	Mandated (Approved)
IPC	ISO	GKS for 3 Dimensions (GKS-3D) Functional Description	8805:1988	Informational (Approved)

3.6.2.1.2 Alternative specifications. No consortia or de facto specifications for vector graphics are available.

3.6.2.1.3 Standards deficiencies. Some features are added to PHIGS implementations to compensate for perceived deficiencies in the standard (e.g., adding the PHIGS Plus Lumiere und Surfaces (PLUS) standard). The is well-established and well-supported by the computer industry, but it is minimal and other capabilities are needed.

3.6.2.1.4 Portability caveats. Most implementations of PHIGS provide extra features that are not part of the PHIGS standard and often are unnecessary. These features must be avoided if possible, since unique features limit portability. As with graphics implementations based on PHIGS, many nonstandard additions in the implementation can impede portability.

3.6.2.1.5 Related standards. The following standards are related to vector graphics API standards:

a. ISO/International Electrotechnical Commission (IEC) 9593-1:1990: PHIGS Language Bindings - Part 1: FORTRAN (corrigendum 1:1993, 2 1994).

b ISO/IEC 9593-3:1990: PHIGS Language Bindings - Part 3: Ada (Amd 1 1994, Corr 1 1993.

c. ISO/IEC 9593-4:1991: PHIGS Language Bindings - Part 4: C (Amd 1 1994 Corr 1 1994).

3.6.2.1.6 Recommendations. The mandated standards are recommended. The PHIGS standards must be used without allowing extra features, and the use of options must be controlled. The GKS functionality (and GKS-3D's functionality) is totally subsumed and extended by PHIGS.

3.6.2.2 Vector graphics data interchange. (This BSA appears in part 5, Data Interchange, and part 6, Graphics.) These standards provide file formats for the storage, exchange, and import/export of raster or vector graphical drawings and images.

3.6.2.2.1 Standards. Table 3.6-4 presents standards for vector graphics data interchange.

TABLE 3.6-4 Vector graphics data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Metafile for Storage/Transfer of Pictorial Description Information (CGM) (as profiled by FIPS PUB 128-1 and MIL-STD-2301)	8632-1,2,3,4:1992 (w/Amd 1&2)	Mandated (Approved)
NPC/IPC	ANSI/ISO/IEC	Programmers' Hierarchical Interactive Graphics System (PHIGS and PHIGS PLUS) (as profiled by FIPS PUB 153-1)	9592-1,2,3,4:1989 with AMD1:1992	Mandated (Approved)
GPC	NIST	Initial Graphics Exchange Specification (IGES) (adopts ASME/ANSI Y14.26M-1989) (IGES ver. 4)	FIPS PUB 177:1992	Informational (Approved)
NPC	ANSI/US PRO	IGES 5.2, Initial Graphics Exchange Specification (Replaces ANSI/ASME Y14.26M-1989)	US PRO/IPO-100 (Nov 1993)	Informational (Approved)
IPC	ANSI/NPESA	Prepress Digital Data Exchange - Tag Image File Format for Image Technology (TIFF/IT)	IT8.8	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-PRF-28000	Informational (Approved)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-PRF-28002	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Illustration Data : CGM Application Profile (based on FIPS 128)	MIL-PRF-28003	Informational (Approved)
GPC	DOD	Computer Graphics Metafile (CGM) Implementation Standard for National Imagery Transfer Format Standard (NITFS) (based on FIPS 128)	MIL-STD-2301A	Informational (Approved)
NPC	ANSI/AIIM	Recommended Practice; File Format for Storage and Exchange of Images; Bi-Level Image File Format: Part 1	MS53-1993	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-D-28000A(1) of 12/14/92	Informational (Superseded)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-R-28002B(1) of 9/20/1993	Informational (Superseded)
GPC	DOD	Digital Representation for Communication of Illustration Data : CGM Application Profile (based on FIPS 128)	MIL-D-28003A(1) of 8/14/1992	Informational (Superseded)
NPC	ANSI/ASME	Digital Representation for Communication of Product Definition Data	Y14.26M:1989	Informational (Superseded)

3.6.2.2.2 Alternative specifications. The following specifications are also available:

a. BMP (Windows Bitmap) - Proprietary.
b. CGI (Computer Graphics Interface)
c. GIF (Graphics Interchange Format) (Used by CompuServe)
d. NAPLPS (North American Presentation Level Protocol Syntax)
e. PDL (Page Description Language) - Proprietary

f. TIFF (Tagged Image File Format) - Proprietary
g. VDM (Virtual Device Metafile)
h. VDI (Virtual Device Interface)

3.6.2.2.3 Standards deficiencies. The CGM standards have limited capabilities for handling 3-D geometries, providing fine control over line drawing details, and using font resource references enabling reasonably accurate font substitution (the latter is an understatement), and describing color. Several addenda and amendments are being developed. The addenda would add a global symbol capability, 3-dimensional geometry extensions, and improved engineering drawing capabilities (such as better control over fine details of line drawings). The amendments listed in table above are concerned with fonts and color. These CGM changes are intended to be upwardly compatible with existing versions of the specification.

3.6.2.2.4 Portability caveats. Portability problems for existing versions of the CGM standard are unknown. Potential portability problems exist for the CGM addenda and amendments, as with any new version of a specification or product, even though the standards groups are developing their specifications with upward compatibility in mind.

3.6.2.2.5 Related standards. The following standards are related to graphics data exchange or graphics data exchange standards:

a. ISO 9281: Identification of Picture Coding Methods.

b. ISO 10918-1: Digital Compression and Coding of Continuous Tone Still Images, Part 1: Requirements and Guidelines.

c. ISO 10918-2: Digital Compression and Coding of Continuous Tone Still Images, Part 2: Compliance Testing.

d. ISO CD 11172: Coding of Moving Pictures and Associated Audio.

e. ISO SC21/WG5, N4192: Proposed FTAM Document Type to Support CGM.

f. ISO SC21/WG5, N5165: FTAM Constraint Set and Document Types for CGM.

g. MIL-HDBK-1300A, NITFS

h. MIL-STD-2500A, National Imagery Transmission Format (NITF) Version 2.0 for the NITFS.

3.6.2.2.6 Recommendations. The mandated standards are recommended.

The following wording from the APP is recommended for specifying data interchange standards:

"All computer graphics metafiles acquired to describe, store, and/or communicate graphical (pictorial) information in vector format among different devices, systems, and installations should comply with the requirements set forth in FIPS PUB 128-1, Computer Graphics Metafile (CGM)."

The use of CGM is widespread, and many (most) off-the-shelf products for graphics data interchange are compatible with it.

It is important to consider the specification of CGM conformance in procurements because CGM is important to the integration of PC applications with the enterprise. Most PC graphics, word processing and desktop publishing programs support the importing and exporting of pictures, bidirectionally to other PC programs and between PC and server/minicomputer/ workstation applications.

3.6.3 Device interfaces. An API is a set of formalized software calls and routines that can be referenced by an application program to access underlying network services. The vector graphics standards mid level service area also fall into this category. Graphical user interfaces are closely related to this area.

3.6.3.1 Device interface API. Device interface API standards provide the capability to write graphics device drivers.

3.6.3.1.1 Standards. Table 3.6-5 presents standards for device interface APIs.

TABLE 3.6-5 Device interface API standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC/IPC	ANSI/ISO/IEC	Interfacing Techniques for Dialogues with Graphical Devices (CGI) - Functional Specification - Part 1: Overview, Profiles, and Conformance	9636-1:1991	Mandated (Approved)
NPC/IPC	ANSI/ISO/IEC	Interfacing Techniques for Dialogues with Graphical Devices (CGI) - Functional Specification - Part 2: Control	9636-2:1991	Mandated (Approved)
NPC/IPC	ANSI/ISO/IEC	Interfacing Techniques for Dialogues with Graphical Devices (CGI) - Functional Specification - Part 3: Output	9636-3:1991	Mandated (Approved)
NPC/IPC	ANSI/ISO/IEC	Interfacing Techniques for Dialogues with Graphical Devices (CGI) - Functional Specification - Part 4: Segments	9636-4:1991	Mandated (Approved)
NPC/IPC	ANSI/ISO/IEC	Interfacing Techniques for Dialogues with Graphical Devices (CGI) - Functional Specification - Part 5: Input and Echoing	9636-5:1991	Mandated (Approved)
NPC/IPC	ANSI/ISO/IEC	Interfacing Techniques for Dialogues with Graphical Devices (CGI) - Functional Specification - Part 6: Raster	9636-6:1991	Mandated (Approved)
IPC	ISO/IEC	Interfacing Techniques for Dialogues with Graphical Devices (CGI) - Data Stream Binding - Part 1: Character Encoding	9637-1:1994	Informational (Approved)
IPC	ISO/IEC	Interfacing Techniques for Dialogues with Graphical Devices (CGI) - Data Stream Binding - Part 2: Binary Encoding	9637-2:1994	Informational (Approved)

3.6.3.1.2 Alternative specifications. Numerous unique proprietary APIs are available for specific vendor devices.

3.6.3.1.3 Standards deficiencies. A single standard and many implementations of a device interface API may add features desirable in future standards.

3.6.3.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.6.3.1.5 Related standards. The following standards are related to device interface API standards:

a. ISO/IEC 9638-1: CGI Language Bindings - Part 1
b. ISO/IEC 9638-2: CGI Language Bindings - Part 2

c. ISO/IEC DIS 9638-3:1993 CGI Language Bindings - Part 3: Ada

3.6.3.1.6 Recommendations. CGI is the recommended device interface API for graphics.

3.6.3.2 Image processing API. Image processing API standards provide basic facilities and interfaces for imaging applications at the machine level.

3.6.3.2.1 Standards. Table 3.6-6 presents standards for image processing APIs.

TABLE 3.6-6 Image processing API standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Image Processing and Interchange (IPI) Functional Specification: Part 1: Common Architecture	12087-1:1995	Informational (Approved)
IPC	ISO/IEC	Image Processing and Interchange (IPI) Functional Specification: Part 2: Programmers Imaging Kernel System API	12087-2:1994	Informational (Approved)
IPC	ISO/IEC	Image Processing and Interchange (IPI) Functional Specification, Part 3: Image Interchange Facility (IIF)	12087-3:1995	Informational (Approved)
IPC	ISO/IEC	Image Processing and Interchange (IPI) API Language Bindings Part 4: C	12088-4:1995	Informational (Approved)
IPC	ISO/IEC	Image Processing and Interchange (IPI) Functional Specification, Part 3: Image Interchange Facility (IIF) Amendment 1: Type Definition, Scoping, and Logical Views for Image Interchange Facility	12087-3 DAM 1:1994	Informational (Draft)
IPC	ISO/IEC	Encoding for the Image Processing and Interchange Standard (IPI) - Encoding for the Image Interchange Facility (IIF)	12089:1994	Informational (Draft)
GPC	NIST	Image Processing and Interchange (IPI) Functional Specification: Programmers Imaging Kernel System API	TBD-Image Processing and Interchange (IPI)	Informational (Formative)

3.6.3.2.2 Alternative specifications. The only other available specifications are proprietary.

3.6.3.2.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.6.3.2.4 Portability caveats. Deficiencies in the existing IPI standards are unknown.

3.6.3.2.5 Related standards. The language interface bindings for IPI (ISO 12088) are related.

3.6.3.2.6 Recommendations. Use the current version of IPI, including the most current drafts of the unfinished parts, and implement a transition to the final standard.

3.6.4 Geospatial (MC&G). Standards for geospatial (Mapping, Charting, and Geodesy) products such as maps, charts, and computer displays include graphics symbols and formats for information storage and processing.

3.6.4.1 Symbology graphics. (This BSA appears in part 5, Data Interchange, and part 6, Graphics.) These are standards for the symbology to be used in geospatial applications such as hardcopy mapping products and computer-generated displays. DoD standards provide definitions for the representation of military and intelligence information.

3.6.4.1.1 Standards. Table 3.6-7 presents standards for symbology graphics.

TABLE 3.6-7 Symbology graphics standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD (US Army)	Human Factors Engineering Design Criteria for Helicopter Cockpit Electro-Optical Display Symbology	MIL-STD-1295A of 6/26/1984	Adopted (Approved)
GPC	DOD (USAF)	Aircraft Display Symbology	MIL-STD-1787B of 6/93	Adopted (Approved)
GPC	DOD (NIMA)	Mapping, Charting and Geodesy (MC&G) Symbology for Graphic Products	MIL-STD-2402 of 2/95	Adopted (Approved)
GPC	DOD (DISA)	Common Warfighting Symbology, Version 1	MIL-STD-2525	Adopted (Approved)
GPC	WMO	Technical Regulation Vol II, Meteorological Services for International Air Navigation	WMO Document #49 of 1988	Adopted (Approved)
GPC	DOD	Military Symbols	Q-STAG 509 of 3/5/1979	Informational (Approved)
NPC	ANSI/SAE	Human Interface Design Methodology for Integrated Display Symbology	ARP 4155 (1990)	Informational (Approved)
GPC	DOD (US Army)	Symbols for Army Air Defense System Displays	MIL-STD-1477B of 2/1/1993	Informational (Approved)
GPC	DOD (DISA)	Common Warfighting Symbology, Version 2	MIL-STD-2525A	Informational (Approved)
GPC	DOD (US Army)	Army Field Manual (FM): Operational Terms and Symbols	FM 101-5-1 SMIGS (Symbols of Oct. 1985)	Informational (Approved)
NPC	ANSI/ISA	Instrumentation Symbols and Identification	S5.1-1984 (R1992)	Informational (Approved)
NPC	ANSI/ISA	Graphic Symbols for Process Displays	S5.5-1985	Informational (Approved)
IPC	NATO	NATO Experimental Tactics and Amplifying Tactical Instructions - AXP-5(B) (Navy/Air)	STANAG 1125	Informational (Approved)
IPC	NATO	Military Symbols for Land Based Systems (APP-6, Ed 3)	STANAG 2019(1) of 11/26/1990	Informational (Approved)
IPC	NATO	Electronically and/or Optically Generated Aircraft Displays for Fixed Wing Aircraft	STANAG 3648 of 6/29/1990	Informational (Approved)
IPC	NATO	Symbols on Land Maps, Aeronautical Charts and Special Naval Charts	STANAG 3675	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	NATO	Symbols for Use on Maps of Training Areas for Land Forces	STANAG 3833	Informational (Approved)
GPC	CJCS	Joint Symbols and Graphics	Joint Pub 1-06	Informational (Draft)
GPC	DOD (US Army)	Army Field Manual (FM): Operational Terms and Symbols	FM 101-5-1A SMIGS	Informational (Draft)
GPC	DOD (NIMA)	Vector Product Format Symbology	MIL-PRF-89045	Informational (Draft)
GPC	DOD (ASPO)	Symbol Automation	MIL-STD-2526	Informational (Draft)
GPC	DIA	Standard Military Graphics Symbols (SMIGS)	DIAM 65-xx	Informational (Draft)
IPC	NATO	Display Symbology and Colors for NATO Maritime Units	STANAG 4420	Informational (Formative)

3.6.4.1.2 Alternative specifications. No other consortia or de facto specifications are available.

3.6.4.1.3 Standards deficiencies. Draft MIL-STD-2525A does not currently contain weather, geospatial (mapping/charting), cockpit display, and engineering design symbology. Therefore NIMA MIL-STD-2402, 2412 should be used for geospatial symbology until such time as a decision is made to modify MIL-STD-2525A to accomodate these symbols.

3.6.4.1.4 Portability caveats. Portability will be reduced if a Geographic Information System (GIS) does not allow users to associate their cartographic data independently with relational database management systems based on Structured Query Language (SQL). Only government standards are available. Most commercial products will not comply with these standards.

3.6.4.1.5 Related standards. The following standards are related to symbology graphics or symbology graphics standards:

a. ISO 6937: Supplementary Characters (for accents to the text)
b. ISO 9292: Picture Coding
c. Autometric, Inc., Lakewood, CO: MOSS
d. Map graphics standards.

3.6.4.1.6 Recommendations. The adopted symbology standards are recommended, as applicable; MIL-STD 2525 is the recommended standard for warrior symbology.

3.6.4.2 Geospatial data interchange. (This BSA appears in part 5, Data Interchange, and part 6, Graphics.) These standards provide formats and facilities for machine-readable graphics-based mapping, charting, and geodesy data.

3.6.4.2.1 Standards. Table 3.6-8 presents standards for geospatial data interchange.

TABLE 3.6-8 Geospatial data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD (NIMA)	World Geodetic System (WGS 84)	MIL-STD-2401 of 21 March 1994	Mandated (Approved)
GPC	DOD (NIMA)	Raster Product Format (RPF)	MIL-STD-2411:1994	Mandated (Approved)
GPC	DOD (NIMA)	Interface Standard for Vector Product Format (VPF)	MIL-STD-2407	Mandated (Approved)
IPC	NATO	Digital Geographic Information Exchange Standard (DIGEST) Part 1 - Generic Standard Part 2 - Minimum Standards Specifications Part 3 - Matrix (Exchange of elevation of data) Part 4 - Spaghetti Vector	STANAG 7074	Informational (Approved)
GPC	NIST	Spatial Data Transfer Standard (SDTS)	FIPS PUB 173-1:1994	Informational (Approved)
IPC	NATO	Digital Terrain Elevation Data, (DTED)	STANAG 3809	Informational (Approved)
GPC	NIST	Representation of Geographic Point Locations for Information Interchange (adopts ANSI X3.61-1986)	FIPS PUB 70-1:1986	Informational (Approved)
GPC	NIST	Codes for Identification of Hydrologic Units in the United States and the Caribbean Outlying Areas (adopts USGS Circular 878-A and ANSI X3.145-1986)	FIPS PUB 103:1983	Informational (Approved)
GPC	DOD (NIMA)	NIMA GGI&S List of Products and Services	NIMAL 805-1A, Jan 1997	Informational (Approved)
GPC	DOD (NIMA)	Arc Digitized Raster Graphics Worldwide Map Images on CD-ROM, 1:5,000 through 1:2,000,000	MIL-A-89007 of 2/22/1990	Informational (Approved)
GPC	DOD (NIMA)	DTED (Machine readable terrain/elevation data for the U.S., the former USSR, Europe, Central Asia, Mideast, Parts of Southern Asia, Northern Canada, 3-Arc-Sec)	MIL-D-89000 of 2/26/90 MIL-D-89001 of 2/26/90 MIL-D-89020 of 5/28/93	Informational (Approved)
GPC	DOD (NIMA)	Digital Chart of the World (DCW) (A comprehensive 1:1,000,000-scale digital base map of the world)	MIL-D-89009 of 4/13/92	Informational (Approved)
GPC	DOD (NIMA)	Digital Cities Data Base (DCDB)	MIL-D-89011 of 7/2/90	Informational (Approved)
GPC	DOD (NIMA)	Firefinder Elevation Data (FED)	MIL-D-89018 of 10/1/92	Informational (Approved)
GPC	DOD (NIMA)	Digital Landmass Blanking (DLMB)	MIL-D-89021 of 6/15/91	Informational (Approved)
GPC	DOD (NIMA)	Interim Terrain Data/Planning Interim Terrain Data (ITD/PITD)	MIL-I-89014 of 11/30/90	Informational (Approved)
GPC	DOD (NIMA)	Video Disc for Mapping, Charting and Geodesy (Worldwide Map Images on 12 inch Video Disk, 1:50,000 through 1:1,000,000)	MIL-V-89300(1) of 11/30/92	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD (NIMA)	World Vector Shoreline (showing Worldwide Coastlines and International Boundaries, 1:250,000 scale)	MIL-W-89012(2) of 11/30/92	Informational (Approved)
GPC	DOD (NIMA)	World Magnetic Model (WMM)	MIL-W-89500 of 6/18/93	Informational (Approved)
GPC	DARPA	SIMNET Geographic Data Model and Database Interchange Specification	BBN DARPA Report 7108:July 1989	Informational (Approved)
GPC	NGDC	Worldwide Coverage for 5 Mini Grid maps: Bathymetric/Elevation Data	ETOPO 5	Informational (Approved)
GPC	USGS	LANDSAT: Worldwide Coverage for 1:1,000,000 Scale Maps: Feature/Terrain Data	LANDSAT	Informational (Approved)
IPC	NATO	Scope and Presentation of Military Geographic Information and Documentation	STANAG 2251	Informational (Approved)
IPC	NATO	Roads and Road Structures	STANAG 2253	Informational (Approved)
IPC	NATO	MGD-Ports	STANAG 2255	Informational (Approved)
IPC	NATO	Indexes to series of Land Maps and Aeronautical Charts and Indexes to Military Geographic Information and Documentation (MGID)	STANAG 3672	Informational (Approved)
IPC	NATO	Preferred Magnetic Tape Standards for the Exchange of Digital Geographic Information	STANAG 3985	Informational (Approved)
IPC	NATO	Digital Data File Transmittal Form for Geographic Information	STANAG 3986	Informational (Approved)
GPC	USGS	Specification for Representation of Geographic Point Locations for Information Interchange (adopts ANSI X3.61-1986)	USGS Circular 878-B of 1983	Informational (Approved)
GPC	USGS	Digital Elevation Models	USGS Circular 895-B of 1983	Informational (Approved)
GPC	USGS	Digital Line Graphs from 1:24,000 Scale Maps	USGS Circular 895-C of 1983	Informational (Approved)
GPC	USGS	Digital Line Graphs from 1:2,000,000 Scale Maps	USGS Circular 895-D of 1983	Informational (Approved)
GPC	USGS	Land Use and Land Cover Digital Data	USGS Circular 895-E of 1983	Informational (Approved)
GPC	USGS	Geographic Names Information System	USGS Circular 895-F of 1983	Informational (Approved)
GPC	CIA	World Data Bank II: Worldwide Coverage for 1:2,000,000 Scale Maps (Lines of Communication, Coastlines, Waterways, International/Political Boundaries)	World Data Bank II	Informational (Approved)
GPC	DOD (USAF)	Arc Digital Raster Imagery (ADRI) Format	MIL-STD-2406	Informational (Final)
GPC	DOD (NIMA)	Standard Linear Format (SLF) Digital Cartographic Feature	MIL-HDBK-854	Informational (Final)
GPC	DOD (AFMC)	Registered Data Values for Raster/Gridded Product Format	MIL-HDBK-856	Informational (Final)
GPC	DOD (NIMA)	Text Product Form (TPF)	MIL-STD-2400	Informational (Final)
GPC	DOD (NIMA)	Mapping Charting and Geodesy Symbology Graphics	MIL-STD-600002	Informational (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	NATO	Header Record Format for Exchange of Digital Geographic Information	STANAG 3984	Informational (Draft)
IPC	NATO	Digital Geographic Information Data Sets Series Numbering	STANAG 7070	Informational (Draft)
GPC	DOD (NIMA)	DFAD (Machine-readable feature data of the U.S., Europe, the former Western USSR, Limited Areas of Far East and Western Asia, 1:250,000 scale)	MIL-D-89005	Informational (Draft)
GPC	DOD (NIMA)	Tactical Terrain Data: Digital Database for 1:50,000 Scale Maps	TBD-Tactical Terrain Data: Digital Database for 1:50,000 Scale Maps	Informational (Formative)

3.6.4.2.2 Alternative specifications. Many existing proprietary map graphics applications vary in complexity to meet users' needs. These applications serve as the cornerstone of the mapping, charting, and geodesy areas requiring further investigation for standardization consideration.

3.6.4.2.3 Standards deficiencies. Many of the standards listed in the table accompanying this section are old. They do not accommodate new sophisticated computerized techniques, and probably will be replaced in the next several years. The standards available pertain almost exclusively to the data rather than the functionality of an application.

3.6.4.2.4 Portability caveats. Portability will be reduced if a GIS does not allow users to associate their cartographic data independently with relational database management systems based on SQL.

The use of different file formats by a GIS reduces portability. However, in the production world several file formats specified by vendors are used so widely that they are considered neutral file formats (e.g., Intergraph's Standard Interchange Format (SIF), Autodesk's Drawing Exchange Format (DXF), and MOSS).

Traditionally, standards governing exchanges among field systems have been the responsibility of the military system development organization. This leads to substantial interoperability problems, particularly international. To maximize interoperability, Digital Geographic Information Exchange Standard (DIGEST) and other map producing data should be exchanged between map-producing agencies, such as the National Imagery and Mapping Agency (NIMA) and not between operational units, and the systems development organizations should use the standards set by such agencies as the NIMA.

Portability difficulties may exist between the Vector Product Format (VPF) and the Spatial Transfer Specification (SDTS).

Portability can be especially difficult in an area where so many standards exist.

3.6.4.2.5 Related standards. The following standards are related to map graphics exchange or exchange standards:

a. ISO 646: 7-bit Coded Character Set for Information Interchange

b. ISO 1001: File Structure and Labeling of Magnetic Tapes for Information Interchange

c. ISO 2375: Non-Latin Alphabets

d. ISO 6937: Supplementary Characters (for accents to the text)

e. ISO 8211:1985 Specification for a Data Descriptive File for Information Exchange

f. ISO 8824/8825: ASN.1

g. ISO 9292: Picture Coding

h. ISO 9660:1988 Volume and File Structure of CD ROM for Information Exchange

i. ANSI/ASME Y14.26M-1989: IGES (Neutral file format)

j. Intergraph Corporation, Huntsville, AL: SIF

k. Autodesk, Inc., Sausalito, CA: DXF

l. Autometric, Inc., Lakewood, CO: MOSS

m. The various data compression standards listed earlier in the section on data compression

3.6.4.2.6 Recommendations. GIS specifications in a procurement should require SQL compatibility so that cartographic data can be associated independently with relational database management systems based on SQL. In each case, consideration of the scale of data and geographic region needed will be a primary determinant in selection. The standards in the table above labeled mandated are recommended. The VPF is preferred.

If a packaged GIS is to be purchased, if possible, it should be standardized around a single GIS file format. If a GIS is to be used on workstations and PCs, this may not be possible. Then the agency's focus will have to be on the use of interoperability protocols and designing applications for portability. GIS specifications should require SQL compatibility so that cartographic data can be associated independently with relational database management systems based on SQL.

3.6.5 Editors. An editor is a software program used to modify programs or files while they are being prepared, or after they are complete. A textual editor is a very rudimentary word processing program. The following editors provide the services for creating and editing nontextual data.

3.6.5.1 Graphics editor. A graphics editor provides an interactive editor to create, edit, and compose drawings, symbols, and maps.

3.6.5.1.1 Standards. Table 3.6-9 presents standards for graphics editors.

TABLE 3.6-9 Graphics editor standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.6.5.1.2 Alternative specifications. The only other available specifications are proprietary.

3.6.5.1.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.6.5.1.4 Portability caveats. This is a high portability risk area, because no standards exist.

3.6.5.1.5 Related standards. The following standards are related to graphics editor standards:

a. ISO 9592:1989 PHIGS.
b. ISO 7942:1985 GKS.
c. ISO 10918-1:1994 JPEG.
d. ISO 11172: MPEG.
e. ANSI X3H3.8: PIK.
f. ISO 10918-2.

3.6.5.1.6 Recommendations. Carefully match specific requirements for a graphics editor to the capabilities offered by any appropriate implementation.

3.6.5.2 Image processor editor. Image processing editors analyze a picture using techniques that can identify shades, colors, and relationships not perceptible by the human eye. These editors also perform image improvement, such as refining a picture in a paint program that has been scanned or entered from a video source.

3.6.5.2.1 Standards. Table 3.6-10 presents standards for image processor editors.

TABLE 3.6-10 Image processor editor standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.6.5.2.2 Alternative specifications. The only other available specifications are proprietary.

3.6.5.2.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.6.5.2.4 Portability caveats. This is a high portability risk area, because no standards exist.

3.6.5.2.5 Related standards. The following standards are related to image processor editor standards:

a. ISO 9592:1989 PHIGS
b. ISO 7942:1985 GKS
c. ISO 10918-1:1994 JPEG
d. ISO 11172: MPEG
e. ANSI X3H3.8: PIK
f. ISO 10918-2

3.6.5.2.6 Recommendations. There are no standards to recommend. It is suggested that requirements be specified to anticipate future needs.

3.6.5.3 Videoprocessor editor. Videoprocessing editors provide an interactive editor to capture, scan, create, and edit live, full-motion video.

3.6.5.3.1 Standards. Table 3.6-11 presents standards for videoprocessor editors.

TABLE 3.6-11 Videoprocessor editor standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.6.5.3.2 Alternative specifications. The only other available specifications are proprietary.

3.6.5.3.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.6.5.3.4 Portability caveats. This is a high portability risk area because no standards exist.

3.6.5.3.5 Related standards. The following standards are related to videoprocessor editor standards:

a. ISO 9592:1989 PHIGS
b. ISO 7942:1985 GKS
c. ISO 10918-1:1994 JPEG
d. ISO 11172: MPEG
e. ANSI X3H3.8: PIK
f. ISO 10918-2:JPEG

3.6.5.3.6 Recommendations. See the Image Processor Editor BSA.

3.6.6 Graphics search and sort. Graphics search and sort standards provide capability and standardized interface to search for and access graphical objects based on file attributes.

3.6.6.1 Graphics search. Graphics search standards provide the capability and standardized interface to search for and access graphical objects based on file attributes.

3.6.6.1.1 Standards. Table 3.6-12 presents standards for graphics searches.

TABLE 3.6-12 Graphics search standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.6.6.1.2 Alternative specifications. The only other available specifications are proprietary.

3.6.6.1.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.6.6.1.4 Portability caveats. This is a high portability risk area because no standards exist.

3.6.6.1.5 Related standards. The following standards are related to graphics search or graphics search standards:

a. ISO 9592:1989 PHIGS
b. ISO 7942:1985 GKS
c. ISO 10918-1:1994 JPEG
d. MIL-STD-188-198: JPEG
e. ISO 11172: MPEG
f. ANSI X3H3.8: PIK
g. ISO 10918-2 JPEG

3.6.6.1.6 Recommendations. Without standards, specifications should reflect current needs and anticipate future changes.

3.6.6.2 Image query and search. Image query and search standards provide the capability and standardized interface to search for and access image data based on file attributes.

3.6.6.2.1 Standards. Table 3.6-13 presents standards for image queries and searches.

TABLE 3.6-13 Image query and search standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.6.6.2.2 Alternative specifications. The only other available specifications are proprietary.

3.6.6.2.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.6.6.2.4 Portability caveats. This is a high portability risk area because no standards exist.

3.6.6.2.5 Related standards. The following standards are related to image query and search standards:

a. ISO 9592:1989 PHIGS
b. ISO 7942:1985 GKS
c. ISO 10918-1:1994 JPEG
d. ISO 11172: MPEG
e. ANSI X3H3.8: PIK
f. ISO 10918-2

3.6.6.2.6 Recommendations. No standard is available to recommend. Only a proprietary solution that best fits the requirements of the system or a custom-developed implementation is possible.

3.6.6.3 Graphical object sorting. Graphical object sorting standards provide the capability and standardized interface to arrange graphical objects and information in a specified order.

3.6.6.3.1 Standards. Table 3.6-14 presents standards for graphical object sorting.

TABLE 3.6-14 Graphical object sorting standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N/A	N.A.	None	N.A.	Informational (N.A.)

3.6.6.3.2 Alternative specifications. The only other available specifications are proprietary.

3.6.6.3.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.6.6.3.4 Portability caveats. This is a high portability risk area because no standards exist.

3.6.6.3.5 Related standards. The following standards are related to graphical object sorting standards:

a. ISO 9592:1989 PHIGS.
b. ISO 7942:1985 GKS.
c. ISO 10918-1:1994 JPEG.
d. ISO 11172: MPEG.
e. ANSI X3H3.8: PIK.
f. ISO 10918-2

3.6.6.3.6 Recommendations. No standards are available to recommend. See the Image query and search BSA.

3.6.7 Graphics security. Graphics security services include graphics security labeling.

3.6.7.1 Graphics security labeling. (This BSA appears in part 6 and part 10.) Graphics security labeling provides a security service for ensuring that graphical data includes labeling information in support of mandatory access control security services, marking security services, handling security services, aggregation security services, sanitization security services, and release security services. Security labeling services produce and maintain the integrity of the security label and its binding to the data with which it is associated.

3.6.7.1.1 Standards. Table 3.6-15 presents standards for graphics security labeling.

TABLE 3.6-15 Graphics security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GFC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	CMW Labeling Encoding Format	DDS-2600-6216-91	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Informational (Approved)

3.6.7.1.2 Alternative specifications. There are no other specifications.

3.6.7.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.6.7.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.6.7.1.5 Related standards. Graphics security labeling should be compatible with MIL-STD-2045-48501, Common Security Label, for any system with a communications interface.

DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

3.6.7.1.6 Recommendations. The mandated standard is recommended. Graphics security labeling should be based on the operating system security label standards. Graphics security labeling should employ binding of strength equal to or greater than that of the operating system. Compatible security labeling standards include the ability to perform a one-for-one mapping or translation between security labeling standards.

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 7 of 14 parts)

COMMUNICATIONS AND NETWORK SERVICES

Version 3.1 - April 7, 1997

AREA TCSS/IPSC/DCPS

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

FOREWORD

The ITSG is the foundation document for the Technical Architecture Framework for Information Management (TAFIM), Volume 7, the Adopted Information Technology Standards (AITS) and provides more detailed information about the standards adopted by the AITS.

The ITSG aligns with the major service areas of the reference model identified in the TAFIM, Volume 2, Technical Reference Model. It is divided by major service areas into separate parts. See part 1 of the ITSG for the table of major service areas and associated ITSG part numbers along with the POC for each major service area. This document, ITSG part 7, addresses the Communications and Network Services Major Service Area.

TABLE OF CONTENTS

LIST OF TABLES

3.7 Communications and network services. Provision of communications and network services for DOD users requires a set of information transfer standards encompassing all end systems and the subnetworks that interconnect them. Most end systems for data use the TCP/IP suite of internet protocols, which support internetworking operations over differing subnetwork technologies. Other end systems support voice, fax, messaging, and video services. This part of the ITSG identifies the base standards which support these communicating end systems, as well as the subnetwork technologies, the transmission systems, and the interworking protocols used to interconnect those end systems.

3.7.1 Base standards. Base standards supporting each of the BSAs are listed in tables provided in 3.7.2 to 3.7.9. The tables provide the standards organization numbers, titles, standards types, and base standards categories. Some of the most used standards types will appear in abbreviated form throughout this part. These types and their abbreviations are: Corporate Private Non-Consensus (CPN-C), Consortia Public Consensus (CPC), Government Public Consensus (GPC), International Public Consensus (IPC), and National Public Consensus (NPC). The ITSG, part 1, provides more information on these standards types. Some base standards are referenced more than once. For example, a base standard applicable to the user-to-network interfaces (UNI) may be referenced once as it applies to the end-system side of the UNI and again as it applies to the network side of the UNI.

3.7.1.1 Base standards categories. Base standards supporting each of the BSAs are categorized as *mandated, adopted, legacy, emerging,* and *informational.* These categories are in addition to the life-cycle status information usually presented. Each of these new categories is described in 3.7.1.1.1 to 3.7.1.1.5.

3.7.1.1.1 Mandated standard. The DOD status "Mandated" is used for those standards mandated by the JTA. A standard is mandatory in the sense that IF a service/interface is going to be implemented, it shall be implemented in accordance with the mandated standard. Although these standards are mandated for C4I only, they should be treated as recommended standards for non-C4I applications.

3.7.1.1.2 Adopted standard. The DOD status "Adopted" is used to mean that the standard in the ITSG is approved by DOD for use in satisfying a function of the BSA where there exists no JTA mandated standard where joint interoperability is impacted. Adopted standards may be implemented but shall not be used in lieu of a mandated standard. Adopted standards also appear in the top rows of the standards tables in the ITSG and are bordered with heavy black lines.

3.7.1.1.3 Legacy standard. A "Legacy" standard is a standard necessary to achieve or maintain interoperability with legacy systems. Legacy systems are systems that are in current use. Legacy standards are not recommended for future procurements. Legacy standards may be supported until the legacy system is no longer being maintained. Examples of legacy standards are X.25 packet switching standards and TRI-TAC/Mobile Subscriber Equipment (MSE) System standards such as MIL-STD-188-256.

3.7.1.1.4 Emerging standard. According to the JTA, a DOD "Emerging" status denotes a candidate standard to be added as, or to replace, a mandated standard. This includes standards required to capitalize on new technologies. These candidates will help the program manager determine those areas that are likely to change in the near term (within three years) and suggest those areas in which "upgradability" should be a concern. The expectation is that emerging standards will be elevated to mandated status in the JTA when implementations of the standards mature. Emerging standards may be implemented but shall not be used in lieu of a mandated standard.

3.7.1.1.5 Informational standard. Informational standards include those remaining standards that fall outside the official DOD status of "mandated", "adopted", "emerging", and "legacy".

3.7.1.2 IAB standards. A number of standards mandated in this part are published by the Internet Architecture Board (IAB), which is responsible for the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and which documents these standards. A list of IAB standards cited in this part of the ITSG and the Request For Comments (RFCs) that make up these standards is given in Table 3.7-1. IAB standards can be obtained via electronic mail from FTP.ISI.EDC by using the RFC-INFO service. Address the request to "rfc-info@isi.edu" with a message body of:

Retrieve: STD
Doc-ID: STDnnnn (where nnnn refers to the number of the STD, e.g., STD0002 for IAB STD 2)

IAB standards, and other Internet documentation, can also be obtained via a WWW browser from URL http://ds.internic.net/ds/dspg0intdoc.html.

TABLE 3.7-1 IAB Standards and RFCs

IAB STANDARD		RFC NUMBER
IAB STD	NAME	
3	Host Requirements	1122, 1123
5	Internet Protocol	0791, 0950, 0919, 0922, 0792, 1112
6	User Datagram Protocol	0768
7	Transmission Control Protocol	0793
8	TELNET Protocol	0854, 0855
9	File Transport Protocol	0959
13	Domain Name System	1034, 1035
15	Simple Network Management Protocol	1157

IAB STANDARD		RFC NUMBER
IAB STD	NAME	
16	Structure of Management Information	1155, 1212
17	Management Information Base	1213
33	Trivial File Transfer Protocol	1350
35	ISO Transport Service on Top of the TCP	1006
37	An Ethernet Address Resolution Protocol	0826
38	A Reverse Address Resolution Protocol	0903
41	Standard for the Transmission of IP Datagrams over Ethernet Networks	0894
43	Standard for the Transmission of IP Datagrams over IEEE 802 Networks	1042
51	The Point-to-Point Protocol (PPP)	1661, 1662

3.7.2 Communications for end systems. End systems may be host computers [data terminal equipment (DTE)], video teleconferencing (VTC) terminals, facsimile terminals, secondary imagery terminals, or telephone terminals.

3.7.2.1 Host application support. Hosts are end-user computer systems that connect to a network. They perform numerous functions corresponding to all layers of the International Standards Organization (ISO) reference model. Host standards for internetwork routing and the higher layers are required so that communicating hosts can interoperate. Lower-layer standards depend on the particular network interface. Base standards for host applications are presented in table 3.7-2.

3.7.2.1.1 Standards. Base standards for host applications are presented in table 3.7-2.

TABLE 3.7-2 Application support standards for hosts

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	Host Requirements	Standard 3/RFC-1122/RFC-1123	Mandated (Approved)
IPC	IAB	TELNET Protocol	Standard 8/RFC-854/RFC-855	Mandated (Approved)
IPC	IAB	File Transfer Protocol	Standard 9/RFC-959	Mandated (Approved)
CPC	IETF	Network Time Protocol (V3)	RFC 1305:1992	Mandated (Approved)
CPC	IETF	Hypertext Transfer Protocol -- HTTP/1.0	RFC 1945:1996	Mandated (Approved)
GPC	DOD	Common Messaging Strategy and Procedures, November 1995	ACP 123 US Supplement No. 1	Mandated (Approved)
IPC	ITU-T	The Directory - Overview of Concepts, Models and Services - Data Communication Networks Directory, 1993	X.500	Mandated (Approved)
GPC	DOD	Connectionless Data Transfer Application Layer Standard, July 27, 1995	MIL-STD-2045-47001	Mandated (Approved)

3.7.2.1.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.2.1.3 Standards deficiencies. The Directory Implementor's Guide, Version 9, April 1996, provides reported defects and their resolutions to the 1988 and 1993 editions of the ITU-T Recommendations X.500. It also includes all approved and draft corrigenda to both editions of the directory specification.

3.7.2.1.4 Portability caveats. X.500 implementations based on 1988 and 1993 specifications will not interoperate if the resolution of defect 052 to the 1988 specification, which provides for version negotiation and rules for extensibility, has not been incorporated.

3.7.2.1.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. IAB STD 27, Telnet binary transmission, 5/1/83.

2. IAB STD 28, Telnet echo option, 5/1/83.

3. IAB STD 32, Telnet extended options: List option, 5/1/83.

4. RFC 1495, Mapping between X.400 and RFC-822 Message Bodies, 8/26/93.

5. RFC 1415, FTP-FTAM gateway specification, 1/27/93.

6. RFC 1708, NTP PICS PROFORMA for the Network Time Protocol, Version 3, 10/26/94.

7. IAB STD 10, SMTP service extensions, 11/6/95.

8. RFC 1830, SMTP Service Extensions for Transmission of Large and Binary MIME Messages, 8/16/95.

3.7.2.1.6 Recommendations. The following base standards should be used in support of related procurements:

a. The standard for electronic-mail support, used by the Defense Message System (DMS), is the International Telecommunications Union - Telecommunication Standardization Sector (ITU-T) X.400-based suite of military messaging standards defined in Allied Communication Publication (ACP) 123, U.S. Supplement No. 1. The U.S. Supplement contains standards profiles that define the DMS "Business Class Messaging" (P772) capability and the Message Security Protocol (MSP). The DMS will interface to SMTP by using multifunction interpreters (MFI). Some loss of functionality will occur when a gateway is used.

b. The X.500 protocol supports individual and organizational directory services and is mandated for use with DMS. X.500 supports directory services that may be used by users or host applications to locate other users and resources on the network. X.500 also supports security services used by DMS-compliant X.400 implementations.

c. The File Transfer Protocol (FTP) will be used in support of basic file transfer. FTP provides a reliable, file transfer service for text or binary files.

d. Basic remote terminal services are supported by the Telecommunications Network (TELNET) protocol. TELNET provides a virtual terminal capability that allows

users to log on to remote systems as if the user's terminal were directly connected to the remote system.

e. IAB STD 3, an umbrella standard, references other documents and corrects errors in some of the referenced documents. IAB STD 3 also adds additional discussion and guidance for implementors.

f. RFC 1305 specifies the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet.

g. RFC 1945 specifies methods for search and retrieval within the World Wide Web.

h. MIL-STD-2045-47001 supports VMF message transmission using a connectionless application layer.

3.7.2.2 Information transport. Information-transport services provide host-to-host communications capability for application-support services.

3.7.2.2.1 Standards. Base standards for information transport are shown in table 3.7-3.

TABLE 3.7-3 Host standards for information transport

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	Host Requirements	Standard 3/RFC-1122/RFC-1123	Mandated (Approved)
IPC	IAB	Internet Protocol	Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112	Mandated (Approved)
IPC	IAB	User Datagram Protocol	Standard 6/RFC-768	Mandated (Approved)
IPC	IAB	Transmission Control Protocol	Standard 7/RFC-793	Mandated (Approved)
IPC	IAB	ISO Transport Service on top of the TCP	Standard 35/RFC-1006	Mandated (Approved)
GPC	DOD	Internet Transport Profile for DoD Communications - Transport and Internet Services	MIL-STD-2045-14502-1A	Mandated (Approved)
IPC	ISO	Connection Oriented Transport Layer Specification (for TP0 only)	ISO 8073	Legacy (Approved)
IPC	ISO	X.25 Packet Level Protocol for DTE	ISO 8208	Legacy (Approved)
IPC	ISO	Use of X.25 to Provide the CONS	ISO 8878	Legacy (Approved)
CPC	IETF	IPv6 Specification	RFC 1883:1995	Emerging (Approved)
CPC	IETF	ICMPv6 for IPv6	RFC 1885:1995	Emerging (Approved)
CPC	IETF	Transition Mechanisms for IPv6 Hosts and Routers	RFC 1933:1996	Emerging (Draft)

3.7.2.2.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.2.2.3 Standards deficiencies. IPv4 does not provide security features such as authentication and privacy.

3.7.2.2.4 Portability caveats. There are many RFCs that specify extensions to TCP. Most vendors' products contain extensions. To maximize portability, reduce the use of extensions as much as possible.

3.7.2.2.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. RFC 1693, An extension to TCP: Partial Order Service, 11/1/94.
2. RFC 1644, T/TCP -- TCP Extensions for Transactions Functional Specification, 7/13/94.
3. RFC 1323, TCP Extensions for High Performance, 5/13/92.
4. RFC 1144, Compressing TCP/IP headers for low-speed serial links, 2/1/90.
5. RFC 1072, TCP extensions for long-delay paths, 10/1/88.
6. RFC 1240, OSI Connectionless Transport Services on Top of UDP - Version 1, 5/26/91.

3.7.2.2.6 Recommendations. The following base standards should be used in support of related procurements:

a. IAB-STD-7 specifies the Transmission Control Protocol (TCP). TCP is the standard transport-level protocol most commonly used and is the protocol upon which many application-support protocols depend. TCP, as mandated by JTA, implements the PUSH flag and the Nagle Algorithm defined in IAB-STD-3.

b. IAB-STD-6 specifies the User Datagram Protocol (UDP). UDP is an alternative transport-level protocol that provides an unacknowledged, connectionless, datagram transport service.

c. IAB-STD-5 specifies the Internet Protocol (IP). RFCs corresponding to this standard are referenced in table 3.7-1. Both TCP and UDP use the IP to transport information across internetworks. IP supports connectionless datagram service. All protocols within the IP suite use IP datagrams as the basic data transport mechanism. Two other protocols are considered integral parts of IP: the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP). ICMP is used to provide error reporting, flow control, and route redirection. IGMP provides multicast extensions for hosts to report their group membership to multicast routers. In addition, all implementations of IP must pass received type-of-service (TOS) values up to the transport layer.

d. MIL-STD-2045-14502-1A specifies a military-unique IP option field that must be used for hosts that are required to transmit or receive multiaddressed datagrams over combat net radio (CNR).

e. IAB-STD-35 supports interworking between Transport Protocol Class 0 (TP0) and TCP transport service when it is necessary for Open Systems Interconnection (OSI) applications to operate over IP-based networks. TP0 is defined by ISO 8073.

f. ISOs 8208 and 8878 are layer 3 standards for legacy X.25 network interfaces.

g. RFC 1883 specifies a new version of IP (IPv6), which has been approved by the Internet Engineering Task Force (IETF). The current version of IP (IPv4)

provides only 32 bits of address space and is facing an inability to provide unique addresses at all entities that require them. RFC 1885 specifies a new internet control message protocol for IPv6. The changes from IPv4 to IPv6 are primarily in the following categories:

- expanded addressing capabilities
- header format simplification
- improved support for extensions and options
- flow labeling capability
- authentication and privacy capabilities.

h. RFC 1933 specifies IPv4 compatibility mechanisms that can be implemented by IPv6 hosts and routers. These mechanisms are designed to allow IPv6 nodes to maintain complete compatibility with IPv4.

3.7.2.3 Domain name system and internet protocol addressing. Domain Name System (DNS), an on-line distributed database system, is used to map human-readable machine names into IP addresses. DNS servers throughout the interconnected internet implement a hierarchical name space that allows sites freedom in assigning machine names and addresses.

3.7.2.3.1 Standards. Base standards relevant to Domain Name System (DNS) and IP Addressing are presented in table 3.7-4.

TABLE 3.7-4 Domain name system and IP addressing standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	Domain Name System	Standard 13/RFC-1034/RFC-1035	Mandated (Approved)
CPC	IETF	Bootstrap Protocol	RFC 951:1985	Mandated (Approved)
CPC	IETF	DHCP Options and BOOTP Vendor Extensions	RFC 1533:1993	Mandated (Approved)
CPC	IETF	Dynamic Host Configuration Protocol (DCHP)	RFC 1541:1993	Mandated (Approved)
CPC	IETF	Clarifications and Extensions for the Bootstrap Protocol	RFC 1542:1993	Mandated (Approved)
CPC	IETF	Uniform Resource Locators	RFC 1738:1994	Mandated (Approved)
CPC	IETF	Relative Uniform Resource Locators	RFC 1808:1995	Mandated (Approved)
CPC	IETF	IPv6 Addressing Architecture	RFC 1884:1995	Emerging (Approved)
CPC	IETF	DNS Extensions to Support IPv6	RFC 1886:1995	Emerging (Approved)
CPC	IETF	IP Mobility Support	RFC 2002:1996	Emerging (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.7.2.3.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.2.3.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.2.3.4 Portability caveats. There are many RFCs that specify extensions to DNS. Most vendors' products contain extensions. To maximize portability, reduce the use of extensions as much as possible.

3.7.2.3.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. RFC 1887, An Architecture for IPv6 Unicast Address Allocation, 1/4/96.

2. RFC 1971, IPv6 Stateless Address Autoconfiguration, 8/16/96.

3. RFC 1912, Common DNS Operational and Configuration Errors, 2/28/96.

4. RFC 1664, Using the Internet DNS to Distribute RFC 1327 Mail Address Mapping Tables, 8/11/94.

5. RFC 1536, Common DNS Implementation Errors and Suggested Fixes, 10/6/93.

6. RFC 1534, Interoperation Between DHCP and BOOTP, 10/8/93.

3.7.2.3.6 Recommendations. The following base standards should be used in support of related procurements:

a. IAB-STD-13 supports computer-addressing services and is mandated for IP-based services. The DNS translates between host names and IP addresses.

b. RFC-951 specifies the Bootstrap Protocol (BOOTP), which assigns IP addresses to workstations with no current IP address.

c. RFCs 1533, 1541, and 1542 specify the Dynamic Host Configuration Protocol (DHCP), which provides an extension of BOOTP to support the passing of configuration information to internet hosts. DHCP consists of two parts, a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for automatically allocating IP addresses to hosts.

d. RFCs 1738 and 1808 specify the Uniform Resource Locator (URL) for locating resources on an internet.

e. RFC 1884 defines the addressing architecture of the IP Version 6 protocol (IPv6). RFC 1886 defines the changes that need to be made to the Domain Name System to support hosts running IPv6.

f. RFC 2002 specifies protocol enhancements that allow transparent routing of IP datagrams to mobile nodes in the Internet. "Mobility Support in IPv6" is an internet draft that specifies the operation of mobile computers using IPv6.

3.7.2.4 Network management for hosts. The objective of network management is to support the establishment, reconfiguration, and maintenance of a stable signaling and user-to-network environment.

3.7.2.4.1 Standards. Base standards for network management of hosts are presented in table 3.7-5.

TABLE 3.7-5 Host standards for network management

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	Simple Network Management Protocol (SNMP)	Standard 15/RFC-1157	Mandated (Approved)
IPC	IAB	Structure of Management Information (SMI)	Standard 16/RFC-1155/RFC-1212	Mandated (Approved)
IPC	IAB	Management Information Base	Standard 17/RFC-1213	Mandated (Approved)
CPC	IETF	Structure of Management Information for Version 2 of the Simple Network Management Protocol	RFC 1902:1996	Informational (Approved)
CPC	IETF	Conformance Statements for Version 2 of the Simple Network Management Protocol	RFC 1904:1996	Informational (Approved)
CPC	IETF	Protocol for Operations for Version 2 of the Simple Network Management Protocol	RFC 1905:1996	Informational (Approved)
CPC	IETF	agement Information Base for Version 2 of the Simple Network Management Protocol	RFC 1907:1996	Informational (Approved)

3.7.2.4.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.2.4.3 Standards deficiencies. The chief disadvantage of SNMPv1 is the fact that its simplicity severely limits the protocol's ability to satisfy users' requirements for event reporting, sufficient control, and extensibility. Because SNMPv1 is so simplistic and limited, it provides more of a monitoring and data gathering capability than a management function.

The SNMPv1 accommodates only limited event reporting by means of the "trap" mechanism. Other events must be discovered by the managing node by means of periodic polling. Its simplicity compromises its ability to support consistent or extensive addressing. It has limited security capabilities, and does not support threshold-driven performance notification except indirectly through side effects or "set" operations on MIB items. SNMP cannot be extended easily.

3.7.2.4.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.2.4.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. RFC 1908, Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework, 1/22/96.

2. RFC 1461, SNMP MIB Extension for Multiprotocol Interconnect over X.25, 5/27/93.

3. RFC 1449, Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), 5/3/93.

4. RFC 1446, Security Protocols for Version 2 of the Simple Network Management Protocol (SNMPv2), 5/3/93.

5. RFC 1445, Administrative Model for Version 2 of Simple Network Management Protocol (SNMPv2), 5/3/93.

6. RFC 1443, Textual Conventions for Version 2 of Simple Network Management Protocol (SNMPv2), 5/3/93.

7. RFC 1441, Introduction to Version 2 of the Internet-standard Network Management Framework, 5/3/93.

3.7.2.4.6 Recommendations. The following base standards should be used in support of related procurements:

a. Hosts will use the Simple Network Management Protocol (SNMP) set of network management protocols. SNMP v1 is specified in IAB-STD-15, -16, and -17.

b. SNMP v2 adds security and authentication capabilities and a new manager-to-manager relationship for distributed management. SNMP v2, which is backward-compatible with SNMP v1, is specified in RFCs 1902, 1904, 1905, and 1907. SNMP v2 has not been accepted by the industry, and few vendors include SNMP v2 in their products. The main complaints focus on the complex design of the security and administrative framework. The IETF is presently working on a next generation version called SNMPng. The first set of internet-drafts are expected in the Spring of 1997.

3.7.2.5 Video teleconferencing. DOD and the video teleconferencing (VTC) industry have developed a profile to provide a standards-based reference document for users as an aid in defining procurement specifications for VTC equipment.

3.7.2.5.1 Standards. Base standards for VTC are presented in table 3.7-6.

TABLE 3.7-6 VTC standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Industry Profile for Video Teleconferencing	VTC001, Revision 1, April 25, 1995	Mandated (Approved)
IPC	ITU-T	Terminal for Low Bit Rate Multimedia Communications, March 19, 1996	H.324	Mandated (Approved)
IPC	ITU-T	VTC over ATM	H.321	Emerging (Approved)
IPC	ITU-T	VTC over Ethernet	H.323	Emerging (Approved)

3.7.2.5.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.2.5.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.2.5.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.2.5.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. FIPS PUB 178, Video Teleconferencing Services at 56 to 1,920 Kb/s, 1992.

2. ANSI T1.314, Digital Processing of Video Signals - Video Coder/Decoder for Audiovisual Services at 56 to 1536 kbits/s, 1991.

3. ANSI T1.801.01, Telecommunications - Digital Transport of Video Teleconferencing/ Video telephony Signals - Video Test Scenes for Subjective and Objective Performance Assessment.

4. RFC 1890, RTP Profile for Audio and Video Conferences with Minimal Control, 1/25/96.

3.7.2.5.6 Recommendations. The following base standards should be used in support of related procurements:

a. VTC 001 applies to video teleconferencing terminals. VTC 001 is based on the H.320 and T.120 series of recommendations and is independent of the type of underlying network service.

b. FIPS PUB 178 is based on the H.320 series of recommendations but lacks the additional DOD requirements contained in VTC 001. The new version of FIPS PUB 178 includes these DOD requirements. Appendix A of the FIPS PUB 178-1 contains VTC 001. FIPS PUB 178-1 is awaiting final approval from NIST. FIPS PUB 178-1 will replace VTC 001 as the DOD mandated standard.

c. ITU-T H.321 and H.323 are emerging standards that support VTC over ATM and Ethernet networks.

d. ITU-T H.324 has been mandated by the JTA for VTC terminals that operate at low bit rates (9.6 to 28.8 kbps).

3.7.2.6 Facsimile. Facsimile terminals may be procured with either a standard analog interface or a standard digital interface.

3.7.2.6.1 Standards. Base standards for facsimile are presented in table 3.7-7.

TABLE 3.7-7 Facsimile standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	EIA/TIA	Group 3 Facsimile Apparatus for Document Transmission, March 21, 1995	465-A	Mandated (Approved)
CPC	EIA/TIA	Procedures for Document Facsimile Transmission	466-A	Mandated (Approved)
GPC	DOD	Interoperability and Performance Standards for Digital Facsimile Equipment, January 10, 1995	MIL-STD-188-161D	Mandated (Approved)

3.7.2.6.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.2.6.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.2.6.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.2.6.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. MIL-STD-188-114A, Electrical Characteristics of Digital Interface Circuits, 12/91.

2. STANAG 5000, Interoperability of Tactical Digital Facsimile Equipment.

3.7.2.6.6 Recommendations. The following base standards should be used in support of related procurements:

a. Facsimile requirements for analog output shall comply with ITU-T Group 3 specifications given in Electronics Industries Association/Telecommunications Industry Association (EIA/TIA) Standards 465-A and 466-A.

b. Digital facsimile terminals operating in tactical, high bit error ratio (BER) environments shall implement digital facsimile equipment standards for Type I, Type II, or both, modes specified in MIL-STD-188-161D. Facsimile transmissions requiring encryption shall also use this military standard.

3.7.2.7 Secondary imagery dissemination. National Imagery Transmission Format (NITF) Standards (NITFS) define the standard formats for digital imagery and imagery-related products to be exchanged between members of the Intelligence Community, DoD, and other departments and agencies of the United States Government. The NITFS includes supporting standards for imagery, image compression, other imagery-related requirements, and the Tactical Communications 2 (TACO2) protocol. The document structure for current and anticipated NITFS documentation is described in MIL-HDBK-1300A.

3.7.2.7.1 Standards. Base standards for secondary imagery dissemination are presented in table 3.7-8.

TABLE 3.7-8 Secondary imagery dissemination standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	National Imagery Transmission Standard (NITFS) Tactical Communications Protocol 2 (TACO2), June 18, 1993	MIL-STD-2045-44500	Mandated (Approved)
GPC	DOD	National Imagery Transmission Format (Version 2.0) for file format	MIL-STD-2500A	Mandated (Approved)
GPC	DOD	Bi-Level Image Compression	MIL-STD-188-196	Mandated (Approved)
GPC	DOD	Joint Photographic Experts Group (JPEG) Image Compression for the NITFS (for Gray Scale and Still Color Images)	MIL-STD-188-198A of 12/15/1993	Mandated (Approved)
GPC	DOD	Vector Quantization (VQ) Decompression	MIL-STD-188-199	Mandated (Approved)
GPC	DOD	Adaptive Recursive Interpolated Differential Pulse Code Modulation (ARIDPCM) for the National Imagery Transmission Format Standards (NITFS)	MIL-STD-188-197A of 10/12/1994	Legacy (Approved)

3.7.2.7.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.2.7.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.2.7.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.2.7.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

MIL-HDBK-1300A, National Imagery Transmission Format Standard, 10/12/94.

3.7.2.7.6 Recommendations. The following base standards should be used in support of related procurements:

a. MIL-STD-2045-44500 is the standard mandated for Tactical Communications Protocol 2 (TACO2). TACO2 is the communications component of the National

Imagery Transmission Format Standard (NITFS) suite of standards used to disseminate secondary imagery. TACO2 supports operation over point-to-point tactical data links in high BER communications environments. TACO2 applies only to users that have simplex and half-duplex links as their only means of communications.

b. MIL-STD-2500A is the NITF Standard that provides a detailed description of the overall structure of the file format, as well as specification of the valid data content and format for all fields defined within a NITF file.

c. The MIL-STD-188-196/199 series defines compression algorithms for imagery. For more information on JPEG standard see ITSG, part 5, Data Interchange Services.

3.7.2.8 High-level data link control protocols. Link-layer protocols based on high-level data link control (HDLC) protocols are used by packet-switched networks, hosts, routers, and for Narrowband-Integrated Services Digital Network (N-ISDN) signaling messages.

3.7.2.8.1 Standards. Base standards for high-level data link control (HDLC)-based link-layer protocols are presented in table 3.7-9.

TABLE 3.7-9 HDLC-based link-layer protocol standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ITU-T	ISDN User-Network Interface - Data Link Layer Specification - Digital Subscriber Signaling System No. 1, 1993	Q.921	Mandated (Approved)
IPC	ISO	HDLC Frame Structures	3309	Legacy (Approved)
IPC	ISO	HDLC Elements of Procedures	4335	Legacy (Approved)
IPC	ISO	X.25 LAPB-Compatible DTE Data Link Procedures	7776	Legacy (Approved)
IPC	ISO	HDLC Procedures, Data-Link Layer Address Resolution/Negotiation in Switched Environments	8471	Legacy (Approved)
IPC	ISO	HDLC Procedures, General Purpose XID Frame Information Field Content and Format	8885	Legacy (Approved)

3.7.2.8.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.2.8.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.2.8.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.2.8.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

ISO 7809, Information Technology - Telecommunications and Information Exchange Between Systems - High-Level Data Link Control (HDLC) Procedures - classes of procedures, Third Edition.

3.7.2.8.6 Recommendations. The following base standards should be used in support of related procurements:

The X.25 link-layer protocol, known as link access procedure balanced (LAPB), is a subset of HDLC and uses the frame structure and procedures specified in ISO 3309 and 4335. LAPB for hosts is specified in ISO 7776. Link-layer address resolution and XID procedures for legacy packet-switch networks is supported by ISO 8471 and 8885, respectively.

LAPD is specified in ITU-T Q.921. LAPD is used as a data link control for ISDN. LAPD differs from LAPB in the following ways:

1. LAPD is designed for multiple access on the link. LAPB is intended for point-to-point operating.

2. LAPD and LAPB use different timers.

3. The address structures are different.

4. LAPD implements HDLC unnumbered information frame (UI). LAPB uses only sequenced information frames.

3.7.2.9 Record traffic protocol. Legacy formal record traffic systems are based on legacy interoperability standards. These standards shall be supported until the legacy systems are replaced by the Defense Message System (DMS).

3.7.2.9.1 Standards. Base standards for record traffic protocols are presented in table 3.7-10.

TABLE 3.7-10 Record traffic protocol standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Interoperability Standards for Information and Record Traffic Exchange, Mode I	MIL-STD-188-171	Legacy (Approved)
GPC	DOD	Interoperability Standards for Information and Record Traffic Exchange, Mode II	MIL-STD-188-172	Legacy (Approved)
GPC	DOD	Interoperability Standards for Information and Record Traffic Exchange, Mode V	MIL-STD-188-173	Legacy (Approved)
GPC	DOD	Interoperability Standards for Information and Record Traffic Exchange, Mode VI	MIL-STD-188-174	Legacy (Approved)

3.7.2.9.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.2.9.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.2.9.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.2.9.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. JANAP 128 Joint Army/Navy/Air Force Publication 128: AUTODIN Operating Procedures, March 1983.

2. ACP 127 Message Relay procedures.

3. Digital Equipment Corporation (DEC) Digital Data Communications Message Protocol (DDCMP).

3.7.2.9.6 Recommendations. The following base standards should be used in support of related procurements:

a. MIL-STD-188-171 will provide the Mode I channel coordination procedure for synchronous, simultaneous, duplex data transfer over terrestrial links.

b. MIL-STD-188-172 will provide the Mode II non-ARQ channel coordination procedure for asynchronous, simultaneous, independent, duplex data transfer.

c. MIL-STD-188-173 will provide the Mode V ARQ channel coordination procedure for asynchronous, simultaneous, independent, duplex data transfer.

d. MIL-STD-188-174 will ·ovide the Mode V ARQ channel coordination procedure for asynchronous, simultaneous, duplex data transfer.

3.7.2.10 Voice encoding for end systems. Several different voice digitization algorithms may be used to support digital voice applications. The method used depends on available bandwidth and type of interface.

3.7.2.10.1 Standards. Base standards for voice encoding are presented in table 3.7-11.

TABLE 3.7-11 Voice encoding standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ITU-T	Pulse Code Modulation (PCM) of voice frequencies (narrowband)	G.711:1989	Adopted (Approved)
IPC	ITU-T	32 kbits/s Adaptive Differential Pulse Code Modulation (ADPCM) - General Aspects of Digital Transmission Systems	G.721:1989	Adopted (Approved)
GPC	NCS	Linear Predictive Coding (LPC)	FED-STD-1015	Adopted (Approved)
GPC	NCS	Analog-to-Digital Conversion of Radio Voice by 4800-bps Code Excited Linear Prediction (CELP0	FED-STD-1016	Adopted (Approved)
GPC	DOD	Analog-to-Digital Conversion Techniques (for CVSD Modulation)	MIL-STD-188-113	Legacy (Approved)

3.7.2.10.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.2.10.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.2.10.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.2.10.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. ANSI T1.302, Telecommunications - Digital Processing of Voice-Band Signals - Line Format for 32-kbits/s Adaptive Differential Pulse-Code Modulation (ADPCM).

2. ANSI T1.310, Telecommunications - Digital Processing of Voice-Band Signals - Algorithms for 5-, 4-, 3-, and 2-bit/Sample Embedded Adaptive Differential Pulse-Code Modulation (ADPCM).

3. ANSI T1.501, Telecommunications - Network Performance - Tandem Encoding Limits for 32 kbits/s Adaptive Differential Pulse-Code Modulation (ADPCM).

3.7.2.10.6 Recommendations. The following base standards should be used in support of related procurements:

a. ITU-T G.711 specifies 64-kbps pulse-code modulation (PCM) for both mu-law and A-law companding.

b. MIL-STD-188-113 specifies 16-kbps continuously variable slope delta (CVSD) modulation.

c. FED-STD-1015 specifies 2.4-kbps linear predictive coding (LPC).

d. FED-STD-1016 specifies 4.8-kbps code-excited linear prediction (CELP).

e. ITU-T G.721 specifies 32-kbps adaptive differential pulse-code modulation (ADPCM).

3.7.3 Communications services for networks. This section addresses standards for different types of networks and other network-related topics. Networks include router networks, local area networks (LANs), packet switch, point-to-point, combat net radio, N-ISDN, broadband-ISDN (B-ISDN), and the asynchronous transfer mode (ATM). Network-related topics include voice digitization, timing and synchronization, network management, interworking, and personal communications services.

3.7.3.1 Routers. IP routers perform internetwork routing. They also perform interface functions needed to pass packets between different networks. IP routers route packets based on destination subnetwork addresses, not destination end-system addresses. IP routers may exist any place within the Defense Information Systems Network (DISN) as either interior or exterior gateways. For the purpose of routing, a group of networks and gateways controlled by a single administrative authority is called an *autonomous system*, which uses interior gateway protocols. Gateways between autonomous systems use exterior gateway protocols.

3.7.3.1.1 Standards. Base standards for routers are presented in table 3.7-12.

TABLE 3.7-12 Router standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	Internet Protocol	Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112	Mandated (Approved)
IPC	IAB	User Datagram Protocol	Standard 6/RFC-768	Mandated (Approved)
IPC	IAB	Transmission Control Protocol	Standard 7/RFC-793	Mandated (Approved)
IPC	IAB	TELNET Protocol	Standard 8/RFC-854/RFC-855	Mandated (Approved)
IPC	IAB	Domain Name System	Standard 13/RFC-1034/RFC-1035	Mandated (Approved)
IPC	IAB	Simple Network Management Protocol (SNMP)	Standard 15/RFC-1157	Mandated (Approved)
IPC	IAB	Structure of Management Information (SMI)	Standard 16/RFC-1155/RFC-1212	Mandated (Approved)
IPC	IAB	Management Information Base	Standard 17/RFC-1213	Mandated (Approved)
IPC	IAB	Trivial FTP (TFTP), to be used for initialization only.	Standard 33/RFC-1350	Mandated (Approved)
CPC	IETF	Bootstrap Protocol	RFC 951:1985	Mandated (Approved)
CPC	IETF	DHCP Options and BOOTP Vendor Extensions	RFC 1533:1993	Mandated (Approved)
CPC	IETF	Dynamic Host Configuration Protocol (DCHP)	RFC 1541:1993	Mandated (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	IETF	Clarifications and Extensions for the Bootstrap Protocol	RFC 1542:1993	Mandated (Approved)
CPC	IETF	Open Shortest Path First Routing Version 2, for unicast routing	RFC 1583:1994	Mandated (Approved)
CPC	IETF	Multicast Extensions to OSPF for multicast routing	RFC 1584:1994	Mandated (Approved)
CPC	IETF	Border Gateway Protocol 4	RFC 1771:1995	Mandated (Approved)
CPC	IETF	Application of BGP In the Internet	RFC 1772:1995	Mandated (Approved)
CPC	IETF	Requirements for IP Version 4 Routers	RFC 1812:1995	Mandated (Approved)
CPC	IETF	IPv6 Specification	RFC 1883:1995	Emerging (Approved)
CPC	IETF	IPv6 Addressing Architecture	RFC 1884:1995	Emerging (Approved)
CPC	IETF	ICMPv6 for IPv6	RFC 1885:1995	Emerging (Approved)
CPC	IETF	DNS Extensions to Support IPv6	RFC 1886:1995	Emerging (Approved)

3.7.3.1.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.3.1.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.3.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.3.1.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. RFC 1970, Neighbor Discovery for IP Version 6 (IPV6), 8/16/96.
2. RFC 1933, Transition Mechanisms for IPv6 Hosts and Routers, 4/8/96.

3.7.3.1.6 Recommendations. The following base standards should be used in support of related procurements:

a. The following standards and RFCs that were mandated for hosts in section 3.7.2.1 also apply to routers: IAB-STD-5, -6, -7, -8, -13, -15, -16, and -17, and RFCs 0951, 1533, 1541, 1542, 1883, 1884, 1885, and 1886.

b. IAB-STD-33 specifies the trivial file transport protocol, which is used by routers for initialization only.

c. RFC 1583 specifies the open shortest path first (OSPF) version 2 protocol for unicast interior gateway routing; RFC 1584 specifies multicast OSPF (MOSPF) for multicast interior gateway routing.

d. RFCs 1771 and 1772 specify the gateway protocol used by routers for exterior gateway routing.

e. RFC-1812, an umbrella standard, references other documents for IPv4 and corrects errors in some of the reference documents.

3.7.3.2 Local area networks. Local Area Networks (LANs) provide connectionless subnetwork service to support information exchange between end systems. The information transfer can be point-to-point, multicast, or broadcast. The link layer consists of two sublayers, logical link control (LLC) and media access control (MAC). Link-layer addresses are used to exchange information between end systems on the same LAN. IP-layer addresses are required for information to be exchanged with end systems on LANs connected to other networks.

3.7.3.2.1 Standards. Base standards for LANs are presented in table 3.7-13.

TABLE 3.7-13 LAN standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 10 Base T Medium-Access Unit (MAU)	8802-3:1993	Mandated (Approved)
IPC	IAB	An Ethernet Address Resolution Protocol	Standard 37/RFC-826	Mandated (Approved)
IPC	IAB	Standard for the Transmission of IP Datagrams Over Ethernet Networks	Standard 41/RFC-894	Mandated (Approved)
IPC	ISO	Logical Link Control	8802-2	Adopted (Approved)
IPC	IAB	A Reverse Address Resolution Protocol (RARP)	Standard 38/RFC-903	Adopted (Approved)
IPC	ISO	Fiber Distributed Data Interface (FDDI)	9314	Adopted (Approved)
NPC	ANSI	FDDI Station Management	X3.229	Adopted (Approved)
IPC	ISO	Token Bus Media Access Control	8802-4	Legacy (Approved)
IPC	ISO	Token Ring Media Access Control	8802-5	Legacy (Approved)
NPC	IEEE	Fast Ethernet	802.3u	Emerging (Approved)
NPC	IEEE	Wireless LAN	802.11	Emerging (Draft)

3.7.3.2.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.3.2.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.3.2.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.3.2.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. ISO 8473-2, Information Technology - Protocol for Providing the Connectionless-Mode Network Service - Part 2: Provision of the Underlying Service by an ISO/IEC 8802 Subnetwork, First Edition.

2. ANSI/IEEE 802.1B, Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Common Specifications - Part 2: LAN/MAN Management.

3. IEC 847, Characteristics of Local Area Networks (LAN), First Edition.

4. ISO ISP 10608-4, Information Technology - International Standardized Profile TAnnn - Connection-Mode Transport Service over Connectionless-Mode Network Service - Part 4: Definition of Profile TA53, Operation over a Token Ring LAN Subnetwork, First Edition.

5. ISO ISP 10608-6, Information Technology - International Standardized Profile TAnnn - Connection-Mode Transport Service over Connectionless-Mode Network Service - Part 4: Definition of Profile TA54, Operation over an FDDI LAN Subnetwork, First Edition.

6. ISO ISP 10609-11, Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-Mode Transport Service over Connectionless-Mode Network Service - Part 11: CSMA/CD Subnetwork - Dependent, Media-Dependent Requirements, First Edition.

7. ISO TR 10178, Information Technology - Telecommunications and Information Exchange Between Systems - the Structure and Coding of Logical Link Control Addresses in Local Area Networks, First Edition.

3.7.3.2.6 Recommendations. The following base standards should be used in support of related procurements:

a. ISO-8802-2 specifies the LLC protocols used in LANs such as ISO 8802-3 (CSMA-CD), ISO 8802-4 (token bus), and ISO 8802-5 (token ring). The link service provided over ISO-8802 LANs shall be a Type-1 connectionless network service, as defined in ISO-8802-2. The LLC generates command packets (or frames) called *protocol data units* (PDU) and interprets them.

b. The MAC sublayer handles the methods for allowing a particular node to transmit on the specific data transmission media available to it. A LAN can be configured as either a bus or a ring topology. Two primary methods are used to control access: carrier sense multiple access/collision detection (CSMA/CD) and token passing. The ISO 8802-3 standard addresses CSMA/CD, ISO 8802-4 addresses token-passing buses, and ISO 8802-5 addresses token-passing ring. ISO 9314

addresses Fiber Distributed Data Interface (FDDI) LANs. For interoperability reasons, the JTA mandates support for only one type of LAN.

c. ANSI X3.229 specifies the Station Management standards for FDDI LANs.

d. IAB-STD-37 and IAB-STD-38 specify the Address Resolution Protocol (ARP) and Reverse ARP (RARP), which are needed for resolution of IP-layer and link-layer addresses.

e. IAB-STD-41 specifies a standard method of encapsulating IP datagrams on an Ethernet.

f. For high-speed LAN requirements, 100-Mbps Ethernet technology may be implemented in accordance with IEEE 802.3u. This standard supports auto-negotiation of the media speed, making it possible for dual-speed Ethernet interfaces to run either at 10 or 100 Mbps automatically.

g. The IEEE 802.11 Committee is developing emerging standards for wireless LAN services across three transmission media: spread-spectrum radio, narrowband radio, and infrared. Wireless technology is useful in environments requiring user mobility or flexible network establishment and reconfiguration.

3.7.3.3 Packet-switch services. Packet switch services are supported by both wide area packet-switched network standards and internet standards.

3.7.3.3.1 Standards. Base standards for packet switches are presented in table 3.7-14.

TABLE 3.7-14 Packet-switch standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI	Core Aspects of Frame Protocol for Use with Frame Relay Bearer Service	T1.618	Adopted (Approved)
IPC	ITU-T	Interface Between DTE and DCE for Terminals Operating in the Packet Mode and Connected to Public Data Networks	X.25	Legacy (Approved)
IPC	ITU-T	Packet-Switched Signaling System Between Public Networks Providing Data Transmission Services	X.75	Legacy (Approved)
IPC	ITU-T	International Numbering Plan for Public Data Networks	X.121	Legacy (Approved)
CPN-C	Bellcore	Generic Switching Requirements in Support of SMDS	TR-TSV-000772	Informational (Approved)

3.7.3.3.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.3.3.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.3.3.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.3.3.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. ISO 8878, Information Technology - Telecommunications and Information Exchange Between Systems - Use of X.25 to Provide the OSI Connection-Mode Network Service, Second Edition.

2. ISO 10588, Information Technology - Use of X.25 Packet Layer Protocol in Conjunction with X.21/X.21 is to provide the OSI Connection-Mode Network Service, First Edition.

3. ISO 8881, Information Processing Systems - Data Communications - Use of the X.25 Packet Level Protocol in Local Area Networks, First Edition.

3.7.3.3.6 Recommendations. The following base standards should be used in support of related procurements:

a. ITU-T X.25 specifies the legacy packet-switch interface to DTEs for both the link and packet layers.

b. ITU-T X.75 specifies the link and packet layer interface used to interconnect legacy packet-switch networks.

c. ITU-T X.121 specifies the numbering plan format used by packet-switch networks.

d. ANSI T1.618 specifies frame relaying of packet-switch data using an ISDN packet-mode bearer service.

e. Bellcore TR-TSV-000772 specifies the interface used to transport packet-switch data using switched multi-megabit data service (SMDS).

3.7.3.4 Point-to-point service. Point-to-point protocols (PPP) support full-duplex, synchronous or asynchronous, communications between end systems. Point-to-point systems include physical-layer interfaces and a link-layer protocol.

3.7.3.4.1 Standards. Base standards for point-to-point systems are presented in table 3.7-15.

TABLE 3.7-15 Point-to-point standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	The Point-to-Point Protocol (PPP)	Standard 51/RFC 1661	Mandated (Approved)
CPC	IETF	PPP Internet Protocol Control Protocol (IPCP)	RFC 1332:1992	Mandated (Approved)
CPC	IETF	PPP Link Quality Monitoring	RFC 1333:1992	Mandated (Approved)
CPC	IETF	PPP Authentication Protocols	RFC 1334:1992	Mandated (Approved)
CPC	IETF	PPP Link Control Protocol (LCP) Extensions	RFC 1570:1994	Mandated (Approved)
NPC	EIA	Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, July 1991	232E	Mandated (Approved)
NPC	EIA	General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, February 1980	449	Mandated (Approved)
NPC	EIA	High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, June 1992, Including Alternate 26-Position Connector, 1992	530A	Mandated (Approved)
IPC	ITU-T	Data Transmission at 48 kbps Using 60-108 kHz Group Band Circuits (Section on NRZ Interface)	V.35	Adopted (Approved)

3.7.3.4.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.3.4.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.3.4.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.3.4.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

RFC 1841, PPP Network Control Protocol for LAN Extension, 9/29/95.

3.7.3.4.6 Recommendations. The following base standards should be used in support of related procurements:

a. IAB-STD-51, RFC-1332, RFC-1333, RFC-1334, and RFC-1570 specify link-layer protocols for point-to-point systems.

b. EIA-232E, EIA-449, EIA-530A, and ITU-T V.35 (section on NRZ Interface) specify physical-layer interfaces for point-to-point systems.

3.7.3.5 Combat net radio. Combat net radios (CNRs) provide voice or data communications for mobile users. These radios provide a half-duplex broadcast transmission media with potentially high BERs.

3.7.3.5.1 Standards. The base standard for CNR is presented in table 3.7-16.

TABLE 3.7-16 Combat net radio standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, July 27, 1995	MIL-STD-188-220A	Mandated (Approved)
GPC	DOD	Internet Transport Profile for DoD Communications - Transport and Internet Services	MIL-STD-2045-14502-1A	Mandated (Approved)

3.7.3.5.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.3.5.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.3.5.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.3.5.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. MIL-STD-188-114A, Electrical Characteristics of Digital Interface Circuits, 12/91.

2. MIL-STD-188-200, System Design and Engineering Standard for Tactical Communication, 6/83.

3. ISO 8802-2, Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 2: Logical Link Control, Second Edition.

4. ISO 8885, Information Technology - Telecommunications and Information Exchange Between Systems - High-Level Data Link Control (HDLC) Procedures - General purpose XID Frame Information Field Content and format, Third Edition.

5. IAB STD 3, Requirements for Internet hosts - communication layers, 10/1/89.

3.7.3.5.6 Recommendations. The following base standards should be used in support of related procurements:

a. MIL-STD-188-220A specifies the method by which IP packets are encapsulated and transmitted over CNR subnetworks.

b. MIL-STD-2045-14502-1A specifies a multiaddressed IP option field that must be used by hosts that are required to transmit or receive multiaddressed datagrams over CNR.

3.7.3.6 N-ISDN. Narrowband-ISDN (N-ISDN) is based on a 64-kbps channel structure. Channels used for user information exchange are called *B-channels*. Separate channels provided for common-channel signaling, called *D-channels*, are used to set up connections and control supplementary services (see 3.7.3.7).

3.7.3.6.1 Standards. Base standards for N-ISDN are presented in table 3.7-17.

TABLE 3.7-17 N-ISDN standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	ANSI	Telecommunications - Integrated Services Digital Network (ISDN) - Primary Rate - Customer Installation Metallic Interfaces (Layer 1 Specification), 1990	T1.408	Mandated (Approved)
NPC	ANSI	Telecommunications - Integrated Services Digital Network (ISDN) - Basic Access Interface for Use on Metallic loops for Application on the Network Side of the NT (Layer 1 Specification), 1992	T1.601	Mandated (Approved)
IPC	ITU-T	Numbering Plan for the ISDN Era, 1991	E.164	Mandated (Approved)
GPC	DOD	System Interface Criteria (section on WNDP)	DCAC 370-175-13	Mandated (Approved)
IPC	ITU-T	ISDN User-Network Interface - Data Link Layer Specification - Digital Subscriber Signaling System No. 1, 1993	Q.921	Mandated (Approved)
IPC	ITU-T	ISDN User-Network Interface Layer 3 Specification for basic Call Control - Digital Subscriber Signaling System No. 1 (DSS 1), Network Layer, User-Network Management, 1989	Q.931	Mandated (Approved)
CPC	IETF	Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode	RFC 1356:1992	Mandated (Approved)
CPC	IETF	PPP over ISDN	RFC 1618:1994	Mandated (Approved)
NPC	ANSI	Signaling System Number 7 (SS7) Message Transfer Part (MTP)	T1.111	Adopted (Approved)
NPC	ANSI	Signaling System Number 7 (SS7) Signaling Connection Control Part (SCCP)	T1.112	Adopted (Approved)
NPC	ANSI	Signaling System Number 7 (SS7) ISDN User Part (ISUP)	T1.113	Adopted (Approved)
NPC	ANSI	Signaling System Number (SS7) Transaction Capabilities Application Part (TCAP)	T1.114	Adopted (Approved)
NPC	ANSI	Basic Access Interface for S and T Reference Points (Layer 1)	T1.605	Adopted (Approved)
NPC	ANSI	Digital Subscriber Signaling System Number 1 (DSS1) Signaling Spec for X.25 Packet Switched Bearer Service	T1.608	Adopted (Approved)
NPC	ANSI	Interworking Between the ISDN User-Network Interface Protocol and SS7 ISUP	T1.609	[illegible]opted [illegible]pproved)
IPC	ITU-T	Numbering Plan for the International Telephone System	E.163	Adopted (Approved)
GPC	NIST	Integrated Services Digital Network (ISDN)	FIPS PUB 182	Informational (Approved)

3.7.3.6.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.3.6.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.3.6.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.3.6.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. ANSI T1.219, Telecommunications - Integrated Services Digital Network (ISDN) Management - Overview and Principles.

2. ANSI T1.236, Telecommunications - Signaling System Number 7 (SS7) - ISDN User Part Compatibility Testing.

3. ANSI T1.239, Telecommunications - Integrated Services Digital Network (ISDN) Management - User-Network Interface Protocol Profile.

4. ANSI T1.604, Telecommunications - Integrated Services Digital Network (ISDN) - Minimal Set of Bearer Services for the Basic Rate Interface.

5. ANSI T1.603, Telecommunications - Integrated Services Digital Network (ISDN) - Minimal Set of Bearer Services for the Primary Rate Interface.

6. ANSI T1.234, Telecommunications - Signaling System Number 7 (SS7) MTP Levels 2 and 3 Compatibility Testing.

3.7.3.6.6 Recommendations. The following base standards should be used in support of related procurements:

a. FIPS PUB 182 provides a basic overview of N-ISDN functionality and bearer services.

b. N-ISDN standards applicable to the UNI interface are given in ANSI T1.408, T1.601, and T1.605 for the physical layer; ITU-T Q.921, for the link layer; ITU-T Q.931, for the network layer when supporting circuit-switched connections; and ANSI T1.608, for the network layer when supporting packet-switched connections.

c. N-ISDN standards applicable to the node-to-network signaling interface are given in ANSI T1.111 to T1.114 and T1.609.

d. Address formats for N-ISDN use the numbering plan and format specified in ITU-T E.163 and E.164. Defense switched networks will support the worldwide numbering and dialing plan specified in DCAC 370-175-13.

e. RFCs 1356 and 1618 have been categorized as JTA mandatory standards when using ISDN packet-switched services to transmit IP packets, and when using the PPP over ISDN switched circuits configured for clear-channel services.

3.7.3.7 N-ISDN supplementary services. A network supplies supplementary services in addition to its basic services. The generic procedures applicable to the control of supplementary services at the user-to-network interface are defined in ANSI T1.610.

3.7.3.7.1 Standards. Base standards for N-ISDN Supplementary Services are presented in table 3.7-18.

TABLE 3.7-18 N-ISDN supplementary services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI	DSS1 - Generic Procedures for the Control of ISDN Supplementary Services	T1.610	Adopted (Approved)
NPC	ANSI	ISDN - Multi-level Precedence and Preemption (MLPP) Service Capability	T1.619	Adopted (Approved)
NPC	ANSI	Conferencing calling supplementary service	T1.647	Adopted (Approved)
NPC	ANSI	Call Waiting Supplementary Service	T1.613	Adopted (Approved)
NPC	ANSI	Call Holding Supplementary Service	T1.616	Adopted (Approved)
IPC	ITU-T	Call Forwarding Supplementary Services	I.252	Adopted (Approved)
NPC	ANSI	ISDN Normal Supplementary Service Call Transfer	T1.632	Adopted (Approved)
IPC	ITU-T	Multiparty Supplementary Services	I.254	Adopted (Approved)
NPC	ANSI	ISDN - User-to-User Supplementary Service	T1.621	Adopted (Approved)
NPC	ANSI	ISDN - Calling Line Identification Presentation and Restriction Supplementary Service	T1.625	Adopted (Approved)
IPC	ITU-T	Completion of call to a Busy Subscriber	I.253.3	Adopted (Approved)
NPC	ANSI	ISDN - Message Waiting Indicator Control and Notification Supplementary Service and Associated Switching and Signaling Specification	T1.622	Adopted (Approved)
NPC	ANSI	Explicit Call Transfer	T1.643	Adopted (Approved)
NPC	ANSI	Call Park	T1.653	Adopted (Approved)
NPC	ANSI	Call Deflection Supplementary Service	T1.642	Adopted (Approved)

3.7.3.7.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.3.7.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.3.7.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.3.7.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. ITU-T I.250, Definition of Supplementary Services - Integrated Services Digital Network (ISDN) - General Structure and Service Capabilities.

2. ITU-T I.251, Number Identification Supplementary Services - Integrated Services Digital Network (ISDN) - General Structure and Service Capabilities.

3. ITU-T I.253, Call Completion Supplementary Services - Integrated Services Digital Network (ISDN) - General Structure and Service Capabilities.

4. ITU-T I.255, Community of Interest Supplementary Services - Integrated Services Digital Network (ISDN) - General Structure and Service Capabilities.

5. ITU-T I.256, Charging Supplementary Services - Integrated Services Digital Network (ISDN) - General Structure and Service Capabilities.

6. ITU-T I.258.1, Terminal Portability (TP) Supplementary Service - Integrated Services Digital Network (ISDN) Service Capabilities.

3.7.3.7.6 Recommendations. In addition to basic services, users should specify the required supplementary services. These services are defined in various ANSI standards and ITU-T Recommendations referenced in Table 3.7-18. The following base standards should be used in support of related procurements:

a. *Multi-level Precedence and Preemption.* The Multi-level Precedence and Preemption (MLPP) service provides a prioritized call-handling service. This service has two parts: precedence and preemption. Precedence involves assigning a priority level to a call. Preemption involves the seizing of resources, which are in use by a call of lower precedence, by a higher-level precedence call in the absence of idle resources. The MLPP service is a network provider's option applicable to a domain of the network, that is, all subscribers, the network, and access resources that belong to the domain. Connections and resources belonging to calls from MLPP subscribers shall be marked with a precedence level and domain identifier and shall be preempted only by calls of a higher precedence from MLPP users in the same domain. Connections and resources belonging to calls from non-MLPP users and users from other MLPP domains shall not be preempted. The maximum precedence level of a subscriber will be set by the service provider, based on the subscriber's need. The subscriber may select a precedence level up to and including the maximum subscribed-to precedence level on a per-call basis. The MLPP service shall be mandatory in DoD networks (both fixed and deployed) and

shall comply with ANSI T1.619. For calls to subscribers in existing deployed (tactical) networks that comply with Tri-Service Tactical Communications (TRI-TAC) specifications, the MLPP service shall comply with MIL-STD-188-105.

b. *Conference Calling*. This service is defined in ANSI T1.647.

c. *Call Waiting*. The Call Waiting service permits a subscriber to be notified of an incoming call with an indication that no interface information channel is available. The subscriber then has the choice of accepting, rejecting, or ignoring the waiting call. This service is defined in ANSI T1.613.

d. *Call Hold*. The Call Hold service allows a user to interrupt communications on an existing call and then subsequently, if desired, reestablish communications. This service is defined in ANSI T1.616.

e. *Call Forwarding*. The Call Forwarding service allows a served user to have the network send to another number all incoming calls for the served user's number. This service is defined in ITU-T I.252.

f. *Normal Call Transfer*. The Normal Call Transfer service allows a user to transfer an established call to a third party. This service is defined in ANSI T1.632.

g. *Multiparty*. The Conference Call service allows a user to establish calls to multiple parties, one at a time, using normal call-handling procedures. The parties may also communicate among themselves. This service is defined in ITU-T I.254, the section titled I.254.1 - Conference Calling Service Description.

h. *User-to-User Signaling*. The User-to-User Signaling service allows users to send and receive limited amounts of user-generated information to and from another user-network interface. This information is passed transparently (without changing contents) through the network. Users can transfer information during the establishment and clearing phases of calls. The information is transmitted in the user-user information element. The user-user information element is an optional element of the following Digital Subscriber Signaling System Number 1 (DSS1) types of messages: Alerting, Connect, Disconnect, Progress, Release, Release Complete, and Setup. This service is defined in ANSI T1.621.

i. *Calling Line Identification Presentation*. The Calling Line Identification Presentation (CLIP) service provides the called party with the calling line identification at call setup on all incoming calls. This service applies to both basic rate and primary rate interfaces. This service is defined in ANSI T1.625.

j. *Calling Line Identification Restriction*. The Calling Line Identification Restriction (CLIR) service notifies the network that the Calling Party Number is not allowed

to be presented to the called party. This service is defined in ANSI T1.625. The service applies to both basic rate and primary rate interfaces.

k. *Call Completion to a Busy Subscriber.* The Call Completion to a Busy Subscriber service allows an authorized user, A, who encounters a busy destination, B, to be notified when B becomes idle. The network reinitiates the call to destination B if user A desires. This service is defined in ANSI Drafts T1S1.1/92-253 and T1S1.2/92-323.

l. *Message Waiting Indicator Control and Notification.* The Message Waiting Indicator (MWI) Control and Notification service is provided by the network to a Message Storage and Retrieval (MSR) system provider. The MSR system may request the network to provide an indication to one of its client users that messages are waiting at the MSR system. This service is defined in ANSI T1.622.

m. *Explicit Call Transfer.* The Explicit Call Transfer service allows a service user that has two independent calls to interconnect the distant parties of the two calls. The served user is thereby released from the call. This service, which is defined in ANSI T1.643, applies to both basic rate and primary rate interfaces.

n. *Call Park.* The Call Park service allows a service user to interrupt speech or voice band data communications on an existing call and then reestablish communications from the same or different terminal equipment within the same Call Park Subscriber Group. A Call Park Subscriber Group is designated by the service provider, who may optionally group together Call Park subscribers into a Call Park Subscriber Group to provide a measure of security. Call Park is a circuit-switched voice service with similar characteristics of Call Hold, except for the ability to reestablish communications from different terminal equipment. This service, which is defined in ANSI T1.653, applies to the basic rate interface.

o. *Call Deflection.* The Call Deflection service permits a served user to respond to an offered call with a request to deflect the call to another number. As a subscription option, the subscriber can invoke the deflection request after answering the call. In addition, the subscriber can limit the time it takes for the deflected-to user to answer the call. If the deflected-to user does not answer within a specified time interval, the network stops the deflection attempt and returns a failure indication to the deflecting user, if the deflecting user is still associated with the call. Unlike Call Forwarding, Call Deflection allows the network to redirect a call only after receipt of a specific user request to deflect that call. This service is defined in ANSI T1.642.

3.7.3.8 B-ISDN and ATM services. B-ISDN signaling standards are basically N-ISDN standards enhanced to support higher-speed networks that use ATM as the underlying switching fabric. B-ISDN standards support all of the N-ISDN 64-kbps transmission services and facilitate migration from N-ISDN to B-ISDN. ATM is a high-speed switching technology that takes advantage of low BER transmission facilities to accommodate intelligent multiplexing of voice, data, video, imagery, and composite input over high-speed trunks. Note that ATM technology is not limited to support of B-ISDN and data rates that are broadband (rates higher than the primary rate interface).

3.7.3.8.1 Standards. Base standards for B-ISDN and ATM are presented in table 3.7-19.

TABLE 3.7-19 B-ISDN and ATM standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	ATM Forum	UNI Specification V 3.1, User-Network Interface, September 1994	AF UNI v3.1	Mandated (Approved)
NPC	ANSI	ATM Adaptation Layer for Constant Bit Rate Services Functionality and Specifications, 1993	T1.630	Mandated (Approved)
NPC	ANSI	ATM Adaptation Layer Type 5 Common Part Functions and Specifications, 1994, which adopts ITU-T I.363, section 6	T1.635	Mandated (Approved)
CPC	IETF	Classical IP and Address Resolution Protocol (ARP) over ATM	RFC 1577:1994	Mandated (Approved)
NPC	ANSI	BISDN - ATM Layer Functionality and Specification	T1.627	Adopted (Approved)
NPC	ANSI	BISDN - ATM Adaptation Layer 3/4 Common Part Functions & Specification	T1.629	Adopted (Approved)
NPC	ANSI	BISDN - Service Specific Connection-Oriented Protocol (SSCOP) Specification	T1.637	Adopted (Approved)
IPC	ITU-T	B-ISDN UNI - Physical Layer Specification	I.432	Adopted (Approved)
IPC	ITU-T	Service-Specific Coordination Function (SSCF) for Signaling at the UNI	Q.2130	Adopted (Approved)
IPC	ITU-T	Service-Specific Coordination Function (SSCF) for Signaling at the NNI	Q.2140	Adopted (Approved)
IPC	ITU-T	BISDN NNI Network Signaling Requirements	Q.2761 to Q.2764	Adopted (Approved)
IPC	ITU-T	BISDN DSS2 UNI L-3 Spec for Basic Call/Connection Control	Q.2931	Adopted (Approved)
IPC	ITU-T	Point-to-Multipoint Call Connection Control	Q.2971	Adopted (Approved)
GPC	DOD	Standardized Profile for Asynchronous Transfer Mode (ATM)	MIL-STD-188-176	Adopted (Approved)
CPC	ATM Forum	Private Network-Network Interface (PNNI)	AF PNNI v1.0	Emerging (Approved)
CPC	ATM Forum	LAN Emulation	AF LANE v1.0	Emerging (Approved)

3.7.3.8.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.3.8.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.3.8.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.3.8.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. ANSI T1.636, Telecommunications - B-ISDN Signaling ATM Adaptation Layer - Overview.

2. ANSI T1.638, Telecommunications - B-ISDN Signaling ATM Adaptation Layer - Service-Specific Coordination Function for Support of Signaling at the User-to-Network Interface.

3. ANSI T1.645, Telecommunications - B-ISDN Signaling ATM Adaptation Layer - Service-Specific Coordination Function for Support of Signaling at the Network Node Interface.

4. ITU-T I.150, B-ISDN Asynchronous Transfer Mode Functional Characteristics.

5. ITU-T I.311 (REV1), B-ISDN General Network Aspects.

6. ITU-T I.361 (REV1), B-ISDN ATM Layer Specification.

7. ITU-T I.363, B-ISDN ATM Adaptation Layer (AAL) Specification - Integrated Services Digital Network (ISDN) - Overall Network Aspects and Functions.

8. ITU-T I.610 (REV1), B-ISDN Operation and Maintenance Principles and Functions.

3.7.3.8.6 Recommendations. The following base standards should be used in support of related procurements:

a. ATM standards adopted for the Department of Defense (DoD) are given in DoD's ATM Standards Profile, MIL-STD-188-176. The network access protocols to connect user equipment to ATM switches are defined in the ATM Forum's User-Network Interface (UNI) Specification v3.1.

b. ATM protocol layers consist of an ATM Adaptation Layer (AAL), the ATM layer, and a physical layer:

(1) The role of AAL is to divide the variable-length data units into 48-octet units to pass to the ATM layer. AAL1, which supports constant bit rate service, is specified in ANSI T1.630. AAL 3/4 and AAL5, which support variable bit rate service, are specified in ANSI T1.629 and T1.635, respectively.

(2) The ATM layer is specified in ANSI T1.627.

(3) Physical-layer standards for different cable interfaces and rates are specified in AF UNI v3.1. Physical media-independent functions are specified in ITU-T I.432.

c. Signaling messages to support switched connections specified in ATM FORUM (AF) UNI v3.1 are based on ITU-T Q.2931 and Q.2971, but the full functionality of these two standards is not supported. Signaling AAL services are specified in ANSI T1.635, T1.637, and ITU-T Q.2130.

d. RFC-1577 supports interworking between ATM networks and IP router networks.

e. The ATM Forum is developing Private Network-to-Network Interface (PNNI) routing and signaling standards to support large, dynamic, multivendor ATM networks. PNNI routing will automatically disseminate network topology and resource information to switches in the network, enabling quality-of-service sensitive routing. Using this information, PNNI signaling will allow calls to traverse large, dynamic networks.

f. Signaling at the NNI is specified by ITU-T Q.2761 to Q.2764. The signaling AAL services are specified in ANSI T1.635, T1.637, and ITU-T Q.2140.

g. LANs, such as Ethernet, can be emulated over ATM networks, using ATM LAN Emulation, Version 1.0.

3.7.3.9 Tactical networks. Existing tactical networks were designed to operate over noisy radio trunks having limited bandwidth. For this reason, military standards were developed for circuit-switch signaling methods, channel structure, and voice digitization. Tactical packet-switch networks, however, use commercial standards (see 3.7.3.3).

3.7.3.9.1 Standards. Base standards developed for TRI-TAC/MSE are presented in table 3.7-20.

TABLE 3.7-20 Tactical network standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Interoperability and Performance Standards for Digital Signaling and Supervision of Tactical Communications Systems	MIL-STD-188-256	Legacy (Approved)
GPC	DOD	Interoperability and Performance Standards for Tactical Digital Transmission Groups	MIL-STD-188-202	Legacy (Approved)
GPC	DOD	Analog-to-Digital Conversion Techniques (for CVSD Modulation)	MIL-STD-188-113	Legacy (Approved)

3.7.3.9.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.3.9.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.3.9.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.3.9.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. MIL-STD-188-200, System Design and Engineering Standards for Tactical Communications, 6/83.

2. FED-STD-1015, Telecommunications: Analog to Digital Conversion of Voice by 2,400 Bits/Second Linear Predictive Coding.

3. STANAG 4198, Parameters and Coding Characteristics That must be Common to Assure Interoperability of 2400 bps Linear Predictive Encoded Digital Speech.

4. STANAG 4209, The NATO Multi-Channel Tactical Digital Gateway - Standards for Analog to Digital Conversion of Speech Signals.

3.7.3.9.6 Recommendations. The following base standards should be used in support of related procurements:

a. MIL-STD-188-256 specifies the trunk and loop signaling messages employed in tactical networks.

b. MIL-STD-188-202 specifies the multiplex signal formats used by tactical circuit switches and multiplexers.

c. MIL-STD-188-113 specifies the CVSD voice-encoding method used in tactical networks.

3.7.3.10 Voice encoding for networks. Networks must be able to switch, rate adapt, and transcode different voice digitization algorithms, as necessary, to meet interoperability requirements.

3.7.3.10.1 Standards. Base standards for voice encoding are presented in table 3.7-21.

TABLE 3.7-21 Voice encoding standards for networks

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ITU-T	Pulse Code Modulation (PCM) of voice frequencies (narrowband)	G.71 :1989	Adopted (Approved)
GPC	NCS	Linear Predictive Coding (LPC)	FED-STD-1015	Adopted (Approved)
GPC	NCS	Analog-to-Digital Conversion of Radio Voice by 4800-bps Code Excited Linear Prediction (CELP)	FED-STD-1016	Adopted (Approved)
IPC	ITU-T	32 kbits/s Adaptive Differential Pulse Code Modulation (ADPCM) - General Aspects of Digital Transmission Systems	G.721:1989	Adopted (Approved)
GPC	DOD	Analog-to-Digital Conversion Techniques (for CVSD Modulation)	MIL-STD-188-113	Legacy (Approved)

3.7.3.10.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.3.10.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.3.10.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.3.10.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. ITU-T G.712, Performance Characteristics of PCM Channels Between 4-wire Interfaces at Voice Frequencies - General Aspects of Digital Transmission Systems; Terminal Equipment.

2. ITU-T G.713, Performance Characteristics of PCM Channels Between 2-wire Interfaces at Voice Frequencies - General Aspects of Digital Transmission Systems; Terminal Equipment (Replaced by Recomm. G.712).

3. STANAG 4198, Parameters and Coding Characteristics That must be Common to Assure Interoperability of 2400 bps Linear Predictive Encoded Digital Speech.

4. STANAG 4209, The NATO Multi-Channel Tactical Digital Gateway - Standards for Analog to Digital Conversion of Speech Signals.

3.7.3.10.6 Recommendations. The following base standards should be used in support of related procurements:

a. ITU-T G.711 specifies the 64-kbps voice-encoding method used in commercial and strategic networks.

b. MIL-STD-188-113 specifies the 16/32-kbps voice-encoding method used in tactical networks.

c. FED-STD-1015 specifies the 2400-bps voice-encoding method used in STU-IIIs.

d. FED-STD-1016 specifies the 4800-bps voice-encoding method used in STU-IIIs.

e. ITU-T G.721 specifies the 32-kbps voice-encoding method used to double the channel capacity of high-cost T-1 transmission facilities.

3.7.3.11 Timing and synchronization. In general, bit timing for hosts and end systems will be slaved to the local network.

3.7.3.11.1 Standards. Base standards for timing and synchronization are presented in table 3.7-22.

TABLE 3.7-22 Timing and synchronization standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI	Synchronization Interface Standards for Digital Service	T1.101	Adopted (Approved)
GPC	NCS	Time and Frequency Reference Information in Telecommunications Systems	FED-STD-1002	Adopted (Approved)
GPC	DOD	Standards for Communications Timing and Synchronization Subsystems	MIL-STD-188-115	Legacy (Approved)

3.7.3.11.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.3.11.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.3.11.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.3.11.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

ITU-T G.810, Considerations on Timing and Synchronization Issues - Digital Networks, Digital Sections and Digital Line Systems.

3.7.3.11.6 Recommendations. The following base standards should be used in support of related procurements:

a. Systems that require time and frequency reference information based on coordinated universal time (UTC) will comply with FED-STD-1002.

b. Local-network and wide-network elements provide stratum-1 clock accuracy, as defined in ANSI T1.101, and buffering sufficient to maintain bit count integrity (BCI) for a minimum of 24 hours.

c. Systems that use bit-timing slaved to the network will comply with MIL-STD-188-115.

3.7.3.12 Network management. Network management includes the capability to control the network's topology, dynamically segment the network into multiple logical domains, maintain network routing tables, monitor the network load, and make routing adjustments to optimize throughput. Network management also provides the capability to review and publish addresses of network objects; monitor the status of network objects; start, restart, reconfigure, or terminate network objects; and detect loss of network objects to support automated fault recovery.

3.7.3.12.1 Standards. Base standards for network management are presented in table 3.7-23.

TABLE 3.7-23 Network management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Adopted (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Adopted (Approved)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) - Part 1: Specification (Includes amendment 1 and 2 of ISO/IEC 9596-1:1990)	9596-1:1991	Adopted (Approved)

3.7.3.12.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.3.12.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.3.12.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.3.12.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. ISO 7498-4, Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management Framework, First Edition.

2. ISO 10165-1, Information Technology - Open Systems Interconnection - Structure of Management Information - Part 1: Management Information Model, First Edition.

3. ISO 10165-2, Information Technology - Open Systems Interconnection - Structure of Management Information - Part 2: Definition of Management Information, First Edition.

4. ISO 10165-4, Information Technology - Open Systems Interconnection - Structure of Management Information - Part 4: Guidelines for the Definition of Managed Objects, First Edition.

5. ISO DIS 10165-7, Information Technology - Open Systems Interconnection - Structure of Management Information - Part 7: General Relationship Model.

3.7.3.12.6 Recommendations. The following base standards should be used in support of related procurements:

DISN network management communications protocol and services, which provide the management information-transfer mechanism, are specified in FIPS-PUB-179, the sections titled *Common Management Information Protocol (CMIP)* and *Common Management Information Services (CMIS).* A complete coverage of CMIP and CMIS can be found in ISO 9596-1 and ISO 9595, respectively.

3.7.4 Interworking services. Interworking standards are required to ensure interoperability between differing networks. Interworking requires transformation and compatibility at the lower three layers.

3.7.4.1 Interworking services. (See the Interworking MLSA, above.)

3.7.4.1.1 Standards. Base standards for interworking are presented in table 3.7-24.

TABLE 3.7-24 Interworking standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	IETF	Classical IP and Address Resolution Protocol (ARP) over ATM	RFC 1577:1994	Mandated (Approved)
IPC	IAB	Standard for the Transmission of IP Datagrams Over Ethernet Networks	Standard 41/RFC-894	Mandated (Approved)
IPC	IAB	Transmission of IP and ARP over FDDI Networks	Standard 36/RFC-1390	Adopted (Approved)
IPC	IAB	Transmission of IP Datagrams over IEEE 802 Networks	Standard 43/RFC-1042	Adopted (Approved)
CPC	IETF	Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode	RFC 1356:1992	Adopted (Approved)
NPC	ANSI	DSS1 Signaling Specification for Frame Relay Bearer Service	T1.617	Adopted (Approved)
NPC	ANSI	Core Aspects of Frame Protocol for Use with Frame Relay Bearer Service	T1.618	Adopted (Approved)
NPC	ANSI	Frame Relaying Bearer Service Interworking	T1.633	Adopted (Approved)
NPC	ANSI	Frame Relaying Service Specific Convergence Sublayer (FR-SSCS)	T1.634	Adopted (Approved)
IPC	ITU-T	Interworking between Signaling System No. 7 Broadband ISDN User Part (BISUP) and Narrowband ISDN User Part (NISUP)	Q.2660	Adopted (Approved)
CPC	Frame Relay Forum	Frame Relay/ATM PVC Network Interworking Implementation Agreement	FRF.5	Adopted (Approved)
CPC	Frame Relay Forum	Frame Relay/ATM PVC Service Interworking Implementation Agreement	FRF.8	Adopted (Approved)
CPC	SMDS Interest Group	Protocol Interface Specification for Implementation over an ATM-based Public UNI	SIG-TWG-008	Adopted (Approved)

3.7.4.1.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.4.1.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.4.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.4.1.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. ANSI T1.609, Telecommunications - Interworking Between the ISDN User-Network Interface Protocol and the Signaling System Number 7 ISDN User Part.

2. ANSI T1.656, Telecommunications - Broadband ISDN - Interworking Between Signaling System Number 7 Broadband (B-ISUP) and ISDN User Part (ISUP).

3. ITU-T Q.608, Miscellaneous Interworking Aspects - Interworking of Signaling Systems.

3.7.4.1.6 Recommendations. The following base standards should be used in support of related procurements:

a. IP level interworking between different LANs is specified in IAB-STD-36, -41, and -43. IP interworking over ATM is specified in RFC 1577.

b. RFC 1356 specifies the method of interworking IP with X.25.

c. For frame relay interworking with N-ISDN, ANSI T1.617 specifies access connections on demand, and ANSI T1.618 specifies the method for multiplexing multiple subscriber data streams onto a single connection. Frame relay interworking with B-ISDN is specified in ANSI T1.633 and T1.634. FRF.5 specifies interworking between frame relay and ATM; FRF.8 specifies the interworking of a frame-relay-service user and an ATM service user.

d. Interworking between N-ISDN and B-ISDN is specified in ITU-T Q.2660.

e. Interworking between SMDS and ATM is specified in SIG-TWG-008.

3.7.5 Personal communications services. Personal communications services (PCS) will support both terminal mobility and personal mobility. Personal mobility allows users to gain access to telecommunication services from any convenient terminal with which they choose to associate themselves. Personal mobility may be provided by either wireline or wireless terminals. Terminal mobility is based on wireless access. Thus, wireless access standards will govern the protocols and procedures for establishing connections among mobile terminals and between them and fixed terminals of a switched network (or mobile terminals of a different cellular system).

3.7.5.1 Wireless access. Cellular mobile systems use wireless access standards to support terminal mobility. Wireless access allows subscribers to place and receive telephone calls over fixed networks wherever cellular service is provided. Two methods for digital access have emerged, time-division multiple access (TDMA) and code-division multiple access (CDMA). In North America the standards for TDMA and CDMA are based on IS-136 and IS-95-A, respectively. Both of these standards use IS-41-C as the standard signaling protocol.

3.7.5.1.1 Standards. Table 3.7-25 presents base standards used in support of cellular mobile and PCS systems.

TABLE 3.7-25 Current wireless access standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	EIA/TIA	800 MHz TDMA Cellular - Radio Interface - Mobile Station - Base Station Compatibility Standard	IS-136	Adopted (Approved)
NPC	ANSI	Personal Station-Base Station Compatibility Requirement for 1.8 to 2.0 GHz CDMA Personal Communications Systems	J-STD-008	Adopted (Approved)
NPC	ANSI	IS-136 Based Mobile Station Minimum Performance 1900 Mhz Standard	J-STD-009	Adopted (Approved)
NPC	ANSI	IS-136 Based Base Station Minimum Performance 1900 Mhz Standard	J-STD-010	Adopted (Approved)
NPC	ANSI	IS-136 Based Air Interface Compatibility 1900 Mhz Standard	J-STD-011	Adopted (Approved)
CPC	EIA/TIA	Cellular Radio Telecommunications Intersystems Operations	IS-41-C	Emerging (Approved)
CPC	EIA/TIA	Cellular System Dual-Mode Mobile Station Base Station Compatibility Standard.	IS-54-B	Emerging (Approved)
CPC	EIA/TIA	Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread-Spectrum Cellular Systems	IS-95-A	Emerging (Approved)

3.7.5.1.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.5.1.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.5.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.5.1.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. EIA TSB47 IS-54, Implementation Issues.

2. EIA TSB51, Cellular Radiotelecommunications Intersystem Operations: Authentication, Signaling Message Encryption and Voice Privacy.

3. EIA TSB56-A, Cellular Application Level Testing for IS-41 Revision B, TSB51 and IS-53.

4. EIA TSB64 IS-41-B, Support for Dual-Mode Wideband Spread Spectrum Mobile Stations.

5. EIA TIA/IS-98, Recommended Minimum Performance Standards for Dual-Mode Wideband Spread Spectrum Cellular Mobile Stations.

3.7.5.1.6 Recommendations. PCS is an emerging technology with the two predominant competing world-wide methodologies: code-division multiple access (CDMA) and time-division multiple access (TDMA). Of these, CDMA offers the best technical advantages for military applications based on its use of Direct Sequence Spread Spectrum (DSSS) techniques which provide increased channel capacity, low probability of intercept (LPI), and protection against jamming. The PCS air-interface standard for CDMA is J-STD-008 which is a frequency upshifted version of IS-95-A, the 800 MHz digital cellular standard for CDMA. The PCS air-interface standard for TDMA is IS-136 which is a frequency upshifted version of IS-54B, the 800 MHz digital cellular standard for TDMA. In North America, the standard signaling protocol for CDMA and TDMA mobile cellular is IS-41-C. It should be recognized that for Operations-Other-Than-War (OOTW), a user may have to support multiple protocols to access region-specific international digital PCS/mobile cellular infrastructures.

3.7.5.2 Future public land mobile telecommunications systems. ITU is now working on standards for future public land mobile telecommunications systems (FPLMTS) standards. The aim of this effort is to achieve better compatibility among various cellular systems so that universal global access supporting terminal mobility will become a reality.

3.7.5.2.1 Standards. The documents shown in table 3.7-26 provide guidance for future implementation of land mobile telecommunications systems.

TABLE 3.7-26 FPLMTS standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ITU-T	Coding of Speech at 16 kbits/s using Low-Delay Code Excited Linear Prediction (LD-CELP).	G.728:1992	Adopted (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
IPC	ITU-T	[illegible]	M.1073	Informational (Draft)
IPC	ITU-T	[illegible]	M.1075	Informational (Draft)
IPC	ITU-T	Security Principles for FPLMTS Speech and Voiceband Data	M.1076	Informational (Draft)
IPC	ITU-T	Performance Requirements for FPLMTS	M.1077	Informational (Draft)
IPC	ITU-T	Framework of FPLMTS Management	FPLMTS.FRAM	Informational (Draft)
IPC	ITU-T	Framework for the Satellite Component of FPLMTS	FPLMTS.SFRK	Informational (Draft)
IPC	ITU-T	Security Mechanisms and Operating Procedures for FPLMTS	FPLMTS.SECMOP	Informational (Draft)
IPC	ITU-T	Videotelephony Service for FPLMTS	F.725	Informational (Draft)
IPC	ITU-T	Reference Connections for Engineering of Land Mobile Networks	E.751	Informational (Draft)
IPC	ITU-T	Network Grade-of-Service Parameters and Target Values for Circuit-switched Public Land Mobile Services	E.771	Informational (Draft)
IPC	ITU-T	Traffic Engineering Methods for Land Mobile Systems	E.790	Informational (Draft)
IPC	ITU-T	TMN Management Service for FPLMTS	M.3321	Informational (Draft)
IPC	ITU-T	FPLMTS Information Flows	Q.FIF	Informational (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)

3.7.5.2.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.5.2.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.5.2.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.5.2.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. ITU-T E.173, Routing Plan for Interconnection Between Public Land Mobile Networks and Fixed Terminal Networks.

2. ITU-T E.201, Reference Recommendation for Mobile Services.

3. ITU-T E.202, Network Operational Principles for Future Public Mobile Systems and Services.

4. ITU-T E.212, Identification Plan for Land Mobile Stations - Telephone Network and ISDN - Operation, Numbering, Routing and Mobile Service.

5. ITU-T E.220, Interconnection of Public Land Mobile Networks.

6. ITU-T F.115, Service Objectives and Principles for Future Public Land Mobile Telecommunication Systems - Operations and Quality of Service - Mobile Service.

7. ITU-T Q.1001, General Aspects of Public Land Mobile Networks - Public Land Mobile Network Interworking with ISDN and PSTN.

3.7.5.2.6 Recommendations. Future Public Land Mobile Telecommunication Systems is an emerging technology. For additional guidance, users should review ITU-T F.115, Service Objectives and Principles for Future Public Land Mobile Telecommunication Systems - Operations and Quality of Service - Mobile Service.

3.7.5.3 Universal personal communications. Universal personal telecommunications (UPT) allows users to gain access to a variety of authorized services without limiting personal mobility, terminal mobility, or both. All authorized services will be available to the user, irrespective of location and limited only by the capabilities of the terminal and the network used.

3.7.5.3.1 Standards. ITU Recommendations (approved or in draft) are listed in table 3.7-27.

TABLE 3.7-27 Universal personal communications standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ITU-T	UPT Service Set 1	F.851	Adopted (Approved)
IPC	ITU-T	UPT Numbering	E.168	Adopted (Approved)
IPC	ITU-T	UPT Grade-of-Service Concept	E.775	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)

3.7.5.3.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.5.3.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.5.3.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.5.3.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. ITU-T E.175, Routing Principles and Guidance for Universal Personal Telecommunications (UPT) - Telephone Network and ISDN - Operation, Numbering, Routing and Mobile Service.

2. ITU-T F.850, Principles of Universal Personal Telecommunication (UPT) - Operations and Quality of Service.

3. ITU-T Q.76, Service Procedures for Universal Personal Telecommunication - Functional Modeling and Information Flows - General Recommendations on Telephone Switching and Signaling - Functions and Information Flows for Services in the ISDN.

3.7.5.3.6 Recommendations. Universal Personal Telecommunications is a new service concept and it is not totally defined. For more information users should review ITU-T F.850, Principles of Universal Personal Telecommunication (UPT) - Operations and Quality of Service.

3.7.6 Transmission media. Transmission media of interest to DoD communications systems includes satellite terrestrial radio and fiber and metallic cable. Also included in this section are standards for multiplexer formats and message formats for tactical digital information links (TADIL).

3.7.6.1 Military satellite communications. The standards for military satellite communications (MILSATCOM) can be categorized in accordance with the frequency band of operation, that is, ultra high frequency (UHF), super high frequency (SHF), and extremely high frequency (EHF).

3.7.6.1.1 Standards. Base standards for MILSATCOM are presented in table 3.7-28.

TABLE 3.7-28 Military satellite communications standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Interoperability Standard for Dedicated 5-kHz and 25-kHz UHF Satellite Communications, September 18, 1992	MIL-STD-188-181	Mandated (Approved)
GPC	DOD	Interoperability Standard for 5kHz UHF DAMA Terminal Waveform, September 18, 1992	MIL-STD-188-182	Mandated (Approved)
GPC	DOD	Interoperability Standard for 25kHz UHF/TDMA/DAMA Terminal Waveform, September 18, 1992	MIL-STD-188-183	Mandated (Approved)
GPC	DOD	Interoperability and Performance Standard for the Data Control Waveform, August 20, 1993	MIL-STD-188-184	Mandated (Approved)
GPC	DOD	Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, January 13, 1995	MIL-STD-188-164	Mandated (Approved)
GPC	DOD	SHF Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), January 13, 1995	MIL-STD-188-165	Mandated (Approved)
GPC	DOD	EHF LDR uplinks and Downlinks, December 10, 1992	MIL-STD-1582	Mandated (Approved)
GPC	DOD	EHF MDR Uplinks and Downlinks, August 26, 1995	MIL-STD-188-136	Mandated (Approved)
GPC	DOD	Interoperability of UHF MILSATCOM DAMA Control System	MIL-STD-188-185	Emerging (Approved)
GPC	DOD	Interoperability and Performance Standards for EHF SATCOM Link Control	MIL-STD-188-166	Emerging (Draft)
GPC	DOD	Interoperability and Performance Standard for SHF SATCOM Demand Assigned	MIL-STD-188-167	Emerging (Draft)
GPC	DOD	Interoperability and Performance Standards for SHF SATCOM Interfaces	MIL-STD-188-168	Emerging (Draft)

3.7.6.1.2 Alternative specification. No other consortia or *de facto* specifications are available.

3.7.6.1.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.6.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.6.1.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. Intelsat Earth Station Standard (IESS) 308, Performance Characteristics for Intermediate Data Rate (IDR) Digital Carriers (Standard A, B, C, E, and F Earth Stations).

2. IESS 309, QPSK/FDMA Performance Characteristics of INTELSAT Business Services (IBS).

3.7.6.1.6 Recommendations. The following base standards should be used in support of related procurements:

a. UHF SATCOM Standards:

(1) The parameters defined in MIL-STD-188-181 provide for the interoperability and performance of UHF SATCOM terminals that use nonprocessed 5-kHz (narrowband) and 25-kHz (wideband) channels. The dedicated/phase-shift keying (PSK) mode is used for narrowband channels. The dedicated/ frequency-shift keying (FSK) mode, or optional PSK modes, are used for wideband channels.

(2) The parameters defined in MIL-STD-188-182 provide for the dynamic sharing of one or more nonprocessed narrowband (5-kHz) UHF SATCOM channels in demand-assignment multiple access (DAMA) mode.

(3) The parameters defined in MIL-STD-188-183 provide for the dynamic sharing of a nonprocessed wideband (25-kHz) UHF SATCOM channel in the TDMA/DAMA mode.

(4) The parameters defined in MIL-STD-188-184 provide for data compression and adaptive error-correction processing of user data.

(5) The parameters defined in MIL-STD-188-185 will provide for centralized control and decentralized management of 5-kHz and 25-kHz UHF military satellite communications (MILSATCOM) resources.

b. SHF SATCOM Standards:

(1) MIL-STD-188-164 defines minimum mandatory rf and IF requirements to ensure interoperability of SATCOM earth terminals operating over C-band, X-band, and Ku-band channels.

(2) MIL-STD-188-165 defines minimum mandatory requirements to ensure interoperability of PSK modems operating in the FDMA mode with SHF SATCOM earth terminals.

(3) MIL-STD-188-166 will define the communications link characteristics required to control and manage access to SHF SATCOM transponders.

(4) MIL-STD-188-167 will define the communications protocols required for assignment of SHF satellite space resources in accordance with demand.

(5) MIL-STD-188-168 will define the formats, protocols, and other communications techniques required for transferring multiple-user information over a single SATCOM link.

c. EHF SATCOM Standards:

(1) MIL-STD-1582 defines a common waveform for low-data-rate (75 to 2400 bps) EHF satellite data links.

(2) MIL-STD-188-136 defines a common waveform for medium-data-rate (4.8 kbps to 1.544 Mbps) EHF satellite data links.

3.7.6.2 Radio communications. Radio communications standards cover the frequency range from low frequencies (LF) to ultra high frequencies (UHF). They provide service to fixed and mobile applications.

3.7.6.2.1 Standards. Base standards for radio communications are presented in table 3.7-29.

TABLE 3.7-29 Radio communications standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Medium and High Frequency Radio Equipment Standard, September 10, 1993	MIL-STD-188-141A	Mandated (Approved)
GPC	DOD	Interoperability Standard Anti-Jam Communications (2-30 Mhz)	MIL-STD-188-148A	Mandated (Approved)
GPC	DOD	Data Modems, Interoperability and Performance Standards, September 30, 1991	MIL-STD-188-110A	Mandated (Approved)
GPC	DOD	Tactical Single Channel (VHF) Radio Equipment, June 20, 1985	MIL-STD-188-242	Mandated (Approved)
GPC	DOD	Tactical Single Channel (UHF) Radio Communications, March 15, 1989	MIL-STD-188-243	Mandated (Approved)
GPC	DOD	Digital Line-of-Sight (LOS) Microwave Radio Equipment, July 28, 1992	MIL-STD-188-145	Mandated (Approved)
GPC	DOD	Equipment Technical Design Standards for Common Long Haul/Tactical Radio Communications in the LF and Lower Frequency Bands	MIL-STD-188-140A	Legacy (Approved)
GPC	NCS	Interoperability Requirements for Meteor Burst Radio Communications Between Conventional Master and Remote Stations	FED-STD-1055	Legacy (Approved)
GPC	NCS	Interoperability Requirements for Encryption of Meteor Burst Radio Communications	FED-STD-1056	Legacy (Approved)
GPC	NCS	Interoperability Requirements for Meteor Burst Radio Communications Between Networks by Master Stations	FED-STD-1057	Legacy (Approved)
GPC	DOD	Joint Technical Interface Specification for VHF SINCGARS Waveform	JIEO Spec 9001	Legacy (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)

3.7.6.2.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.6.2.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.6.2.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.6.2.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. MIL-STD-188-200, System Design and Engineering Standards Tactical Communication.

2. MIL-STD-449, Radio Frequency Spectrum Characteristics, Measurement of.

3. MIL-STD-461, Electromagnetic Interface Characteristics, Requirements for Equipment.

4. MIL-STD-462, Electromagnetic Interface Characteristics, Measurements of.

5. MIL-STD-463, Definition and System of Units, Electromagnetic Interface and Electromagnetic Compatibility Technology.

6. STANAG 4204, Technical Standards for Single Channel VHF Radio Equipment.

3.7.6.2.6 Recommendations. The following base standards should be used in support of related procurements:

a. LF radio communications standards: Parameters for radio subsystems operating in the low frequency (LF) and lower bands are defined in MIL-STD-188-140A.

b. MF and HF radio communications standards: Parameters for radio subsystems operating in the medium frequency (MF) and high frequency (HF) bands are defined in MIL-STD-188-141A. Standards for HF radio automatic link establishment (ALE) and HF automatic operation in stressed environments are provided in MIL-STD-188-141A.

c. HF radio communications standards: Parameters for HF radio anti-jam (AJ) transmission systems are defined in MIL-STD-188-148A and MIL-STD-188-110A. Emerging standards for HF store-and-forward service and for automatic HF networking to multiple transmission media will be in FED-STD-1047 and FED-STD-1048, respectively.

d. Meteor burst radio communications standards: Meteor burst radio communications relies on the billions of meteors that enter the earth's atmosphere daily, are vaporized by atmospheric friction, and produce ionized trails. A high percentage of these trails lasts less than one-half second, although some trails last up to several seconds. Trail occurrence and duration are random events. FED-STD-1055, FED-STD-1056, and FED-STD-1057 are intended for use by systems that use meteor burst communications.

e. VHF radio communications standards: Parameters for radio subsystems using frequencies between 30 and 300 MHz are defined in MIL-STD-188-242. Parameters for VHF radios requiring transmission security are defined in Joint Interoperability and Engineering Organization (JIEO) Specification 9001.

f. UHF radio communications standards: Parameters for radio subsystems using frequencies between 300 and 3000 MHz are defined in MIL-STD-188-243. Parameters for UHF radios requiring transmission security are defined in Standardization Agreement (STANAG) 4372.

g. SHF radio subsystems: Parameters for radio subsystems using frequencies between 3 and 30 GHz are defined in MIL-STD-188-145.

3.7.6.3 Cable interfaces. Cable interfaces apply to terminal access and user-to-network interfaces (UNI). They also apply within networks for trunking between switches.

3.7.6.3.1 Standards. Base standards for cable interfaces are presented in table 3.7-30.

TABLE 3.7-30 Cable interfaces standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI	Digital Hierarchy - Optical Interface Specifications (SONET) (Single Mode - Short Reach), 1991	T1.117	Mandated (Approved)
IPC	ITU-T	Physical/Electrical Characteristics of Hierarchical Digital Interfaces (For E-1)	G.703	Informational (Approved)
CPC	ATM Forum	ATM Physical Medium Dependent Interface Specification for 155 Mbps over Twisted Pair Cable	AF-PHY-0015.00	Informational (Approved)
CPC	ATM Forum	DS-1 Physical Layer Specification	AF-PHY-0016.00	Informational (Approved)
CPC	ATM Forum	Mid-range Physical Layer Specification, Category 3, Unshielded Twisted Pair	AF-PHY-0018.00	Informational (Approved)
NPC	ANSI	Digital Hierarchy - Optical Interface Specifications (Single Mode)	T1.106	Informational (Approved)
GPC	DOD	Joint Interoperability via Fiber Optic Cable	JIEO Spec 9109	Legacy (Approved)
GPC	DOD	Subsystem Design and Engineering Standards for Common Long Haul/Tactical Cable and Wireless Communications	MIL-STD-188-112	Legacy (Approved)
GPC	DOD	System Design and Engineering Standards for Tactical Communications (Conditioned Diphase)	MIL-STD-188-200	Legacy (Approved)

3.7.6.3.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.6.3.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.6.3.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.6.3.5 Related standards. No related standards have been identified.

3.7.6.3.6 Recommendations. The following base standards should be used in support of related procurements:

a. AF-PHY-0015.00, AF-PHY-0016.00, and AF-PHY-0018.00 are the ATM Forum's physical-layer base standards that apply to the UNI.

b. ANSI T1.106, ANSI T1.117, and ITU-T G.703 standards apply to optical and metallic cables used for trunking applications.

c. Joint Interoperability and Engineering Organization (JIEO) Spec 9109, MIL-STD-188-112, and MIL-STD-188-200 apply to access, to the UNI, and to trunking for tactical cable interfaces.

3.7.6.4 Multiplex format. Where necessary, support of various low transmission rates across a high-rate connection is accomplished through the employment of synchronous multiplexing.

3.7.6.4.1 Standards. Base standards for multiplex formats are presented in table 3.7-31.

TABLE 3.7-31 Multiplex format standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI	Telecommunications - Synchronous Optical Network (SONET) - Basic Description Including Multiplex Structure, Rates and Formats (ATIS) (Revision and Consolidation of ANSI T1.105-1991 and ANSI T1.105A-1991), 1995	T1.105	Mandated (Approved)
NPC	ANSI	Digital Hierarchy - Formats Specifications, 1995	T1.107	Mandated (Approved)
IPC	ITU-T	Synchronous Frame Structures Used at Primary and Secondary Hierarchical Levels (for E-1)	G.704	Informational (Approved)

3.7.6.4.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.6.4.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.6.4.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.6.4.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. ANSI T1.119, Telecommunications - Synchronous Optical Network (SONET) - Operations, Administration, Maintenance, and provisioning (OAM&P) Communications.

2. ITU-T G.782, Types and General Characteristics of Synchronous Digital Hierarchy (SDH) Multiplexing Equipment.

3.7.6.4.6 Recommendations. The following base standards should be used in support of related procurements:

a. ANSI T1.105 specifies the multiplexing format supported by SONET systems. SONET multiplexing results in a family of standard rates and formats, which are multiples of the basic 51.84-Mbps Synchronous Transport Signal Level-1 (STS-1) rate. SONET systems support sub-STS-1 rate signals by multiplexing lower-rate signals onto a SONET format.

b. The multiplex formats applicable to DS1 and DS3 interfaces are defined in ANSI T1.107.

c. The E1 interface uses the basic frame structure defined in ITU-T G.704.

3.7.6.5 Tactical digital information links. Standard message formats and related information for tactical digital information links (TADIL) are published in documents called TADILs. A TADIL consists of a combined information medium and hardware protocol, and a message format standard. The waveform standard is identified in 3.7.6.5.1. Information exchange standards are addressed in ITSG Part 5. TADILs are migrating away from unique data links to achieve seamless information exchange. TADILs will conform to a standardized TADIL family. All TADILs will migrate to this standard unless granted a migration exemption. The J-Series Family of TADILs, described fully in the Joint Tactical Data Link Management Plan (JTDLMP), dated April 1996, enables this migration while accommodating differences in information exchange requirements.

3.7.6.5.1 Standards. Base standards for TADILs are presented in table 3.7-32. (Note: STANAGs for TADILs are presented in 3.7.8.7.)

TABLE 3.7-32 TADIL standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	JTIDS System Segment Specification (Class 2 Terminal)	JTIDS Spec	Mandated (Approved)
GPC	DOD	Interoperability and Performance Standard for TADIL A	MIL-STD-188-203-1	Legacy (Approved)
GPC	DOD	Interoperability and Performance Standards for Tactical Digital Information Link (TADIL) B (NOTE 4)	MIL-STD-188-212 of 10/17/1992	Legacy (Approved)
GPC	DOD	Interoperability and Performance Standards for Tactical Digital Information Link (TADIL) C (NOTE 5)	MIL-STD-188-203-3 of 10/5/88	Legacy (Approved)
GPC	DOD	Manual for Employing Joint Tactical Communications (for ATDL-1)	CJCSM 6231	Legacy (Approved)
GPC	DOD	Waveform for Maritime Operational Data Link (for USN and [illegible])	Link 22	Emerging (Draft)

3.7.6.5.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.6.5.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.6.5.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.6.5.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. STANAG 4175, Technical Characteristics of the Multi-functional Information Distribution System (for TADIL J).

2. STANAG 5516, Tactical Data Exchange Link-16 (for TADIL J).

3.7.6.5.6 Recommendations. The following base standards should be used in support of related procurements:

a. Technical characteristics of TADIL A subsystems are specified in MIL-STD-188-203-1.

b. Technical characteristics of TADIL B subsystems are specified in MIL-STD-188-212.

c. Technical characteristics of TADIL C subsystems are specified in MIL-STD-188-203-3.

d. Technical characteristics of Army Tactical Data Link-1 (ATDL-1) are specified in CJCSM 6231.

e. Link 22 messages will be used for the exchange of maritime operational data between tactical data systems using line-of-sight (LOS) UHF radio and HF radio for beyond LOS. The Link 22 standard is under development.

3.7.7 Strategic/tactical interoperability. Legacy tactical networks are based on Tri-Service Tactical Communications (TRI-TAC) specifications. Future tactical and strategic networks will be based on the same set of commercial standards, eliminating current interoperability problems that result from using military-unique standards in tactical systems. In the meantime, strategic/tactical gateway facilities will be needed to achieve interoperability. Gateways will support five capabilities:

- Five levels of precedence and preemption
- Common-channel-signaling message conversion
- Choice of rate adaptation or transcoding for voice algorithm conversion
- Direct digital interfacing that preserves bit-count integrity (BCI)
- Support of end-to-end transmission and reception of secure voice and secure data.

3.7.7.1 Transcoding. A transcoder performs direct digital-to-digital conversion between two different voice-encoding schemes without returning the signals to analog form. For nonsecure voice, strategic/tactical gateway facilities will transcode PCM-encoded voice to and from CVSD-encoded voice. The method of transcoding does not need to be standardized. It is necessary only to meet the PCM interface standard on one side and the CVSD interface standard on the other side of the transcoder.

3.7.7.1.1 Standards. Base standards for transcoding are presented in table 3.7-33.

TABLE 3.7-33 Transcoding standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ITU-T	Pulse Code Modulation (PCM) of voice frequencies (narrowband)	G.711:1989	Adopted (Approved)
GPC	DOD	Analog-to-Digital Conversion Techniques (for CVSD Modulation)	MIL-STD-188-113	Legacy (Approved)

3.7.7.1.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.7.1.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.7.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.7.1.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

STANAG 4209, The NATO Multi-Channel Tactical Digital Gateway - Standards for Analogue to Digital Conversion of Speech Signals.

3.7.7.1.6 Recommendations. The following base standards should be used in support of related procurements:

The standards for PCM and CVSD are ITU-T G.711 and MIL-STD-188-113, respectively.

3.7.7.2 Rate adaptation. Information sources that operate at rates of 600, 1200, 2400, 4800, 9600, 16000, 19200, or 32000 bps may be rate-adapted to a 64-kbps channel.

3.7.7.2.1 Standards. Base standards for rate adaptation are presented in table 3.7-34.

TABLE 3.7-34 Rate adaptation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
TPC	ITU-T	Support of Data Terminal Equipments (DTEs) with V-series interfaces by ISDN	V.110	Legacy (Approved)
IPC	ITU-T	Multiplexing, Rate Adaptation and Support of Existing Interfaces	I.460	Legacy (Approved)
GPC	DOD	Interoperability Standards for Data Adapter Control Mode (for multisampling)	MIL-STD-188-216	Legacy (Approved)

3.7.7.2.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.7.2.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.7.2.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.7.2.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

> ITU-T I.464 Multiplexing, Rate Adaptation and Support of Existing Interfaces for Restricted 64 kbits/s Transfer Capability - Integrated Services Digital Network (ISDN) - Overall Network Aspects and Functions, ISDN User-Network Interfaces.

3.7.7.2.6 Recommendations. The following base standards should be used in support of related procurements:

The rate adaptation of bit rates up to 32 kbps uses the multi-stage approach defined in ITU-T V.110, the section titled *Adaptation of V-series data signaling rates to the intermediate rates.* Rate adaptation of 8-, 16-, and 32-kbps signals is accomplished in accordance with ITU-T I.460, the section titled *Rate adaptation of 8-, 16-, and 32-kbps streams.* Information sources, linked to a tactical network, that operate at rates of 75, 600, 1200, 2400, 4800, or 9600 bps, may be rate-adapted to a 16-kbps channel, as described in MIL-STD-188-216, the section titled *Multisampling*.

3.7.7.3 Signaling message conversion. Interoperability between tactical circuit switches and ISDN circuit switches will occur through appropriate transformation of signaling messages at the gateway function. The gateway function translates out-of-band signaling messages between the tactical circuit-switched network and ISDN switched networks for calls initiated in either direction.

3.7.7.3.1 Standards. The base standard for signaling message conversion is presented in table 3.7-35.

TABLE 3.7-35 Signaling message conversion standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	All-Digital Tactical-to-Strategic Gateway	MIL-STD-188-105	Legacy (Approved)

3.7.7.3.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.7.3.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.7.3.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.7.3.5 Related standards. No related standards have been identified.

3.7.7.3.6 Recommendations. The following base standards should be used in support of related procurements:

Signaling message conversion for the tactical-to-strategic gateway is defined in MIL-STD-188-105.

3.7.8 NATO interoperability. NATO standardization agreements (STANAGs) identified in this section are agreements between NATO nations for the interoperability of their communications networks and end systems.

3.7.8.1 NATO tactical digital gateway. The interface between U.S.-tactical and NATO-tactical switched networks will comply with the series of STANAGs developed for the NATO Digital Gateway. This series of STANAGs, is based to a large degree on U.S. legacy tactical circuit-switch specifications.

3.7.8.1.1 Standards. Base standards for the NATO Tactical Digital Gateway are presented in table 3.7-36.

TABLE 3.7-36 NATO tactical digital gateway standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	NATO	The NATO Multi-Channel Tactical Digital Gateway System Standards	STANAG 4206	Legacy (Approved)
IPC	NATO	The NATO Multi-Channel Tactical Digital Gateway Mux Group Framing	STANAG 4207	Legacy (Approved)
IPC	NATO	The NATO Multi-Channel Tactical Digital Gateway Signaling Messages and Protocols	STANAG 4208	Legacy (Approved)
IPC	NATO	The NATO Multi-Channel Tactical Digital Gateway A/D Conversion of Speech	STANAG 4209	Legacy (Approved)
IPC	NATO	The NATO Multi-Channel Tactical Digital Gateway Metallic Cable	STANAG 4210	Legacy (Approved)
IPC	NATO	The NATO Multi-Channel Tactical Digital Gateway System Control	STANAG 4211	Legacy (Approved)
IPC	NATO	The NATO Multi-Channel Tactical Digital Gateway Radio Relay	STANAG 4212	Legacy (Approved)
IPC	NATO	The NATO Multi-Channel Tactical Digital Gateway Routing	STANAG 4214	Legacy (Approved)
IPC	NATO	The NATO Multi-Channel Tactical Digital Gateway Fiber Optic cables	STANAG 4290	Legacy (Approved)

3.7.8.1.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.8.1.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.8.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.8.1.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

1. STANAG 4213, The NATO Multi-Channel Tactical Digital Gateway - Data Transmission standards.

2. STANAG 4249, The NATO Multi-Channel Tactical Digital Gateway - Data Transmission standards (Packet Switching Service).

3.7.8.1.6 Recommendations. The following base standards should be used in support of related procurements:

The interface between U.S. tactical circuit-switch networks and NATO tactical circuit-switch networks will be based on STANAGs 4206 to 4212, 4214, and 4290.

3.7.8.2 Packet-switch networks. The network-to-network interface between U.S.-tactical and NATO-tactical packet-switched networks will comply with STANAG 4249. STANAG 4249 specifies the network-to-network international interface for tactical packet-switch networks. To achieve DTE-to-DTE interoperability across NATO gateway links requires additional agreements. This is being worked in several NATO technical working groups. The agreement expected will use TCP/IP, which is independent of the underlying subnetworks, including LANs, that may exist in national networks.

3.7.8.2.1 Standards. The base standards for interfacing packet-switch networks across a NATO Tactical Digital Gateway are presented in table 3.7-37.

TABLE 3.7-37 Packet-switch network standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	NATO	NATO Standardized Profile - Connection-oriented Mode Gateway Between Tactical Packet-Switched Data Networks Using Digital Data Circuits	STANAG 4249	Legacy (Approved)
IPC	NATO	The NATO Multi-Channel Tactical Digital Gateway	STANAG 4213	Legacy (Approved)

3.7.8.2.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.8.2.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.8.2.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.8.2.5 Related standards. Related standards are informative documents related to the base standards. Normative references are include' in the base standards.

1. IAB STD-35, ISO Transport Service on Top of the TCP.

2. RFC 1356, Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode.

3.7.8.2.6 Recommendations. The following base standards should be used in support of related procurements:

a. STANAG 4249 supports both switched virtual circuits (SVC) and permanent virtual circuits (PVC) across NATO gateway links. SVCs and PVCs will support connectionless IP traffic between terminals on different national subnetworks.

b. STANAG 4213 specifies the forward error correction code applicable to the layer 1 interface between tactical packet-switch networks.

3.7.8.3 NATO data network. Current NATO standards for data networks are aligned with the OSI reference model. It is expected that NATO standards will be expanded to support IP router networks.

3.7.8.3.1 Standards. Base standards for NATO data networks are presented in table 3.7-38.

TABLE 3.7-38 NATO data network standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	NATO	NATO Reference Model for OSI Layer 1 (Physical Layer) Service Definition	STANAG 4251	Legacy (Approved)
IPC	NATO	NATO Reference Model for OSI Layer 2 (Data Link Layer) Service Definition	STANAG 4252	Legacy (Approved)
IPC	NATO	NATO Reference Model for OSI Layer 3 (Network Layer) Service Definition	STANAG 4253	Legacy (Approved)
IPC	NATO	NATO Reference Model for OSI Layer 5 (Session Layer) Service Definition	STANAG 4255	Legacy (Approved)
IPC	NATO	NATO Reference Model for OSI Layer 6 (Presentation Layer) Service Definition	STANAG 4256	Legacy (Approved)
IPC	NATO	NATO Reference Model for OSI Layer 1 (Physical Layer) Protocol Specification	STANAG 4261	Legacy (Approved)
IPC	NATO	NATO Reference Model for OSI Layer 2 (Data Link Layer) Protocol Specification	STANAG 4262	Legacy (Approved)
IPC	NATO	NATO Reference Model for OSI Layer 3 (Network Layer) Protocol Specification	STANAG 4263	Legacy (Approved)
IPC	NATO	NATO Reference Model for OSI Layer 5 (Session Layer) Protocol Specification	STANAG 4265	Legacy (Approved)
IPC	NATO	NATO Reference Model for OSI Layer 6 (Presentation Layer) Protocol Specification	STANAG 4266	Legacy (Approved)

3.7.8.3.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.8.3.3 Standards deficiencies. No deficiencies have been identified in the existing standards. However, there are some NATO efforts to enhance the capability of NATO data network standards.

3.7.8.3.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.8.3.5 Related standards. No related standards have been identified.

3.7.8.3.6 Recommendations. The following base standards should be used in support of related procurements:

The STANAG 4250 series defines the services that a layer provides to the layer above. The STANAG 4260 series defines the protocols for operation between layer peers.

3.7.8.4 Digital facsimile. Facsimile transmissions requiring interoperability with NATO countries will use digital facsimile.

3.7.8.4.1 Standards. The base standard for facsimile interoperability with NATO allies is given in table 3.7-39.

TABLE 3.7-39 Facsimile standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	NATO	Interoperability for Tactical Digital Facsimile	STANAG 5000	Legacy (Approved)

3.7.8.4.2 Alternative specifications. No other consortia or *de facto* specifications are available.

3.7.8.4.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.8.4.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.8.4.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

EIA/TIA-466-A, Procedures for Document Facsimile Transmission.

3.7.8.4.6 Recommendations. The following base standards should be used in support of related procurements:

Facsimile transmissions requiring encryption or interoperability with NATO countries will use digital facsimile, as defined in STANAG 5000.

3.7.8.5 Single channel radios. Voice and data may be exchanged between different national forces using single channel radios.

3.7.8.5.1 Standard. Base standards for single channel radios for NATO are presented in Table 3.7-40.

TABLE 3.7-40 Single channel radio standards for NATO

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	NATO	Transmission Characteristics for Data Exchange between Land Tactical Data Processing Equipment over Single Channel Radio Links	STANAG 4202	Legacy (Approved)
IPC	NATO	Technical Standard for Single Channel HF Radio Equipment	STANAG 4203	Legacy (Approved)
IPC	NATO	Technical Standard for Single Channel VHF Radio Equipment	STANAG 4204	Legacy (Approved)
IPC	NATO	Technical Standard for Single Channel UHF Radio Equipment	STANAG 4205	Legacy (Approved)
IPC	NATO	Secure and Jam-resistant HF Low Speed Data Communications System	STANAG 4245	Legacy (Approved)
IPC	NATO	HAVE QUICK: UHF Secure and Jam-resistant Low Speed Data Communications Equipment	STANAG 4246	Legacy (Approved)
IPC	NATO	1200/2400/3600 MODEM for HF Radio Links	STANAG 4285	Legacy (Approved)
IPC	NATO	Standards to Achieve Communication between Single Channel Tactical Combat Net Radio Equipment and Frequency Hopping Radios Operating in the VHF Band (30 - 88 MHZ)	STANAG 4292	Legacy (Approved)
IPC	NATO	SATURN, a Fast Frequency Hopping ECCM mode for UHF Radio	STANAG 4372	Legacy (Approved)

3.7.8.5.2 Alternative specification. No other consortia or *de facto* specifications are available.

3.7.8.5.3 Standard deficiencies. No deficiencies have been identified in the existing standards.

3.7.8.5.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.8.5.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

STANAG 4291, 2400 wireless modem.

3.7.8.5.6 Recommendations. The following base standards should be used in support of related procurements:

a. STANAG 4202 defines the error detection and correction techniques for DTEs to exchange information over HF, VHF, and UHF single channel radios.

b. STANAG 4203 defines the technical characteristics for single channel HF radio equipment.

c. STANAG 4204 defines the technical characteristics for single channel VHF radio equipment.

d. STANAG 4205 defines the technical characteristics for transmission of voice/data/teletype over single channel UHF radio equipment.

e. STANAG 4246 defines the technical characteristics for airborne radios operating at UHF.

f. STANAG 4285 defines the call establishment procedures and modem characteristics for low speed data transmission over HF radio links.

3.7.8.6 Satellites. UHF satellites may be used to support exchange of voice and data between different national forces.

3.7.8.6.1 Standard. Base standards for Satellites for NATO are presented in Table 3.7-41.

TABLE 3.7-41 Satellite standards for NATO

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	NATO	Digital Interoperability between UHF Satellite Communications Terminals	STANAG 4231	Legacy (Approved)

3.7.8.6.2 Alternative specification. No other consortia or *de facto* specifications are available.

3.7.8.6.3 Standard deficiencies. No deficiencies have been identified in the existing standards.

3.7.8.6.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.8.6.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

MIL-STD-188-181, Interoperability Standard for Dedicated 5-kHz and 25-kHz UHF Satellite Communications Channels.

3.7.8.6.6 Recommendations. The following base standards should be used in support of related procurements:

STANAG 4231 specifies the minimum necessary parameters to achieve interoperability of UHF SATCOM terminals for teletype, low speed data, or voice.

3.7.8.7 TADILs. Standard message formats and related information for tactical digital information links (TADIL) are published in documents called TADILs. TADIL J has been standardized for use in NATO.

3.7.8.7.1 Standard. Base standards for TADILs are presented in Table 3.7-42.

TABLE 3.7-42 NATO TADILs standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	NATO	Technical Characteristics of the Multifunctional Information Distribution System (MIDS)	STANAG 4175, Edition 1, August 29, 1991	Mandated (Approved)

3.7.8.7.2 Alternative specification. No other consortia or de facto specifications are available.

3.7.8.7.3 Standard deficiencies. No deficiencies have been identified in the existing standards.

3.7.8.7.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.8.7.5 Related standards. Related standards are informative documents related to the base standards. Normative references are included in the base standards.

STANAG 5516, Tactical Data Exchange Link-16 (for TADIL J)

3.7.8.7.6 Recommendations. The following base standards should be used in support of related procurements:

Technical characteristics and waveform parameters of TADIL J subsystems are specified in STANAG 4175.

3.7.9 Communications and network services security. Communications and network services security protects the information, components, and mechanisms of the communications and network system. Use of, and compliance with, the security standards identified in this document does not constitute authorization to process classified data. DOD policy covering the security accreditation process must still be followed to obtain approval for processing classified data.

3.7.9.1 Network security architecture. (This BSA appears in both part 7 and part 10.) OSI security architecture defines the general security-related architectural elements, provides a general description of security services and related mechanisms, and defines the positions within the OSI Reference Model at which the services and mechanisms may be provided. Open systems security frameworks address data elements and sequences of operations that are used to obtain security services.

Note: The security architecture and framework standards are intended to provide guidance and background information to developers. In general, these standards do not provide implementable specifications against which conformance can be claimed.

3.7.9.1.1 Standards. Table 3.7-43 presents standards for network security architecture.

TABLE 3.7-43 Network security architecture standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Network Interpretation	NCSC-TG-005, Version 1: 1987	Mandated (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems - Part 2: Authentication Framework	10181-2:1996	Informational (Approved)
IPC	ISO	OSI Upper Layer Security Model	10745:1993	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO/IEC	Lower Layer Security Model	TR 13594:1995	Informational (Approved)
GPC	IETF	Security Architecture for the Internet Protocol	RFC 1825: 1995	Emerging (Draft)
GPC	IETF	Security Architecture for the Internet Protocol	draft-ietf-ipsec-arch-sec-04.txt, 10 November 1995	Informational (Draft)
IPC	IEEE	Standard for Interoperable LAN Security - Part A: The Model	IEEE 802.10G: 1989	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems, Part 1: Overview	10181-1	Informational (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 3: Access Control	10181-3	Informational (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)

3.7.9.1.2 Alternative specifications. There are no alternative specifications.

3.7.9.1.3 Standards deficiencies. The Upper Layer Security Model (ISO 10745) primarily addresses FTAM requirements and does not deal with Directory, Transaction Processing, and X.400.

3.7.9.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.9.1.5 Related standards. NCSC-TG-011, Version 1, 1 August 1990, Trusted Network Interpretation Environments Guideline - Guidance for Applying the Trusted Network Interpretation is a guideline supporting the TCSEC.

3.7.9.1.6 Recommendations. The standards listed as mandated are recommended. Implementations involving security services should require conformance to the security principles and concepts of the DGSA (TAFIM, Volume 6) and supporting standards. RFC 1825 is an emerging standard that provides the current view of how to implement security functions within an Internet Protocol (IP) suite network. The Internet Draft document draft-ietf-ipsec-arch-sec-01.txt is a "work-in-progress" revision of RFC 1825.

3.7.9.2 Security risk management. (This BSA appears in part 2, part 7, part 9, and part 10.) Security risk management supports accreditation through a risk analysis of an information system and its operational environment, and the steps taken to manage the risk requirements.

3.7.9.2.1 Standards. Table 3.7-44 presents standards for security risk management.

TABLE 3.7-44 Security risk management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	NIST	Guideline for the Analysis of Local Area Network Security	FIPS PUB 191:1994	Informational (Approved)
GPC	NIST	Guideline for Automated Data Processing Risk Analysis	FIPS PUB 65:1979	Informational (Approved)
GPC	NIST	Guidelines for Automatic Data Processing Physical Security and Risk Management	FIPS PUB 31:1974	Informational (Approved)

3.7.9.2.2 Alternative specifications. There are no alternative specifications.

3.7.9.2.3 Standards deficiencies. Because of its age, FIPS PUB 31 does not include information about modern security concepts.

3.7.9.2.4 Portability caveats. Portability problems with the existing standards are unknown.

3.7.9.2.5 Related standards. The following standards are related to the TCSEC standard:

a. CSC-STD-003-85 25 June 1985, Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer Security Evaluation Criteria in Specific Environments

b. CSC-STD-004-85, 25 June 1985, Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer Security Evaluation Criteria in Specific Environments

3.7.9.2.6 Recommendations. The mandated standard is recommended. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," provides guidance on effective security risk management of federal information systems. NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook" provides additional guidance on risk management. DOD Directive 5200.28 requires a risk analysis of an information system be conducted in its operational environment to support accreditation of the information system. System implementors should perform the risk analysis in accordance with CSC-STD-003-85 and CSC-STD-004-85 to determine the appropriate DOD-5200.28-STD class.

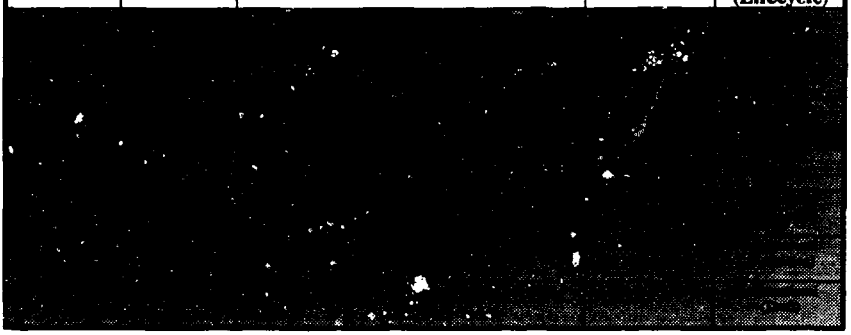
3.7.9.3 Security management. (This BSA appears in part 7, part 8, part 9, and part 10.) Security management is a particular instance of information system management. Security management provides supporting services that contribute to the protection of information and resources in open systems in accordance with information domain and information security policies. The basic elements that must be managed are users, security policies, information, information processing systems that support one or more security policies, and the security functions that support the security mechanisms (automated, physical, personnel, or procedural) used to implement security services. For each of these elements, the managed objects that constitute them must be identified and maintained. For example, users must be known and registered, security policies must be represented and maintained and information objects must be identified and maintained. Security policies, security services and security mechanisms are the first classes of managed objects.

3.7.9.3.1 Standards. Table 3 7-45 presents standards for security management.

TABLE 3.7-45 Security management standards

Standard Type	Sponsor	Standard	Standard Referenc	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Network Interpretation	NCSC-TG-005, Version 1: 1987	Mandated (Approved)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
IPC	ITU-T	The Directory: Procedures for Distributed Operation (X-ref: ISO 9594-4)	X.518: 1993	Informational (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) - Part 1: Specification (Includes amendment 1 and 2 of ISO/IEC 9596-1:1990)	9596-1:1991	Informational (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 7: Security Alarm Reporting Function (same as ITU-T X.736)	10164-7:1992	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 8: Security Audit Trail Function (same as ITU-T X.740)	10164-8:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 9: Objects and Attributes for Access Control	10164-9:1995	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)



3.7.9.3.2 Alternative specifications. There are no alternative specifications.

3.7.9.3.3 Standards deficiencies. Deficiencies exist in standardization of security policy rule representation; key management, including generation, distribution, and accounting; audit information formats; exchange of security management information; and remote security management.

The DGSA principle of decision and enforcement separation requires that the functions determining how to enforce a security policy and the actual enforcement of the policy be implemented independently. That is, the enforcement mechanisms do not need any knowledge of security policy. Standards are needed for object class definitions for classes of managed objects and for methods of representing security policy.

The DGSA calls for a separation mechanism, such as separation kernel, to mediate all calls to security critical functions to ensure that strict isolation is maintained. Standardization of object class definitions for management of critical functions used within the separation kernel is needed.

The present ISO/IEC 10164-7 "Security Alarm Reporting Function," and 10164-8, "Security Audit Trail Function," standards were designed with network security in mind. Little work has been done, either in standards groups or in products, on how to use these standards for general system management (e.g., computer systems and software).

FIPS PUB 179-1 supersedes FIPS PUB 179. The present GNMP specifications require ISO Common Management Information Service/Protocol (CMIS/CMIP) to communicate management information and ISO OSI networking protocols. Plans are for the GNMP eventually to provide a capability to integrate the present GNMP with Simple Network Management Protocol (SNMP). One reason for this goal is the widespread use of SNMP.

No Ada bindings exist for any of the ISO or consortia system management specifications.

The Institute of Electrical and Electronic Engineering (IEEE) POSIX Security Working Group (formerly P1003.6) is defining security extensions to the base POSIX interface standard (ISO 9945-1), to include support for audit, privilege, discretionary and mandatory access control, and information labels. These have been redesignated IEEE P1003.1c and IEEE P1003.2c. The draft standards are still incomplete, and the specifications may change.

The POSIX/UNIX permission bits are inadequate for fine-grained control over exactly which users can perform specified actions to particular files.

In the IETF, efforts to develop an acceptable security standard for SNMPv2 have been on hold since September 1995 when the IETF SNMP Working Group failed to agree on the proposals submitted. Since then, two sets of proposals for providing SNMPv2 security have emerged. The first set of proposed specifications, the User-based Security Model (USEC), also referred to as SNMPv2u, consists of two documents: RFC 1909, "An Administrative Infrastructure for SNMPv2" and RFC 1910, "The User-based Security Model for SNMPv2." Both RFCs were issued 28 February 1996 and are classified by the IETF as experimental RFCs. The other proposal is known as SNMPv2*, which its proponents claim is heavily based on USEC. Neither USEC nor SNMPv2* has been approved for a standards track by IETF.

3.7.9.3.4 Portability caveats. The structure of certain traditional UNIX directories, such as the familiar "/tmp," "/usr/spool," and "/usr/spool/mail" directories must be expressly managed to accommodate the P1003.1e and P1003.2c security standards. This is because these are directories to which all users have access and to which many programs write. A change in the way programs write to directories has the potential for causing software portability and systems administrator portability problems.

The traditional UNIX permission bits that have been carried into POSIX are inadequate for defining exactly which user can perform specific actions on specific files. Eliminating the permission bits in favor of Access Control Lists could make the secure POSIX systems incompatible with non-POSIX compliant systems and many applications.

OSF DCE Version 1.1's authentication services are based on Kerberos Version 5 (RFC 1510), but is not totally compatible with RFC 1510. DCE 1.2.2 adds testing and official support for Kerberos Version 5.

3.7.9.3.5 Related standards. ISO/IEC 9945-1 as profiled by FIPS PUB 151-2 is related to IEEE P1003.1e and IEEE P1003.2c.

3.7.9.3.6 Recommendations. The mandated standards are recommended.

All IEEE P1003.1e and IEEE P1003.2c security systems should incorporate Access Control Lists as an optional feature in addition to permission bits (not "in place of" permission bits). The incompatibilities between the two access control methods (permission bits and access control

lists) are not resolvable. The best method for resolving the overall problems seem to be incorporation Access Control Lists as an optional feature on top of permission bits. The permission bits would represent the lowest common denominator of security, showing the maximum amount of openness possible in a system. Organizations needing only the lowest level of security could continue to use the familiar permission bits and associated "chmod" command. Use of access control lists will require a change in security policy such that access is granted if and only if permission is granted and access control permits it.

3.7.9.4 Security association and key management. (This BSA appears in part 7, part 9, and part 10.) A security association is the totality of communication and security mechanisms and functions (e.g., communications protocols, security protocols, doctrinal mechanisms, security-critical mechanisms and functions) that securely binds together two security contexts in different end systems or relay systems supporting the same information domain. A security association is an application association that includes additional support from security functions and mechanisms. Key management provides procedures for handling cryptographic keying material to be used in symmetric or asymmetric cryptographic mechanisms. It includes key generation, key distribution, key storage, key archiving, and key deletion.

3.7.9.4.1 Standards. Table 3.7-46 presents standards for security association and key management.

TABLE 3.7-46 Security association and key management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NSA	Key Exchange Algorithm	R21-TECH-23-94: 1994	Mandated (Approved)
GPC	NSA	Secure Data Network System (SDNS) Key Management Protocol (KMP)	SDN.903, Version 3.2: 1989	Mandated (Approved)
GPC	NIST	Key Management Using ANSI X9.17	FIPS PUB 171:1992	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 2:Security Exchange Service Element Definition	11586-2:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 3: Security Exchange Service Element Protocol Specification	11586-3:1994	Informational (Approved)
IPC	ISO	Banking Key Management (wholesale)	8732:1988	Informational (Approved)
NPC	ANSI	Financial Institution Key Management (wholesale)	X9.17-1991	Informational (Approved)
NPC	IEEE	Standard for Interoperable LAN Security - Part C: Key Management Protocol (SKMP)	802.10c	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems: Part 6: Key Management	10181-6	Informational (Draft)
GPC	IETF	Internet Security Association and Key Management Protocol (ISAKMP)	draft-ietf-ipsec-isakmp-07.txt, 24 February 1997	Informational (Draft)
GPC	IETF	The Photuris Session Key Management Protocol	draft-simpson-photuris-11.txt, 13 June 1996	Informational (Draft)
GPC	IETF	Simple Key Management for Internet Protocols (SKIP)	draft-ietf-ipsec-skip-07.txt, August 1996	Informational (Draft)
GPC	IETF	The Oakley Key Determination Protocol	draft-ietf-ipsec-oakley-01.txt, 5/1996	Informational (Draft)
NPC	IEEE	Standard for Public-Key Cryptography	P1363	Informational (Formative)

3.7.9.4.2 Alternative specifications. There are no alternative specifications.

3.7.9.4.3 Standards deficiencies There is a lack of guidance for establishing a Public Key Infrastructure (PKI) to automatically manage public keys through the use of public key certificates. In April 1994, National Institute of Standards and Technology (NIST), in conjunction with seven other federal agencies, completed a study on automated management of public keys and associated public key certificates on a nationwide basis. Based on the recommendations of the study, GSA is establishing a PKI pilot project to provide public key certificate services for participating government agencies.

3.7.9.4.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.9.4.5 Related standards. There are no related standards.

3.7.9.4.6 Recommendations. The mandated standards are recommended. In FORTEZZA applications, the NSA-developed Key Exchange Algorithm, R21-TECH-23-94, must be used.

IEEE P1363, Standard for Public-Key Cryptography, is under development, with the first version expected to be ready for balloting in 1997.

The IETF's IP Security Protocol (IPSEC) Working Group (WG) is developing an Internet Key Management Protocol (IKMP) that will be specified as an application layer protocol independent of the lower layer security protocol. The IKMP will be based on ISAKMP/Oakley work begun in the Internet Draft documents for ISAKMP and the Oakley Key Determination Protocol.

3.7.9.5 Security audit. (This BSA appears in part 7, part 9, part 10, and part 11.) Security auditing is a review or examination of records and activities to test controls, ensure compliance with policies and procedures, detect breaches in security, and indicate changes in operation (paraphrased from ISO 7498-2).

3.7.9.5.1 Standards. Table 3.7-47 presents standards for security audit.

TABLE 3.7-47 Security audit standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 8: Security Audit Trail Function (same as ITU-T X.740)	10164-8:1993	Informational (Approved)
CPC	X/Open	Security Interface Specification: Auditing and Authentication	S020: 1990	Informational (Approved)

3.7.9.5.2 Alternative specifications. There are no alternative specifications.

3.7.9.5.3 Standards deficiencies. ISO Transaction Processing Security work (WDAMs to ISO 10026-1,2,3) is in the early stages. Its content is not defined, and it cannot be used for procurement. ISO 10164-8 does not define a security audit, or explain how to perform one. It does not define implementation aspects, occasions where the use of the security audit trail function is appropriate, or the services necessary for the establishment and normal or abnormal release of a management association.

There is a need for a standard for programming interfaces to support development of portable tools for audit trail analysis and configuration.

3.7.9.5.4 Portability caveats. Proposed amendments to ISO 10026 have ceased. This is a high portability risk area.

3.7.9.5.5 Related standards. The following guidelines support the TCSEC standard:

a. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation

b. NCSC-TG-011, Version 1, 1 August 1990, Trusted Network Interpretation Environments Guideline - Guidance for Applying the Trusted Network Interpretation

c. NCSC-TG-001, Version 2, June 1988, A Guide to Understanding Audit in Trusted Systems

3.7.9.5.6 Recommendations. The mandated standard is recommended.

3.7.9.6 Security alarm reporting. (This BSA appears in part 7, part 9, part 10, and part 11.) Security alarm reporting is the capability to receive notifications of security-related events, alerts of any misoperations in security services and mechanisms, alerts of attacks on system security, and information as to the perceived severity of any misoperation, attack, or breach of security.

3.7.9.6.1 Standards. Table 3.7-48 presents standards for security alarm reporting.

TABLE 3.7-48 Security alarm reporting standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 7: Security Alarm Reporting Function (same as ITU-T X.736)	10164-7:1992	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)

3.7.9.6.2 Alternative specifications. There are no alternative specifications.

3.7.9.6.3 Standards deficiencies. FIPS PUB 179-1 supersedes FIPS PUB 179. ISO 10164-7 does not define implementation aspects, specify the manner in which management is accomplished by the user of the Security Alarm Reporting Function (SARF), define interactions that result in the use of the SARF, or specify the services necessary for the establishment and normal and abnormal release of a management association.

3.7.9.6.4 Portability caveats. Portability problems with the existing standards are unknown

3.7.9.6.5 Related standards. There are no related standards.

3.7.9.6.6 Recommendations. There are no recommended standards for security alarm reporting.

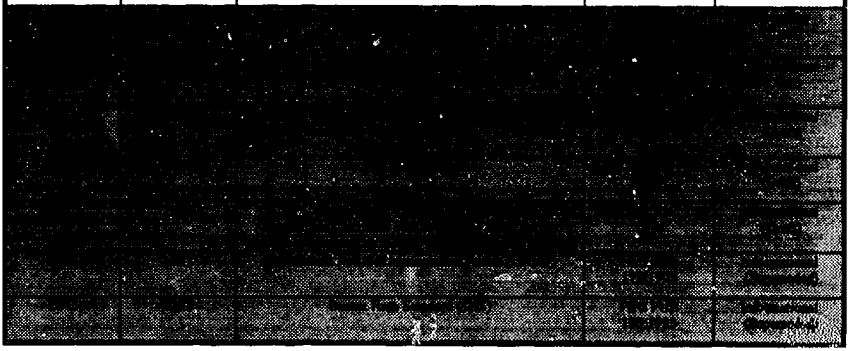
3.7.9.7 Network authentication. (This BSA appears in part 7 and part 10.) Network authentication services establish the validity of a claimed identity (peer-entity) or origin (data) (paraphrased from ISO 7498-2).

3.7.9.7.1 Standards. Table 3.7-49 presents standards for network authentication.

TABLE 3.7-49 Network authentication standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Information Technology - Defense Standardized Profiles AMHXn(D)- Message Handling Systems - Message Security Protocol (MSP) Parts 1-5	MIL-STD-2045-18500: 1993	Mandated (Approved)
IPC	ITU-T	The Directory: Authentication Framework (X-ref: ISO 9594-8)	X.509, Version 3: 1993	Mandated (Approved)
GPC	DOD	Trusted Network Interpretation	NCSC-TG-005, Version 1: 1987	Mandated (Approved)
GPC	NIST	Digital Signature Standard (DSS)	FIPS PUB 186:1994	Mandated (Approved)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180-1:1995	Mandated (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 3 (SP3)	SDN.301, Revision 1.5: 1989	Mandated (Approved)
GPC	DOD	FORTEZZA Interface Control Document	FORTEZZA ICD Rev P1.5: 1994	Mandated (Approved)
GPC	DOD	FORTEZZA Plus Interface Control Document	FORTEZZA Plus ICD Rel 3.0: 1995	Mandated (Approved)
NPC	IEEE	Standard for Interoperable LAN Security - Part B: Secure Data Exchange (SDE)	802.10b:1992	Legacy (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, Rev. 3.0: 1994	Legacy (Approved)
GPC	NSA	ssage Security Protocol (MSP)	SDN.701, v. 4.0, Rev. A: 1997	Emerging (Approved)
IPC	ISO	Information Processing Systems - Open Systems Interconnection - Service Definition for the Association Control Service Element (ACSE), Revised Edition	8649:1992 (Incorporates AM 1&2)	Informational (Approved)
IPC	ISO	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the ACSE, Revised Edition	8650:1992 (Incorporates AM 1)	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 2:Security Exchange Service Element Definition	11586-2:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 3: Security Exchange Service Element Protocol Specification	11586-3:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 4: Protecting Transfer Syntax Specification	11586-4:1994	Informational (Approved)
IPC	ISO	Transport Layer Security Protocol (TLSP) (Includes Amendment 1)	10736:1994	Informational (Approved)
IPC	ISO	Network Layer Security Protocol (NLSP)	11577:1994	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems - Part 2: Authentication Framework	10181-2:1996	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
CPC	IETF	Privacy Enhancement for Internet Electronic Mail	RFC 1421-1424:1993	Informational (Draft)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 4 (SP4)	SDN.401, Rev. 1.3:1989	Informational (Approved)
GPC	NSA	Message Security Protocol (MSP) with MIME	SDN.704, Rev. 1.4: 1996	Informational (Approved)



3.7.9.7.2 Alternative specifications. There are no alternative specifications.

3.7.9.7.3 Standards deficiencies. FIPS PUB 179-1 supersedes FIPS PUB 179. Procurements requiring authentication in FTAM cannot specify a standard at this time. The ISO FTAM security effort is in its early stages. Current proprietary FTAM security is based on passwords for authentication. ISO TP security work is in the early stages. Its content is not defined, and it cannot be used in a procurement.

3.7.9.7.4 Portability caveats. Proposed security enhancements to FTAM (WDAM4 to ISO 8571) have ceased. This is a high portability risk area.

3.7.9.7.5 Related standards. NCSC-TG-011, Version 1, 1 August 1990, Trusted Network Interpretation Environments Guideline - Guideline for Applying the Trusted Network Interpretation, supports NCSC-TG-005.

3.7.9.7.6 Recommendations. The mandated standards are recommended.

MIL-STD-2045-18500 describes the security provided by MSP. It should be used for DOD message systems that are required to exchange classified and sensitive but unclassified information. It is based on Version 3.0 of the MSP documented in SDN701, "Secure Data Network System (SDNS) Message Security Protocol," Revision 1.5, 1 August 1989. MSP is under revision to Version 4.0 to accommodate, in part, Allied requirements. This DOD Standardized Profile (DSP) standard will be replaced by a portion of the U.S. Supplement to Allied Communications Publication (ACP) 123 or ACP 120, Common Security Protocol, when the revision to MSP is complete.

SP3 provides connectionless security services and is the basis for ISO 11577. SP3 is designed to be used at the top of layer 3.

DSS is intended to specify general security requirements for generating digital signatures. Conformance to this standard does not assure that a particular implementation is secure. The responsible authority in each Government agency or department shall assure that an overall implementation provides an acceptable level of security. DSS can be used in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication. It uses the Secure Hash Algorithm (SHA) specified in FIPS PUB 180-1, which supersedes FIPS PUB 180. NIST is developing a validation program to test implementations for conformance to DSS.

The following two documents should be consulted for systems required to interface with the Defense Message System (DMS):

a. FORTEZZA Interface Control Document, Rev. 1.5, 22 December 1994

b. FORTEZZA Plus Interface Control Document, Release 3.0, 1 June 1995

SDN.701, Rev.3.0, is used with DMS, Phase 1. It is for use with legacy systems only.

IEEE 802.10b is for use with legacy LANs only.

3.7.9.8 Network access control. (This BSA appears in part 7, part 9, and part 10.) Access control is the prevention of unauthorized use of a resource, including its use in an unauthorized manner.

3.7.9.8.1 Standards. Table 3.7-50 presents standards for network access control.

TABLE 3.7-50 Network access control standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Information Technology - Defense Standardized Profiles AMHXn(D)- Message Handling Systems - Message Security Protocol (MSP) Parts 1-5	MIL-STD-2045-18500: 1993	Mandated (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 3 (SP3)	SDN.301, Revision 1.5: 1989	Mandated (Approved)
NPC	IEEE	Standard for Interoperable LAN Security - Part B: Secure Data Exchange (SDE)	802.10b:1992	Legacy (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO	Transport Layer Security Protocol (TLSP) (Includes Amendment 1)	10736:1994	Informational (Approved)
IPC	ISO	Network Layer Security Protocol (NLSP)	11577:1994	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
GPC	NIST	Guidelines for Security of Computer Applications	FIPS PUB 83:1980	Informational (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 4 (SP4)	SDN.401, Rev. 1.3:1989	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179:1992	Informational (Superseded)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, v. 4.0, Rev. A: 1997	Emerging (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, Rev. 3.0: 1994	Legacy (Approved)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - The Directory - Parts 1-4 (DAM1): Access Control	ISO/IEC 9594-1:1993/ DAM1	Informational (Draft)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - The Directory - Part 8: Authentication Framework, DAM1: Access Control	ISO/IEC 9594-8:1993/ DAM1	Informational (Draft)
IPC	ISO	OSI File Transfer, Access and Management (FTAM) - Parts 1-4: Amendment 4: Enhancement to FTAM Security Services	ISO/IEC 8571-1,2,3,4:1988/ WD.4:1997	Informational (Draft)

3.7.9.8.2 Alternative specifications. There are no alternative specifications.

3.7.9.8.3 Standards deficiencies. Deficiencies in the existing standards are unknown. FIPS PUB 179-1 supersedes FIPS PUB 179.

3.7.9.8.4 Portability caveats. Proposed security enhancements to FTAM (WDAM4 to ISO 8571) has ceased. This is a high portability risk area because no standards exist.

3.7.9.8.5 Related standards. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation, and NCSC-TG-011, Version 1, August 1990, Trusted Networks Interpretation Environments Guideline - Guideline for Applying the Trusted Network Interpretation, supports the DOD 5200.28-STD.

3.7.9.8.6 Recommendations. The mandated standards are recommended.

MIL-STD-2045-18500 describes the security provided by MSP. It should be used for DOD message systems that are required to exchange classified and sensitive but unclassified information. It is based on Version 3.0 of the MSP documented in SDN.701, "Secure Data Network System (SDNS) Message Security Protocol," Revision 1.5, 1 August 1989. MSP is under revision to Version 4.0 to accommodate, in part, Allied requirements. This DOD Standardized Profile (DSP) standard will be replaced by a portion of the U.S. Supplement to ACP 123 or ACP 120, Common Security Protocol, when the revision to MSP is complete.

SDN.701, Rev.3.0, is used with DMS, Phase 1. It is for use with legacy systems only.

SP3 provides connectionless security services and is the basis for ISO 11577. SP3 is designed to be used at the top of layer 3.

The work on File Transfer, Access, and Management (FTAM) security (WDAM4 to ISO 8571) security enhancements has been suspended. Procurements requiring access control for FTAM and transaction processing should not use these standards.

IEEE 802.10b is for use with legacy LANs only.

3.7.9.9 Data encryption security. (This BSA appears in part 5, part 7, part 10, and part 11.) Encryption is the cryptographic transformation of data to produce cipher text. Standards for data encryption security services describe services such as definitions/algorithms, modes of operation, and guidelines for use for those systems that require their data to be encrypted using data encryption security services. None of these standards are for systems processing classified information.

3.7.9.9.1 Standards. Table 3.7-51 presents standards for data encryption security.

TABLE 3.7-51 Data encryption security standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Escrowed Encryption Standard (EES)	FIPS PUB 185: 1994	Mandated (Approved)
GPC	NIST	Data Encryption Standard (DES) (related to ANSI X3.92-1981/R1987/R1993)	FIPS PUB 46-2:1993 (Reaffirmed until 1998)	Informational (Approved)
GPC	NIST	Guidelines for Implementation and using the NBS Data Encryption Standard	FIPS PUB 74:1981	Informational (Approved)
GPC	NIST	Data Encryption Standard (DES) Modes of Operation (related to ANSI X3.106-1983)	FIPS PUB 81:1980	Informational (Approved)
GPC	NIST	Security Requirements for Cryptographic Modules	FIPS PUB 140-1:1994	Informational (Approved)
IPC	ISO	Modes of Operation for a 64-Bit Block Cipher Algorithm (Related to ANSI X3.106)	8372:1987	Informational (Approved)
NPC	ANSI	Data Encryption Algorithm	X3.92-1981 (R1993)	Informational (Approved)
NPC	ANSI	Digital Encryption Algorithm - Modes of Operation	X3.106-1983 (R1990)	Informational (Approved)
GPC	NIST	Advanced Encryption Standard	FIPS PUB [illegible]	Informational (Emerging)

3.7.9.9.2 Alternative specifications. The only other available specifications are proprietary, for example, RSA.

3.7.9.9.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.7.9.9.4 Portability caveats. DES applications are not interoperable with non-DES systems. Portability problems related to the EES are unknown. The U.S. controls export of cryptographic technologies, products, and related technologies as munitions. On October 1, 1996, a new federal policy allowing U.S. vendors to export products using up to 56-bit encryption, provided the vendors sign an agreement to make their 56-bit encryption technologies key-recovery-compliant within 24 months.

3.7.9.9.5 Related standards. FIPS PUB 113, Computer Data Authentication, is related to DES security mechanisms and their standards.

3.7.9.9.6 Recommendations. The mandated standard is recommended. FIPS PUB 185, EES, supports lawful authorized access to the keys required to decipher enciphered information for systems requiring strong encryption protection of sensitive but unclassified information. EES provides stronger protection than DES against unauthorized access. Devices conforming to EES may be used when replacing Type II and Type III (DES) encryption devices owned by the Government. Implementations requiring use of EES should require conformance with FIPS PUB 140-1.

On 2 January 1997, NIST announced plans to develop a FIPS, Advanced Encryption Standard, incorporating an advanced encryption algorithm to replace DES (FIPS PUB 46-2).

3.7.9.10 Traffic flow confidentiality. (This BSA appears in part 7 and part 10.) Traffic flow confidentiality is a service to protect against unauthorized traffic analysis (ISO 7498-2) by concealing presence, absence, amount, direction, and frequency of traffic.

3.7.9.10.1 Standards. Table 3.7-52 presents standards for traffic flow confidentiality.

TABLE 3.7-52 Traffic flow confidentiality standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 3 (SP3)	SDN.301, Revision 1.5: 1989	Informational (Approved)
IPC	ISO	Network Layer Security Protocol (NLSP)	11577:1994	Informational (Approved)

3.7.9.10.2 Alternative specifications. There are no alternative specifications.

3.7.9.10.3 Standards deficiencies. There are no mandated standards for traffic flow confidentiality.

3.7.9.10.4 Portability caveats. Work on proposed amendments to ISO 10026 has ceased. This is a high portability risk area, because no standards exist.

3.7.9.10.5 Related standards. There are no related standards.

3.7.9.10.6 Recommendations. No standards are recommended.

SP3 is the basis for ISO 11577.

3.7.9.11 Network integrity. (This BSA appears in part 7 and part 10.) Network integrity ensures that data is not altered or destroyed in an unauthorized manner when transmitted across a network.

3.7.9.11.1 Standards. Table 3.7-53 presents standards for network integrity.

TABLE 3.7-53 Network integrity standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Information Technology - Defense Standardized Profiles AMHXn(D)- Message Handling Systems - Message Security Protocol (MSP) Parts 1-5	MIL-STD-2045-18500: 1993	Mandated (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 3 (SP3)	SDN.301, Revision 1.5: 1989	Mandated (Approved)
NPC	IEEE	Standard for Interoperable LAN Security - Part B: Secure Data Exchange (SDE)	802.10b:1992	Legacy (Approved)
IPC	ISO	Transport Layer Security Protocol (TLSP) (Includes Amendment 1)	10736:1994	Informational (Approved)
IPC	ISO	Network Layer Security Protocol (NLSP)	11577:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 4: Protecting Transfer Syntax Specification	11586-4:1994	Informational (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 4 (SP4)	SDN.401, Rev. 1.3:1989	Informational (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, v. 4.0, Rev. A: 1997	Emerging (Approved)

3.7.9.11.2 Alternative specifications. There are no alternative specifications.

3.7.9.11.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.7.9.11.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.7.9.11.5 Related standards. ITU-T X.500: 1993 (same as ISO 9594-1), Information Technology - Open Systems Interconnection - The Directory - Overview of Concepts, Models, and Services, is a related standard.

3.7.9.11.6 Recommendations. The mandated standards are recommended.

MIL-STD-2045-18500 describes the security provided by MSP. It should be used for DOD message systems that are required to exchange classified and sensitive but unclassified information. It is based on Version 3.0 of the MSP documented in SDN.701, Secure Data Network System (SDNS) Message Security Protocol," Revision 1.5, 1 August 1989. MSP is

under revision to Version 4.0 to accommodate, in part, Allied requirements. This DSP standard will be replaced by a portion of the U.S. Supplement to ACP 123 or ACP 120, Common Security Protocol, when the revision to MSP is complete.

SP3 provides connectionless security services and is the basis for ISO 11577. SP3 is designed to be used at the top of layer 3.

SP4 is the basis for ISO 10736.

IEEE 802.10b is for use with legacy LANs only.

3.7.9.12 Systems non-repudiation. (This BSA appears in part 5, part 7, part 10, and part 11.) These standards provide the security services for non-repudiation in systems.

3.7.9.12.1 Standards. Table 3.7-54 presents standards for systems non-repudiation.

TABLE 3.7-54 Systems non-repudiation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Digital Signature Standard (DSS)	FIPS PUB 186:1994	Mandated (Approved)
GPC	DOD	Information Technology - Defense Standardized Profiles AMHXn(D)- Message Handling Systems - Message Security Protocol (MSP) Parts 1-5	MIL-STD-2045-18500: 1993	Mandated (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, Rev. 3.0: 1994	Legacy (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, v. 4.0, Rev. A: 1997	Emerging (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 4: Protecting Transfer Syntax Specification	11586-4:1994	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible] (Draft)
IPC	ISO	[illegible]	[illegible]	Informational (Draft)
IPC	ISO	[illegible]	[illegible]	Informational (Draft)
IPC	ISO	OSI Distributed Transaction Processing (DTP) - Draft Amendments to Parts 1 to 3: Transaction Processing Security	WDAMs (SC21 N [illegible] to ISO 10026-1,2,3) 1991	Informational (Draft)

3.7.9.12.2 Alternative specifications. There are no alternative specifications.

3.7.9.12.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.7.9.12.4 Portability caveats. Portability problems in the existing standards are unknown.

3.7.9.12.5 Related standards. FIPS PUB 180-1, Secure Hash Standard, must be used with FIPS PUB 186. FIPS PUB 180-1 provides the Secure Hash Algorithm used in generating and verifying electronic signatures.

3.7.9.12.6 Recommendations. The mandated standards are recommended for non-repudiation.

MIL-STD-2045-18500 describes the security provided by MSP. It should be used for DOD message systems that are required to exchange classified and sensitive but unclassified information. It is based on Version 3.0 of the MSP documented in SDN.701, "Secure Data Network System (SDNS) Message Security Protocol," Revision 1.5, 1 August 1989. MSP is under revision to Version 4.0 to accommodate, in part, Allied requirements. This DSP standard will be replaced by a portion of the U.S. Supplement to ACP 123 or ACP 120, Common Security Protocol, when the revision to MSP is complete.

MSP provides for signed receipts. S/MIME, an Internet Draft specification, does not provide for signed receipts.

3.7.9.13 Electronic signature. (This BSA appears in part 5, part 7, and part 10.) Electronic signature is the process that operates on a message to ensure message source authenticity and integrity, and source non-repudiation. Electronic signatures are composed so that the identity of a signatory and integrity of the data can be verified.

3.7.9.13.1 Standards. Table 3.7-55 presents standards for electronic signature.

TABLE 3.7-55 Electronic signature standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Digital Signature Standard (DSS)	FIPS PUB 186:1994	Mandated (Approved)
IPC	ISO	Digital Signature Scheme Giving Message Recovery	9796:1991	Informational (Approved)

3.7.9.13.2 Alternative specifications. Rivest-Shamir-Adelman (RSA) Public Key Algorithm RC-5 was developed and published in 1994. It is proprietary, but RSA Data Security is working to have it included in numerous Internet standards. At present, RC-5 is not recommended for DOD use because it is proprietary.

3.7.9.13.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.7.9.13.4 Portability caveats. DSS applications are not interoperable with non-DSS systems.

3.7.9.13.5 Related standards. FIPS PUB 180-1, Secure Hash Standard, must be used with FIPS PUB 186. FIPS PUB 180-1 provides the Secure Hash Algorithm used in generating and verifying electronic signatures.

3.7.9.13.6 Recommendations. The mandated standard is recommended. FIPS PUB 186 is implemented in the FORTEZZA cryptographic card, a PC card (formerly called a Personal Computer Memory Card International Association (PCMCIA) standard card) that can be integrated into personal computers and workstations to provide security in commercial applications. FORTEZZA is being used in the Defense Message System. FIPS PUB 186 is the government-wide key cryptographic signature system.

3.7.9.14 Electronic hashing. (This BSA appears in part 5, part 7, part 8, and part 10.) Electronic hashing services compute a condensed representation of a message or a data file, often used as a measure of data integrity checking.

3.7.9.14.1 Standards. Table 3.7-56 presents standards for electronic hashing.

TABLE 3.7-56 Electronic hashing standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180-1:1995	Mandated (Approved)
IPC	ISO	Hash Functions, Part 1: General Model	10118-1:1994	Informational (Approved)
IPC	ISO	Hash Functions, Part 2: Hash Functions Using an N-Bit Block Cipher Algorithm	10118-2:1994	Informational (Approved)

3.7.9.14.2 Alternative specification. There are no alternative specifications.

3.7.9.14.3 Standards deficiencies. Deficiencies in the existing specifications are unknown.

3.7.9.14.4 Portability caveats. Portability problems with the existing standards are unknown.

3.7.9.14.5 Related standards. FIPS PUB 180-1 supersedes FIPS PUB 180 and is required for use with FIPS PUB 186, Digital Signature Standard.

3.7.9.14.6 Recommendations. The mandated standard is recommended. FIPS PUB 180-1 specifies SHA, which can be used to generate a message digest. SHA is required for use with the DSA as specified in FIPS PUB 186 and whenever an SHA is required for federal applications.

3.7.9.15 Data communications security labeling. (This BSA appears in part 7 and part 10.) Data communications security labeling encompasses the application of security labeling, which is used as the basis for mandatory access control security services and release security services.

3.7.9.15.1 Standards. Table 3.7-57 presents standards for data communications security labeling.

TABLE 3.7-57 Data communications security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Common Security Label (CSL)	MIL-STD-2045-48501: 1995	Mandated (Approved)
IPC	ISO	Transport Layer Security Protocol (TLSP) (Includes Amendment 1)	10736:1994	Informational (Approved)
IPC	ISO	Network Layer Security Protocol (NLSP)	11577:1994	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Informational (Approved)
GPC	NIST	Standard Security Label (SSL) for Information Transfer	FIPS PUB 188:1994	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.7.9.15.2 Alternative specifications. There are no alternative specifications.

3.7.9.15.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.7.9.15.4 Portability caveats. Portability problems related to the existing standards are unknown.

3.7.9.15.5 Related standards. DOD 5200.28-STD is a related standard. DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for

safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

3.7.9.15.6 Recommendations. The mandated standard is recommended and should be used for new acquisitions. MIL-STD-2045-48501 supports the exchange of security attributes, for example, sensitivity labels. It provides a means to label and protect data as it passes through communications systems and implements FIPS PUB 188 for the DOD environment. MIL-STD-2045-48501 and FIPS PUB 188 apply only to layers 3 and 4. TSIG TSIX(RE) 1.1, "Trusted Systems Interoperability Group, Trusted Security Information Exchange for Restricted Environments," includes options compatible with MIL-STD-2045-48501.

IEEE 802.10g is consistent with the SSL and the CSL.

RFC 1108 makes RFC 1038 obsolete. RFC 1108 should be used for legacy systems only. RFC 1038 is not recommended.

Acronym List

Acronyms. The acronyms used in Part 7 are defined as follows:

AAL	ATM adaptation layer
ACP	Allied Communication Publication
ADPCM	adaptive differential pulse-code modulation
AF	ATM Forum
AITS	Adopted Information Technology Standard
AJ	anti-jam
ALE	automatic link establishment
ANSI	American National Standards Institute
ARIDPCM	Adaptive Recursive Interpolated Differential PCM
ARP	Address Resolution Protocol
ATDL-1	Army Tactical Data Link 1
ATM	asynchronous transfer mode
B-Channel	bearer channel
BER	bit error ratio
B-ISDN	broadband-ISDN
BOOTP	BOOTSTRAP protocol
bps	bit per second
CDMA	code-division multiple access
CELP	code-excited linear prediction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CNR	combat net radio
CONS	connection-oriented network service
CPC	Consortia Public Consensus
CPN-C	Corporate Private Non-Consensus
CSMA/CD	carrier sense multiple access/collision detection
CVSD	continuously variable slope delta
C4I	command, control, communications, computers, and intelligence
DAMA	demand-assignment multiple access
D-channel	16- or 64-kbps channel for signaling and data
DCE	data circuit-terminating equipment
DEC	Digital Equipment Corporation
DHCP	Dynamic Host Configuration Protocol
DMS	Defense Message System
DoD	Department of Defense
DSN	Defense Switched Network
DS1	Digital Interface Rate 1 (1.544 Mbps)
DS3	Digital Interface Rate 3 (44.736 Mbps)

DSS1	Digital Subscriber Signaling System Number 1
DSS2	Digital Subscriber Signaling System Number 2
DTE	data terminal equipment
EHF	extremely high frequency
EIA	Electronic Industries Association
FDDI	Fiber Distributed Data Interface
FDMA	frequency-division multiple access
FED-STD	federal standard
FPLMTS	future public land mobile telecommunications system
FIPS	Federal Information Processing Standard
FTAM	file transfer, access, and management
FTP	File Transfer Protocol
GPC	Government Public Consensus
HDLC	high-level data link control
HF	high frequency
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IESS	Intelsat Earth Station Standard
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	internet protocol
IPC	International Public Consensus
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISUP	ISDN User Part
ITSG	Information Transfer Standards Guidance
ITU	International Telecommunications Union
ITU-T	ITU-Telecommunication Standardization Sector (formerly CCITT)
JTA	Joint Technical Architecture
JTIDS	Joint Tactical Information Distribution System
kbps	kilobit per second
kHz	kilohertz
LAN	local area network
LAP	link access protocol
LAPB	LAP balanced

LAPD	LAP on the D-channel
LF	low frequency
LLC	logical link control
LOS	line-of-sight
LPC	linear predictive coding
Mbps	megabit per second
MF	medium frequency
MIB	management information base
MIL-STD	military standard
MLPP	Multi-level Precedence and Preemption
MSE	Mobile Subscriber Equipment
MSP	message security protocol
MSR	message storage and retrieval
MTP	message transfer part
NATO	North Atlantic Treaty Organization
N-ISDN	narrowband ISDN
NIST	National Institute of Standards and Technology
NITF	National Imagery Transmission Format
NITFS	NITF standard
NNI	network-node interface
NPC	National Public Consensus
NRI	net radio interface
NRZ	non-return-to-zero
NSA	National Security Agency
OSI	Open Systems Interconnection
PCM	pulse-code modulation
PCS	personal communications services
PICS	protocol implementation conformance statement
PNNI	private node network interface
PPP	point-to-point protocol
PVC	permanent virtual circuit
QPSK	quadrature phase shift keying
rf	radio frequency
RFC	request for comment
SCCP	signaling connection control part
SHF	super high frequency
SINCGARS	Single-Channel Ground and Airborne Radio System
SMDS	switched multi-megabit data service

SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SONET	synchronous optical network
SS7	Signaling System Number 7
STANAG	standardization agreement
STU	secure telephone unit
SVC	switched virtual circuit
TAC02	Tactical Communications Protocol 2
TADIL	tactical digital information link
TAFIM	Technical Architecture Framework for Information Management
TCP	transmission control protocol
TDM	time-division multiplexing
TDMA	time-division multiple access
TIA	Telecommunications Industry Association
TOS	type of service
TP0	transport protocol class 0
TRI-TAC	Tri-Service Tactical Communications
UDP	user datagram protocol
UHF	ultra high frequency
UNI	user-to-network interface
UPT	universal personnel telecommunications
URL	uniform resource locator
UTC	coordinated universal time
VHF	very high frequency
VMF	variable message format
VTC	video teleconferencing
WNDP	worldwide numbering and dialing plan
XID	exchange identification

Index of Standards

Standard **Page**

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 8 of 14 parts)

OPERATING SYSTEM SERVICES

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

TABLE OF CONTENTS

LIST OF TABLES

3.8 Operating system services. Operating system services are the core services needed to operate and administer the application platform and provide functions for which application software can access the platform. Application programmers will use operating system services to obtain operating system functionality. However, implementors of other services may bypass the operating system to obtain functionality. Operating system services include kernel operations, commands, utilities, system management, and system security. Throughout section 3.8, references to IEEE 1003.n, 1003.n, and POSIX.n indicate the same standard and will be used interchangeably.

NOTE: Throughout Part 8, all tables have abbreviations listed under the column (Standard Type) as follows:

a. National Public Consensus = NPC
b. International Public Consensus = IPC
c. Government Public Consensus = GPC
d. Consortia Public Consensus = CPC
e. Consortia Private Non-Consensus = CPN-C
f. National Public Non-Consensus = NPN-C
g. Publicly Available Specifications = PAS

3.8.1 Kernel operations. Basic kernel services are system services that run the hardware. They provide a virtual machine for the user and programmer and are resident in memory. Kernel operations provide low-level services necessary to create and manage processes, execute programs, define and communicate signals, define and process system clock operations, manage files and directories, and control input and output processing to and from peripheral devices.

3.8.1.1 Process management and core operating system services. (This BSA appears in both part 8 and part 9.) Core operating system services are basic operating system services and interfaces, including traditional process management, memory management, time services, scheduling, terminal handling, error and exception management services, file-oriented services, and generalized input and output.

3.8.1.1.1 Standards. Table 3.8-1 presents standards for process management and core operating system services.

TABLE 3.8-1 Process management and core operating system services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
CPC	XOpen	Single UNIX Specification, System Interface Definitions, Version 2, Issue 5	C605 (2/97)	Emerging (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) Amendment 2: Threads Extension [C Language]	1003.1c:1995	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
NPC	IEEE	Test Methods for Measuring Conformance to POSIX - System Interfaces	2003.1:1992	Informational (Approved)
NPC	IEEE	POSIX-Based Supercomputing Application Environment Profile	1003.10:1995	Informational (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	IEEE	POSIX - Part 1: Protocol Independent Interfaces	P1003.1g	Emerging (Draft)
NPC	IEEE	POSIX Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1a	Emerging (Draft)
NPC	IEEE	POSIX Multiprocessor Application Environment Profile	P1003.14	Emerging (Draft)
NPC	IEEE	POSIX Interactive System Application Environment Profile	P1003.18	Emerging (Draft)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C language]. (as profiled by FIPS PUB 151-2:1993)	9945-1:1990	Informational (Superseded)
CPC	X/Open	Single Unix Specification: Spec. 1170, System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Informational (Superseded)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.8.1.1.2 Alternative specifications. Other consortia or de facto alternative specifications (such as ECMA APIW) for the Portable Operating System Interface for Computer Environments (POSIX) standard P1003.1 are available.

3.8.1.1.3 Standards deficiencies. ISO 9945-1:1996 incorporated IEEE 1003.1b Realtime and IEEE 1003.1c Threads. This resolves some of the deficiencies in the original POSIX.1, but the following deficiencies remain in the available standards:

a. Lacks batch scheduling for distributed computing.

b. Has weak event, error, and exception management services.

c. Has weak or no generalized I/O device driver services.

d. Has reentry problems when used for multiprocessing.

e. Reliability and maintainability not reflected in the standard.

f. The tasking model on which Ada is based does not map well to the process model on which POSIX.1 is based.

g. Has tape handling facilities requiring long backup times.

3.8.1.1.4 Portability caveats. Different specifications and implementations conforming with POSIX (e.g., OSF/1, SVID, SVR4, X/Open, and vendor products) often support the same function, but support them slightly differently. For example, the names of system calls may be identical, but unanticipated incompatibilities will arise because of differences in the data types of the function, the data types of the arguments, the return values, the required header files, and the symbolic error values.

Implementations conforming with POSIX may require extra header files for function calls that are ported from a system not requiring header files to another requiring header files. Although the impact of requiring extra header files is not always clear, differences in header file requirements can reduce portability. For example, if a program is ported from a system not requiring a header file for a particular function call, to a system requiring it, the call to that function may be undefined and generate an error message about the nonexistent header file.

Differences within header files can reduce portability when moving from a system that does not require a header file to one that does. For example, a header file may define attributes like data types or symbols conflicting with locally defined symbols.

Implementations of systems conforming with POSIX may refer to devices by logical names, numeric indicators, data structures, or pointers. Superset functions in implementations conforming with POSIX are important to have and convenient to use, but they reduce portability.

The meaning of ownership of "symbolic links" is not clear or consistent across different systems. Only the meaning of owning a file is consistent.

Many system attributes, such as system limits and configuration values limits, are defined by implementation.

3.8.1.1.5 Related standards. The following standards are related to process management and core operating system services or their standards:

a. IEEE 1003.2:1992: POSIX - Shell and Utilities.
b. IEEE 1003.2a:1992: POSIX - User Portability Extension.
c. IEEE P1003.1e: POSIX - Security Interface Extensions.

d. IEEE P1003.21: POSIX - Real Time Distributed Systems Communications.
e. X/Open Common Desktop Environment (XCDE) - Definitions and Infrastructure.

3.8.1.1.6 Recommendations. The mandated standards are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. IEEE 1003.1b (section 3) standardized additional functions not in 9945-1:1990 such as memory management and clocks and timers. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. It specifies many of the implementation-defined system limits related to files and directories and input/output.

To ensure maximum portability and smooth running information processing functions, it is important to determine, at a detailed level (e.g., arguments, order of the arguments, data types of the function and arguments, return values, symbolic error numbers), the specific areas of incompatibility between POSIX and the systems bid by vendors.

To ensure that no harm will result if an application is ported from a system that requires and supports a header file to a system that does not require the "include" statement in the system call, remove the header file from the application.

Avoid the use of extensions to POSIX. However, if extensions to POSIX must be used (they may be convenient), the applications in which they are used must be designed carefully for portability (e.g., separate the portable from the nonportable code, carefully document all nonportable code).

Including those header files required by POSIX.1 will ensure that properly written programs will build successfully on all FIPS-certified POSIX.1, regardless of which header files may be optional on a given vendor's platform.

Specifying that systems must conform to the X/Open's Single Unix Specification as demonstrated by a current X/Open Branding Certificate will eliminate the portability problems identified in the first paragraph of the portability caveats section.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.1.2 File management services. File management is the system of rules and policies for maintaining a set of files including how files can be created, accessed, retrieved, and deleted. The application program interfaces provide a vehicle for an application program to access and update a file whether the file is on a local or remote system. Commands and protocols required to access remote files are covered by the Distributed File Services BSA.

3.8.1.2.1 Standards. Table 3.8-2 presents standards for file management services.

TABLE 3.8-2 File management services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume I Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	IEEE	POSIX, Part 1: Real Time System API Extensions	P1003.1d	Emerging (Draft)
NPC	IEEE	POSIX - Part 1: System API Amendment: Real-Time Distributed System Communication	P1003.21	Emerging (Draft)
NPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1g	Emerging (Draft)
GPC	NIST	POSIX Real Time Extensions	FIPS PUB (future)	Informational (Formative)
CPC	X/Open	Single Unix Specification (Spec 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C455 (6/94)	Informational (Superseded)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C language]. (as profiled by FIPS PUB 151-2:1993)	9945-1:1990	Informational (Superseded)

3.8.1.2.2 Alternative specifications. The following specifications are also available:

a. Berkeley 4.2/4.3 Unix: Unix File System (UFS) (Tahoe fast file system).
b. Unix COFF file format

3.8.1.2.3 Standards deficiencies. POSIX does not support mandatory file locking . The advisory locking that it supports instead can lead to accidental file access collisions and corrupted

data, unless the processes using the advisory locking cooperate and use the advisory mechanism before doing input and output operations on the file.

POSIX.1 lacks the "seekdir" capability (to set a position in a directory stream) and the "telldir" capability (to tell a position in the directory stream). These are popular capabilities supported by X/Open, and System V Interface Definition. They have been proposed for the POSIX.1a revision.

POSIX.1 lacks the following symbolic link capabilities: "symlink()" to make a symbolic link, "readlink() to read a symbolic link, and "lstat() to get the status of a symbolic link. Symbolic links are important because they allow users and vendors to provide backward compatibility and portability for applications, without requiring changes to every line of code in every application that refers to a file that is no longer in a particular directory. The "symlink()," "readlink()," and "lstat()" are supported by the SVID. They have been proposed for the POSIX.1a revision.

POSIX.1a lacks all interfaces for mounting file systems and getting file system information about a mounted file system (e.g., "mount()," "statfs()," "statvfs()," "fstatfs()," "vstatvfs()," and "ustat()"), and does not plan to standardize such capabilities in the future. These capabilities are included in the Remote File Access base service area.

POSIX.1 lacks the following capabilities supported by the SVID, but are not proposed for the POSIX.1a revision. Of these, "poll()" may be proposed for the POSIX.1a revision, and "fsync()" was moved to the POSIX.1b real time standard under a new and separate option (_POSIX_FSYNC, ...):

"ftw"	Traverse a file tree
"mknod()"	Make a special file (for a device)
"mktemp()"	Make a unique file name
"poll()"	Test or wait for file events
"sync()"	Synchronize a file's state

POSIX.1 lacks the following capabilities to manipulate a binary search tree: "tsearch()," "tfind()," "tdelete()," and "twalk()." These capabilities are supported by X/Open, and the SVID, but are not proposed for the POSIX.1a revision.

3.8.1.2.4 Portability caveats. Too many "standard" file systems exist. This significantly reduces the chances of portability. POSIX does not define the directory tree organization or the files located in particular directories. Therefore, applications written to different vendors' operating systems compliant with POSIX may be nonportable. Directory and file organizations are generally similar in most Unix-like implementations. However, System V.4's directory and file organization differs from the one in System V.3 and Berkeley Unix and OSF/1 (which is based on Berkeley Unix). The difference in the file and directory organization is one of the major causes of nonportability across System V.4 and Berkeley Unix.

3.8.1.2.5 Related standards. The following standards are related to file management or file management standards:

a. IEEE 1003.2:1992: POSIX - Shell and Utility Application Interface.

b. IEEE R1003.5: 1992 Ada Language Binding (under revision).

c. IEEE P1003.1e: Security Interface Standards for POSIX.

d. IEEE P1387.1: POSIX System Administration - Part 1:Overview.

e. IEEE 1387.2:1995: POSIX System Administration - part 2:Software.

f. IEEE P1387.3: POSIX System Administration - Part 3:User and Group Administration.

g. IEEE P1003.1g: Protocol Independent Interfaces.

h. IEEE 1224.2-1993: Directory Services Application Program Interface (API).

i. IEEE P1003.1f: Network Services for Portable Application (former 1003.8).

j. X/Open Common Desktop Environment (XCDE) - Services and Applications.

3.8.1.2.6 Recommendations. The mandated standards are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. It specifies group ID settings. IEEE 1003.1b added to file management utilities (truncate and synchronize) found in the 1990 version of 9945-1. The SUS adds capabilities for directories and links.

Directory and file organizations are generally similar across most Unix implementations (e.g., System V.3). However, System V.4's directory and file organization differs from the one in System V.3 and Berkeley Unix. Therefore, standardization probably will be based on a particular Unix-based variant's file system organization (e.g., X/Open XPG4, SVID) in addition to POSIX.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.1.3 Input/Output control. (This BSA appears in both part 8 and part 9.) Input/Output (I/O) control standards include services such as device initialization, device attachment, asynchronous operation, error notification, raw I/O, and other services needed to implement logical device drivers in a system.

Input/output control enables control of different media devices over the network through software. The media devices include video cassette recorders, laser disc players, video cameras, CD players, and so on. Control capabilities may be available on the workstation through a graphical user interface (GUI). They are similar to the controls on the device, such as play, record, reverse, eject, and fast forward. Input/output control is important because it enables the operator to control video and audio remotely without requiring physical access.

3.8.1.3.1 Standards. Table 3.8-3 presents standards for input/output control.

TABLE 3.8-3 Input/Output control standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, System Interface Definitions, Version 2, Issue 5	C605 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
NPC	IEEE	POSIX Part 1: Real Time System API Extensions	P1003.1d	Emerging (Draft)
NPC	IEEE	POSIX Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1e	Emerging (Draft)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C language]. (as profiled by FIPS PUB 151-2:1993)	9945-1:1990	Informational (Superseded)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (Part of XPG4)	C434 (9/94)	Informational (Superseded)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.8.1.3.2 Alternative specifications. The following specifications are also available:

a. Berkeley 4.2/4.3 Unix.
b. OSF: OSF/1 (product implementation).

3.8.1.3.3 Standards deficiencies. POSIX.1 provides basic input/output primitives, but lacks the generalized services needed to implement device drivers for many types of devices. POSIX.1b provides support for asynchronous and synchronized I/O, but also lacks generalized services needed to implement device drivers for many types of devices.

3.8.1.3.4 Portability caveats. The "ioctl" function, which is associated with the control of an asynchronous device (including terminal characteristics) has been identified repeatedly as a source of portability problems. It is an old system call, and during the many years it has been in Unix, several variants have evolved. The differences appear at low levels. However, it is not always easy to spot these differences, because each "ioctl" is defined loosely and makes its own assumptions. As networking becomes more common, the device drivers executing some code may be located across a network, remote from the source of the system call. The many variants and interpretations of "ioctl," complicate networking because the same "ioctl" system call possibly cannot be used across a network to control a remote peripheral. For example, the SVID version of "ioctl" looks like a completely different call. Because of the difficulty in reaching agreement on a standardized version of the "ioctl," the POSIX standards groups eliminated "ioctl" from the standard early. Because the POSIX.1b real time group believes that most devices communicate using "ioctl," there was a move to reinstate and standardize "ioctl" in the P1003.1b standard. The final result, however, was the incorporation of specfic "tc" (terminal control) functions to replace each "ioctl" function.

The use of "ioctl" calls to set certain terminal modes causes problems because a single, standard terminal interface or portable mechanism to set the modes of an asynchronous terminal does not exist. Such a standard has not been defined, because it would require the "raw" (unprocessed) and "cooked" (processed) modes to be defined. Defining these would create other problems. However, not defining them could cause application codes to be written in a nonportable way.

The SVID and XPG support the "ioctl" call as part of their device service interfaces. In practice, this support is different on every different implementation of these specifications. The "ioctl" function, while deprecated for asynchronous terminal control in favor of the POSIX.1 "tc" functions, is still required to control other, less common device types. Unfortunately there is no standard for programmatic control of video cameras, etc., even though every system which supports such a device will provide the basic control functionality needed in some way.

3.8.1.3.5 Related standards. The following standards are related to input/output control or input/output control standards:

a. ISO 10164-7: Security Management.

b. IEEE P1003.1e: Security Interface Standards for POSIX.

c. IEEE 1003.2d:1994: POSIX Batch Environment Amendments.

d. IEEE P1201.1: Uniform API-GUI.

e. NIST FIPS 179-1:1995: GNMP (Government Network Management Protocol): Authentication.

f. MIT Consortium: X Window System.

3.8.1.3.6 Recommendations. The mandated standards are recommended for input/output control. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. It specifies read/write functionality. The "tc-functions" were introduced into POSIX.1 to solve portability issues arising from "ioctl" calls. X/Open SUS covers all the core POSIX functions.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.1.4 Interprocess communication. Interprocess communication (IPC) facilities enable different processes to exchange information, either within a single computer, or across a network. Some communications methods are designed strictly for use within a single computer but others, while providing local communications, were designed for networked operations. The following interprocess mechanisms have been standardized:

a. Message Queues. Message queues provide a fast local IPC mechanism well suited to real time applications.

b. FIFOS. FIFOS, also known as "named pipes", provide the same functionality as traditional Unix pipes, but unlike traditional pipes, the readers and writers of a FIFO do not need to have an "ancestor process" in common to prepare the pipe for use.

c. Sockets. Berkeley BSD Unix 4.2 introduced the concept of the socket as a protocol-independent method of accessing network functionality. The socket API provides access to both local and remote processes over a variety of network protocols including TCP/IP and the OSI protocol family.

d. XTI. XTI is X/Open's specification of the System V TLI API, which also provides a protocol independent method for accessing network functionality.

3.8.1.4.1 Standards. Table 3.8-4 presents standards for interprocess communication.

TABLE 3.8-4 Interprocess communication standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, Networking Services, Version 2, Issue 5	C523 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interface Definitions, Version 2, Issue 5	C605 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	IEEE	POSIX - Part 1: Protocol Independent Interfaces	P1003.1g	Emerging (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.1.4.2 Alternative specifications. The following specifications are also available:

a. Berkeley 4.2/4.3 Unix.
b. OSF: OSF/1 (product implementation).
c. SAE ARD 50067 Draft: Avionics Operating System API Requirements.

3.8.1.4.3 Standards deficiencies. The POSIX.1b message-passing services are minimal and are designed with emphasis on performance rather than robustness to make the best match of functions and interfaces of real time kernels used for embedded systems. POSIX.1b only supports sending messages between processes on a single machine (no network capability is specified). POSIX.1b does not support the ability to wait on multiple message queues simultaneously and does not provide a facility to broadcast a single message to multiple queues.

3.8.1.4.4 Portability caveats. The POSIX.1b message-passing interface differs from and is incompatible with the message-passing interfaces in XPG4, SVID, and Berkeley Unix. However, XPG3, XPG4, SVID, and Berkeley Unix support the same message passing interfaces. POSIX.1b message passing interfaces designate separate commands for each function, rather than following the SVID technique of providing a single command with multiple variables for many functions.

The POSIX.1b message-passing interface includes asynchronous notification to apprise a task of the availability of a message on the queue. The receiving task is notified of the time at which a message was sent, the sender of the message, and the use of pathnames for identifying message queues. Neither System V nor Berkeley Unix providers such an asynchronous notification.

POSIX.1b message prioritization allows the application to determine the order in which messages are received. Prioritization of messages is a key facility provided by most real time kernels, is

used heavily by the applications, and helps to avoid priority inversions in the message system. Neither System V Streams nor Berkeley Unix sockets supports classification of message and out-of-order selective receipt according to the classification. This POSIX.1b capability allows applications to be designed to eliminate a significant problem with Ada rendezvous in which Ada queues tasks in strict FIFO order, ignoring priorities. However, it also increases the incompatibilities between POSIX.1b and the SVID.

3.8.1.4.5 Related standards. The following standard is related to interprocess communication:

a. IEEE P1003.1e: Security Interface Standards for POSIX.

3.8.1.4.6 Recommendations. The mandated standards are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. If real-time IPC is required on a single computer, then POSIX.1b message queues (incorporated into ISO/IEC 9945-1:1996) are recommended. Unfortunately, there are as yet, no internationally approved standards for real-time IPC between computers on a network. However, both the IEEE P1003.1g and the IEEE P1003.21 draft standards provide APIs for process-to-process communication over a network. If a broad range of IPC mechanisms are required, then X/Open SUS should be considered, since it provides the full range of functions.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.1.5 Environment and internationalization services. Environment and internationalization (I18N) services provide an application with a variety of attributes and variables to set and retrieve attributes of the operating system environment in which the application is executing. Some of the environment attributes which are usually available are user ID, group ID, process ID, terminal ID, network node identification, stack size, and current time and date. The I18N attributes that are available are timezone, language to be used for messages, currency symbol, and date format.

3.8.1.5.1 Standards. Table 3.8-5 presents standards for environment and internationalization services.

TABLE 3.8-5 Environment and internationalization services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Services and Applications	C323 (4/95)	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Definitions and Infrastructure	C324 (4/95)	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, Commands and Utilities, Issue 5, Version 2	C604 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interface Definitions, Version 2, Issue 5	C605 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
GPC	NIST	C (Adopts ANSI/ISO/IEC 9899:1992)	FIPS PUB 160:1992	Informational (Approved)
GPC	NIST	Representation of Calendar Date and Ordinal Date for Information Interchange (adopts ANSI X3.30-1985/R1991)	FIPS PUB 4-1:1988 Change Notice 3/25/96	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1a	Emerging (Draft)
NPC	IEEE	POSIX, Part 2: Shell and Utilities - (Additional Utilities)	P1003.2b	Emerging (Draft)
IPC	ISO/IEC	C, Amendment 1: Integrity Addendum	9899:1994 PDAM	Informational (Draft)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Informational (Superseded)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Informational (Superseded)
CPC	X/Open	Single UNIX Specification (Spec. 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C436 (9/94)	Informational (Superseded)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.1.5.2 Alternative specifications. The following specification is also available:

a. Berkeley 4.2/4.3 Unix.

3.8.1.5.3 Standards deficiencies. ANSI C defines the base functionality for program internationalization, but it is lacking in certain areas. X/Open Single Unix Specification (SUS) provides a full set of internationalization APIs, but its support for multibyte character sets (such as those used by Asian languages) is based on an old draft of the MSE standard from ISO.

ISO/IEC 9945-1:1996 POSIX.1 does not support the function "cuserid()" to get the control terminal login-user name, even though this function was specified in the IEEE POSIX.1:1988 standard.

POSIX.2 lacks several environment variables present in the SVID, such as "SEV_LEVEL" (to set the severity level for error messages), "MSGVERB" (message format selection control), and "NETPATH" (network identifiers).

POSIX.1 does not support the "putenv()" function to add or change an environment variable or the "clearenv()" variable to clear the process environment, because these functions were considered to be more oriented toward system administration than ordinary applications. Objectors have since identified application uses, and the "putenv()" and "clearenv()" functions have been proposed for the POSIX.1a revision.

3.8.1.5.4 Portability caveats. A number of locale-specific environment variables associated with POSIX actually are set in the American National Standards Institute (ANSI) C <locale.h> headers. As a result, non-POSIX operating systems can provide a certain degree of compatibility with operating systems based on POSIX. For the same reasons, systems compliant with POSIX and running Ada, Fortran, and other non-C programs may exhibit areas of incompatibility. The environment variables and functions related to internationalization face potential application portability problems.

The function "cuserid()" (common terminal login user name) is specified by X/Open (to be withdrawn), and the SVID, but not POSIX.

The POSIX "getgrp()" function to obtain the process group ID for a specified process is based on the System V "getpgrp()" function, rather than the more complex Berkeley 4.3 Unix "getpgrp()" function and is incompatible with the Berkeley Unix function.

The "putenv()" function is specified by X/Open and the SVID, but not by POSIX.

The "clearenv()" function is specified only by OSF/1.

Because the multibyte character support mandated by X/Open is required to conform to an older draft of the ISO MSE, there will be portability problems when moving internationalized code between systems which conform to X/Open SUS and systems which have been tracking the emerging standards in this area more closely. Once the draft MSE standard has been approved, X/Open will be aligning SUS with the standard.

3.8.1.5.5 Related standards. The following standards are related to environment services or environment services standards:

a. X/Open T906:3/95: X/Open Portability Guide (XPG4).

3.8.1.5.6 Recommendations. The mandated standards are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. It specifies the number of group IDs. SUS adds I18N APIs. FIPS 160 defines program I18N. Use the function "getpwuid(geteuid())" to get the information previously supplied by the no longer supported POSIX.1 function "cuserid()."

Systems requiring the "MSGVERB" environment variable or the Berkeley-style "getpgrp" call should specify conformance to X/Open's Single Unix Specification (Spec 1170), which includes POSIX.1 conforming APIs, as well as the traditional interfaces and functions discussed above. Regardless, non-POSIX APIs should be avoided, if there is a POSIX interface which provides equivalent functionality, in order to increase the portability of the application to future platforms. Systems which will be made available to NATO partners and thus require the ability to support multiple languages should mandate X/Open SUS conformance.

In a GUI environment, XCDE provides information about screen size, resolution, number of colors available, and other programs which are active.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.1.6 Login services. To login is to gain access or sign in to a computer system. If restricted, it requires a user to identify himself by entering an ID number and/or password.

3.8.1.6.1 Standards. Table 3.8-6 presents standards for login services.

TABLE 3.8-6 Login services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.1.6.2 Alternative specifications. The following specifications are also available:

a. Berkeley 4.2/4.3 Unix.
b. OSF: OSF/1.

3.8.1.6.3 Standards deficiencies. The current operating system standards do not specify login. An operating system must provide a way to login, so implementations provide this service in nonstandard ways.

3.8.1.6.4 Portability caveats. Because login services are used almost exclusively by users, rather than applications, the only difficulty caused by the lack of login service standards is one of drivability. Login was not included in X/Open's Single Unix Specification because login utility is terminal oriented, not used by application programs.

3.8.1.6.5 Related standards. The following standards are related to login services or login service standards:

a. IEEE P1201.1: Uniform API-Graphical User Interfaces.

3.8.1.6.6 Recommendations. There are no recommended standards.

3.8.1.7 Storage device management. (This BSA appears both in part 8 and part 9.) Storage device management is familiar to most people as "Logical Volume Management." With logical volume management, a logical volume manager provides disk partition flexibility by allowing the disk partitions to grow automatically as the system runs, and by allowing files to span physical volumes. This allows a given file to be larger than any one disk. This flexibility is possible because the logical volume manager manages the disk space by creating what it calls "logical volumes." The logical volume manager determines the correspondences between the logical volumes and the actual physical volumes. A logical drive is an allocated part of a physical drive designated and managed as an independent unit. Hierarchical storage management and archiving addresses the ability to handle different levels of storage transparently, such as disks, tapes, and juke boxes.

3.8.1.7.1 Standards. Table 3.8-7 presents standards for storage device management.

TABLE 3.8-7 Storage device management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Distributed File Service (DFS)	DCE 1.1 DFS:1994	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE): Network File Service (NFS)	DCE 1.1 NFS:1994	Informational (Approved)
CPC	OSF	OSF/1 Operating System	OSF/1 O.S.	Informational (Approved)
CPC	UDI Group	Uniform Driver Interface (UDI) Specification	UDI Rev 0.75	Informational (Permissive)

3.8.1.7.2 Alternative specifications. Future releases of SVR4 will support the Logical Volume Manager, but no other alternative specifications are available.

3.8.1.7.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.8.1.7.4 Portability caveats. Portability caveats are unknown at this time.

3.8.1.7.5 Related standards. No standards are related to storage device management.

3.8.1.7.6 Recommendations. Open Software Foundation's Distributed File Service is recommended. Logical volume managers are extremely valuable, as many system managers know who have had to back up a system, take it down, repartiation it to accommodate the growth of applications and data in certain partitions, and restore the system, only to do the same thing months later. The logical volume manager eliminates this problem by allowing partitions to grow dynamically.

3.8.1.8 System operator services. System operator services are used by a system administrator or network manager to monitor a system or network, usually on a console or another computer.

3.8.1.8.1 Standards. Table 3.8-8 presents standards for system operator services.

TABLE 3.8-8 System operator services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1a	Emerging (Draft)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) [C language] (as profiled by FIPS PUB 151-2 (1993)	9945-1:1990	Informational (Superseded)

3.8.1.8.2 Alternative specifications. The following specification is also available:

a. Berkeley 4.2/4.3 Unix.

3.8.1.8.3 Standards deficiencies. POSIX lacks services allowing the system operator to control the system services or reconfigure system software so that the platform can perform properly. POSIX has only minimal services and interface to access configuration information or system status.

3.8.1.8.4 Portability caveats. Portability problems with the existing standards are unknown.

3.8.1.8.5 Related standards. The following standards are related to system operator services or system operator service standards:

a. IEEE 1003.2:1992: POSIX - Shell and Utility Application Interface.

b. IEEE P1003.1e: Security Extension to POSIX.

c. IEEE P1387.1: POSIX System Administration - Part 1: Overview.

d. IEEE 1387.2:1995: POSIX System Administration - Part 2:Software.

e. IEEE P1387.3: POSIX System Administration - Part 3: User and Group Administration.

f. IEEE P1003.1g: Protocol Independent Interfaces.

g. IEEE 1224.2:1993: Directory Services API Language Independent.

h. IEEE P1201.1: Uniform API-Graphical User Interfaces.

i. IEEE 1224:1993: OSI Abstract Data Manipulation: API (X.400).

j. IEEE P1238.1: OSI API - FTAM.

k. IEEE P1351: OSI API - ACSE.

l. NIST FIPS 179-1:1995 GNMP.

3.8.1.8.6 Recommendations. The mandated standards are recommended. ISO 9945-1:1996 incorporates IEEE 1003.1b which standardizes scheduling functions not in the original POSIX.1. FIPS 151-2 specifies job control functions. POSIX provides only minimal operator services.

3.8.1.9 Process checkpoint and restart. (This BSA appears both in part 8 and part 9.) Checkpoint and restart is a method of recovering from a system failure. A checkpoint is a copy of the computer's memory saved periodically on disk along with the current register settings (e.g., the last instruction executed). In the event of any failure, the last checkpoint serves as a recovery point. When the problem has been fixed, the restart program copies the last checkpoint into memory, resets all the hardware registers, and starts the computer from that point. Any transactions in memory after the last checkpoint was taken until the failure occurred will be lost. Checkpoint restart is helpful in any system running long jobs and requiring more time than can be expected between system down-times, and in any job that would be inconvenient to start over in the event of a system failure.

3.8.1.9.1 Standards. Table 3.8-9 presents standards for process checkpoint and restart.

TABLE 3.8-9 Process checkpoint and restart standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.1.9.2 Alternative specifications. The only other specifications available are proprietary.

3.8.1.9.3 Standards deficiencies. P1003.1a does not specify how files and directories are identified in the checkpoint file.

3.8.1.9.4 Portability caveats. One checkpoint restart implementation provides a value of "RESTART_FORCE" to restart a checkpoint file or directory, whether or not it could be restarted rationally. This behavior cannot be used in a portable way, since no predictable meaning exists for restarting a process that was in a condition that could not be checkpointed.

3.8.1.9.5 Related standards. ISO IS 9804/9805: CCR is related to process checkpoint and restart.

3.8.1.9.6 Recommendations. Too many unresolved issues are in the checkpoint restart specification in the P1003.1m draft standard to specify the emerging checkpoint restart specification. Issues range from the error codes to how much of the process state to specify explicitly.

Checkpoint/restart, originally in P1003.1a system services as a separate API is now a separate IEEE project work item under P1003.1m. This work was started by the Super Computer and Batch processing systems working groups in conjunction with the P1003.1a working groups to provide mechanisms to suspend a long executing job and/or provide checkpoints along the way so it could be restarted if something happened during execution.

3.8.1.10 System resource limits. (This BSA appears both in part 8 and part 9.) Resource limits functionality allows system administrators to control the amount of system resources available to users.

3.8.1.10.1 Standards. Table 3.8-10 presents standards for system resource limits.

TABLE 3.8-10 System resource limits standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Adopted (Approved)
NPC	IEEE	POSIX-Based Supercomputing Application Environment Profile	1003.10:1995	Informational (Approved)
NPC	IEEE	POSIX - Part 1: System API, Amendment 1: C Language Limits Interface (C Language)	P1003.1b	Emerging (Permissive)
CPC	X/Open	Single UNIX Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C455 (6/94)	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (Replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.8.1.10.2 Alternative specifications. The following specifications are also available:

a. Berkeley 4.3 Unix.
b. Cray Research, Inc.: "limits" interfaces.
c. OSF: OSF/1 Operating System: "getrlimit/setrlimit."

3.8.1.10.3 Standards deficiencies. The Berkeley Unix and System V "setrlimit" and "ulimit" interfaces have the limitation that users may act only to make their limits more restrictive.

3.8.1.10.4 Portability caveats. The actual numeric limit values for different resource limits are not portable across various platforms. Applications need to provide some sort of configuration parameters to specify the actual numeric values for each site.

3.8.1.10.5 Related standards. The following standards are related to resource limits or resource limit standards:

a. ISO/IEC 9945-1:1996: POSIX.1 System Application Programming Interfaces.
b. IEEE P1003.1e: Security Interface Standards for POSIX.
c. IEEE P1387.1: POSIX System Administration - Part 1: Overview.
d. IEEE 1003.2d:1994: POSIX Batch Environment Amendments.

3.8.1.10.6 Recommendations. X/Open Single Unix Specification (SUS) provides "setrlimit/getrlimit" functionality.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.1.11 Kernel language bindings. These standards provide programming language interfaces to kernel services.

3.8.1.11.1 Standards. Table 3.8-11 presents standards for kernel language bindings.

TABLE 3.8-11 Kernel language bindings standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, Networking Services, Version 2, Issue 5	C523 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
NPC	IEEE	POSIX Ada Language Interfaces, Part 1: Binding for System API	1003.5:1992	Informational (Approved)
NPC	IEEE	POSIX Ada Language Interfaces - Part 1:Binding for Realtime Extensions	1003.5b:1996 (former 1003.20)	Informational (Approved)
NPC	IEEE	POSIX FORTRAN 77 Language Interfaces - Part 1: Binding for System API	1003.9:1992	Informational (Approved)
NPC	IEEE	Test Methods for Measuring Conformance to POSIX - System Interfaces	2003.1:1992	Informational (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1a	Emerging (Draft)
NPC	IEEE	POSIX, Part 1: System API - Amendment a: Protection, Audit, and Control Interfaces (C Language), Draft 15	1003.1e: 1995	Emerging (Draft)
NPC	IEEE	POSIX, Part 1: Network-Transparent File Access	P1003.1f	Emerging (Draft)
NPC	IEEE	POSIX - Part 1: Protocol Independent Interfaces	P1003.1g	Emerging (Draft)
NPC	IEEE	POSIX - Protocol Independent Interfaces (Ada Language)	P1003.5c	Informational (Draft)
NPC	IEEE	POSIX, Part 1: System Application Programming Interface, Language Independent Specification	P1372 (former 1003.1 LIS)	Informational (Formative)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Informational (Superseded)
CPC	X/Open	Single Unix Specification (Spec. 1170), Networking Services, Issue 4 (part of XPG4)	C438 (9/94)	Informational (Superseded)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C language] (as profiled by FIPS PUB 151-2:1993)	9945-1:1990	Informational (Superseded)

3.8.1.11.2 Alternative specifications. No applicable consortia or industry specifications for kernal bindings to C or Ada exist because ANSI C and ISO Ada bindings are provided by the standard. However, XPG4, SVID, and OSF/1 include a C language binding.

3.8.1.11.3 Standards deficiencies. No standard, consortia, or de facto specifications exist or are in progress for POSIX.1, Unix, or OSF/1 bindings to Cobol, C++, APL, Common Lisp, Modula-2, PL/1, or Prolog.

3.8.1.11.4 Portability caveats. The Fortran-77 binding uses some nonstandard features, such as longer names, that the proposers believed will become available soon in compilers and linkers. Also, under the Fortran-77 binding, all system service calls begin with the characters "F77." In addition, the Fortran-77 binding uses procedure calls for all interactions with system services, instead of using traditional Fortran statements like "OPEN" and "READ" to accomplish similar tasks. Such non-Fortran standard features leave open questions about interactions between the redundant ways of doing things, and the intermixing of POSIX calls and ordinary Fortran-77 services dealing with the same resources.

The C language bindings have no known problems.

3.8.1.11.5 Related standards. The following standards are related to kernal language bindings:

a. ISO 1539:1991: Fortran-90.
b. ISO 8652, FIPS 119, DOD MIL-STD 1815A:1983: Ada.
c. IEEE 1003.2:1992: POSIX - Shell and Utility Application Interfaces.
d. IEEE P1003.2a: POSIX - User Portability Extension.
e. ANSI X3.9-1978: Fortran-77.
f. ANSI 9899-1990: C Programming Language.
g. X/Open C140:8/91: Xlib - C Language Binding.

3.8.1.11.6 Recommendations. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. ISO/IEC 9945-1:1996 and FIPS 151-2 provide binding guidance to POSIX.1. The operating system binding requirement for FIPS 151-2 must reflect the programming language used in the application. POSIX 1003.5 and 1003.9 provide binding guidance for other languages. X/Open Single Unix Specification Networking Services covers the interfaces in the IEEE draft P1003.1g, Protocol Independent Interfaces. The Fortran-77 binding is quite workable, and undoubtedly will provide the means for making POSIX services more available to Fortran programs. Some members of the POSIX.9 Group have characterized the Fortran-77 bindings as a "stopgap" measure while defining the POSIX.1 binding for Fortran 90, an area in which work has begun.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of

Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.1.12 Threads interface. (This BSA appears in both part 8 and part 11.) A traditional UNIX process has a single thread of control. A thread of control, or more simply a thread, is a sequence of instructions executed in a program. A thread has a program counter (PC) and a stack to keep track of local variables and return addresses. A thread is one transaction or message in a multithreaded system or an individual process within a single application. Thread interfaces are specifications for interfacing with these processes.

Thread services provide an underlying service for multiple concurrent executions within a single computer process. They are designed to allow independent operation and are essential for functions such as multiple process communications in a distributed computing environment. Threads provide improved software responsiveness through increased use of the inherent synchronous execution (i.e., parallelism) of programs. The threads service in DCE allows all DCE-enabled applications to execute multiple actions simultaneously. Applications can accept information from users, execute RPCs, and access databases at the same time. The threads service is used by several DCE services, including the RPC, Security, Directory, and Time Services. The OSF has designed the threads service to be easily accessible by programmers wishing to use it in applications. Services can be accessed through the C programming language, and through other high-level programming languages.

3.8.1.12.1 Standard. Table 3.8-12 presents standards for threads interface.

TABLE 3.8-12 Threads interface standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) Amendment 2: Threads Extension [C Language]	1003.1c:1995	Informational (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Threads (based on the draft 4 version of IEEE 1003.1c.)	DCE 1.1 Threads:1994	Informational (Approved)
NPC	IEEE	POSIX Part 1: System API - Amend a: Technical Corrigenda to Threads API Extensions (C Language)	P1003.1a	Emerging (Formative)
CPC	X/Open	Aspen Threads Extension	Aspen Threads	Informational (Formative)

3.8.1.12.2 Alternative specification. The OSF/1 Operating System's Mach-Based Multithreaded Kernel is also available.

3.8.1.12.3 Standard deficiencies. Because the Pthreads interface is not designed specifically for Ada, it can impose a great overhead burden on an Ada run-time system. The Ada rendezvous feature is not supported by Pthreads, which is a major problem for real time applications.

OSF DCE Threads are incompatible with Ada Tasking. Programmers can use one or the other, but not both. Since DCE Threads underlie OSF RPC, Ada progrmmers should be cautious in the use of tasking. (Reference: Understanding DCE by Rosenberry, Kenney, and Fisher)

3.8.1.12.4 Portability caveats. Ada83 and, to an even greater extent, Ada9x already contain many of the capabilities defined in the 1003.1c standard. This can cause many conflicts with Ada. Vendors may implement Ada tasks in a way that interferes with the implementation of Pthreads. Also, if the Ada vendor does not implement tasks as pthreads, conflicts may arise between what Ada can and cannot do and what pthreads can do. For example, the Ada rendezvous feature is not supported by Pthreads. On the other hand, Pthreads provides some extended features, such as dynamic priorities, that have not been standardized by the Ada language, but that are in demand, especially by real time users.

3.8.1.12.5 Related standards. The following standards are related to threads services:

a. IEEE P1003.1e: Security Interface Standards for POSIX.

b. IEEE P1003.21: POSIX - Real Time Distributed Systems Communication.

c. NIST FIPS 151-2:1993, Portable Operating System Interface (POSIX)-System Application Program Interface [C Language] (ISO/IEC 9945-1:1990) 1993.

3.8.1.12.6 Recommendations. The mandated standards are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. The OSF DCE threads is based on a draft version of IEEE P1003.1c Pthreads. OSF intends to move to the new IEEE 1003.1c standard in a future version of DCE. In the meantime, DCE users should specify DCE threads to ensure compatibility with currently available DCE products. However, they should also specify that these products will be able to migrate to the new version of DCE when OSF adopts the approved 1003.1c standard.

To the extent an Ada runtime system uses standard POSIX interfaces, it will be portable across operating systems compliant with POSIX. Some of the problems caused by Ada operations not currently mapped to Pthreads will be resolved by the Ada binding to the 1003.1c Pthreads standard.

3.8.1.13 Threads extension language binding. These standards provide a programming language interface to POSIX.

3.8.1.13.1 Standards. Table 3.8-13 presents standards for threads extension language binding.

TABLE 3.8-13 Threads extension language binding standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.1.13.2 Alternative specifications. The POSIX/Ada Real-Time (PART) project (a project at Florida State University, Tallahassee, FL, which is funded by the Ada Joint Program Office under the Ada Technology Insertion Program through the U.S. Army Communications-Electronics Command (CECOM) and Telos Corporation) has developed an Ada binding specification for P1003.1c (formerly P1003.4a) Pthreads.

Studies show that POSIX Pthreads conflict with Ada. (The Ada-Pthreads conflicts, under "Portability caveats," are taken from David K. Hughes' (Comcon, Inc., Moorestown, NJ) paper circulated in POSIX.5 (Ada Bindings)).

3.8.1.13.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.8.1.13.4 Portability caveats. Developing an Ada binding for the Pthreads Extension to POSIX will be more difficult than developing the Ada binding for P1003.1 and P1003.1b because the overlap between the services provided by Pthreads and the Ada language is much greater. This can cause model, style, and kernel-level conflicts. Similar problems arising with signals and process creation in the P1003.5 standard were resolved by reserving certain operations for use by the Ada run-time system and providing some operations to the application with warnings that they are unsafe. This approach also can be used with Pthreads, but it will need to be applied to the whole Pthreads.
The following are some of the Ada-Pthreads conflicts, excerpted from Hughes' paper:

a. pthread_once. Use of pthread_once would affect style adversely.

b. pthread_create. Pthread_create is not consistent with elaboration,activation, or dynamic allocation of task. It is in direct conflict with Ada at the application level.

c. pthread_attr_setlgetstacksize. Without access to pthread_create, these functions can have no effect on an underlying pthread implementation of Ada tasks from the application level.

d. pthread_join. Pthread_join is not like Ada. It does not conflict with any Ada construct directly, but can interfere with task rendezvous and task hierarchy. It requires a link with RTS from the application level.

e. pthread_detach. Pthread_detach may conflict with implementation specific and implementation-defined pragmas.

f. pthread_exit. Pthread_exit conflicts with scoping rules and Ada task termination semantics at the application level.

g. pthread_mutex*_*.

h. pthread_cond*_*. Pthread_cond*_* has an adverse effect on Ada programming conventions at the application level, with potential for run-time complexity and conflict. Interference with implementation-defined pragmas is a real danger. The shared memory semantics are problematic. Its signal effects by priority are also problematic.

i. pthread_kill. Pthread_kill conflicts with abort at the application level.

j. pthread_cancel.

k. pthread_setintr.

l. pthread_setintrtype.

m. pthread_testintr. Pthread_testintr is in direct conflict with Ada at all levels.

n. pthread_cleanup_pushlpop. Pthread_cleanup_pushlpop is tied to thread cancellation. It is fundamentally incompatible with Ada style, because it lacks pointer-to-function in Ada. Visibility at the application level is hazardous, as RTS may rely on the content of the cancellation handler.

3.8.1.13.5 Related standards. The following standards are related to POSIX.1c bindings:

a. ISO/IEC 9945-1:1996: POSIX System Application Programming Interfaces.

b. IEEE P1003.1e: Security Extension to POSIX.

c. IEEE P1003.5b: POSIX - Ada Language Interfaces -- Part 1: Binding for Realtime Extensions.

3.8.1.13.6 Recommendations. The POSIX.1c standard is not ready to be the basis for early Ada application use. The standard needs an Ada binding, and the Ada binding committee needs a firm platform to resolve the threads versus tasks issue.

Most potential portability problems concerning Ada and Pthreads will have to be resolved by the Ada Binding to Pthreads.

3.8.1.14 Data typing services. Because POSIX and UNIX files are simple byte streams, with no structure imposed on them by the O/S, as is common in mainframe environment, the type of data stored in a file must be tagged in some way. Common methods of tagging data include using the file name suffix as an indicator (for example, ".c" or "tar") or writing a recognizable header in the first part of the file (so-called "magic numbers").

3.8.1.14.1 Standard. Table 3.8-14 presents standards for data typing services.

TABLE 3.8-14 Data typing services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Services and Applications	C323 (4/95)	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Definitions and Infrastructure	C324 (4/95)	Mandated (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.1.14.2 Alternative specification. The following specifications are also available:

a. Berkeley 4.2/4.3 Unix.
b. OSF OSF/1.
c. Mortice Kern Systems' MKS Toolkit ("file" command).

3.8.1.14.3 Standard deficiencies. The "file" command, as defined by POSIX, does not provide for user definition of new files types.

3.8.1.14.4 Portability caveats. All of the alternative specifications provide for a "magic" file which allows new file types to be defined. Although the basic format of this file is the same for all implementations, there are minor differences between them which hinder the sharing of this file. POSIX.2b is attempting to remedy this by defining a standard format for the magic file, but no implementations which conform to this draft standard exist.

3.8.1.14.5 Related standards. None

3.8.1.14.6 Recommendations. ISO 9945-2 is recommended. If user configuration is required, conformance to the draft P1003.2b standard for the format of the magic file is recommended. In a GUI environment, the XCDE data typing services are recommended. Data typing facilities are inherent in the format of the OpenDoc "Bento" storage structure.

3.8.1.15 Large file support. As UNIX systems have become increasingly more powerful, a number of system vendors and UNIX independent software vendors have developed a requirement to access files that contain more information than can be addressed using a signed long integer. A number of system vendors and users have been meeting at the "Large File Summit" to develop a set of changes to the existing Single UNIX Specification (SUS) that allow both new and converted programs to address files of arbitrary sizes. This set of changes was included in the latest version of the SUS. In addition, a set of transitional extensions intended to permit users to immediately implement large file support on typical 32-bit UNIX operating systems has been included.

3.8.1.15.1 Standards. Table 3.8-15 presents standards for large file support.

TABLE 3.8-15 Large file support standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)

3.8.1.15.2 Alternative specification. There are no alternative specifications.

3.8.1.15.3 Standard deficiencies. Standards deficiencies are unknown.

3.8.1.15.4 Portability caveats. Portability problems with existing specifications are unknown.

3.8.1.15.5 Related standards. Standards related to large file support are unknown.

3.8.1.15.6 Recommendations. Users with a requirement to create/access large files should continue to monitor the actions of the Large File Summit.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

For current systems, users should ensure that vendors incorporate the set of extensions to the SUS in their current compliant products.

3.8.1.16 Dynamic linking. Dynamic linking is a mechanism that allows executable code to be segmented into distinct modules called dynamically linked libraries (DLLs). An application can, with some restrictions, directly call the functions provided by a DLL after linking with it. Furthermore, any given Dll can be concurrently linked to and used by multiple applications.

3.8.1.16.1 Standards. Table 3.8-16 presents standards for dynamic linking.

TABLE 3.8-16 Dynamic linking standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Single UNIX Specification, Commands and Utilities, Issue 5, Version 2	C604 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interface Definitions, Version 2, Issue 5	C605 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)

3.8.1.16.2 Alternative specification. There are no alternative specifications.

3.8.1.16.3 Standard deficiencies. Deficiencies in the existing standards are unknown.

3.8.1.16.4 Portability caveats. Portability is a problem in this area because there are no established standards.

3.8.1.16.5 Related standards. There are no related standards.

3.8.1.16.6 Recommendations. Dynamic linking specifications are being formalized to include in the next version of the Single Unix Specification.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.2 Media handling. Media handling refers to standards for disk and tape formatting for data and interchange of data with applications. The concept of layered storage is not described in standards documents. However, a digital data interchange (DDI) reference model was presented to ANSI X3/SPC by the NIST representative to X3 media committees. This model is Level 4, Special application on media; Level 3, Logical format for media; Level 2, Physical format on media; Level 1, Media.

3.8.2.1 Backup and restore. (This BSA appears both in part 8 and part 9.) Backup and restore standards provide facilities and interfaces to save data as a precaution to system failure and restore the system to a previous data state after failure.

3.8.2.1.1 Standards. Table 3.8-17 presents standards for backup and restore.

TABLE 3.8-17 Backup and restore standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	[illegible] System Interface (POSIX) Part 1: [illegible] 9945-1:1990 and incorporates [illegible] and 1003.1i)	9945-1:1996	Mandated (Approved)
IPC	ISO/IEC	Information Technology - [illegible] Operating System Interface (POSIX) - Part 2: Shell and Utilities (profiled by FIPS PUB 189)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, Commands and Utilities, Issue 5, Version 2	C604 (2/97)	Emerging (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	ANSI	Recorded Magnetic Tape for Information Interchange (1600 cpi, Phase Encoded)	X3. 39-1986 (R1992)	Informational (Approved)
NPC	ANSI	Recorded Magnetic Tape for Information Interchange (6250 cpi, Group-Coded Recording)	X3. 54-1986 (R1992)	Informational (Approved)
CPC	OSF	OSF/1 Operating System	OSF/1 O.S.	Informational (Approved)
NPC	IEEE	POSIX - Part 1: System API Supplement - Removable Media Support	P1003.1E	Emerging (Formative)
CPC	X/Open	Single UNIX Specification Spec. 1170 Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C435 (9/92)	Informational (Superseded)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C language] (as profiled by FIPS PUB 151-2:1993)	9945-1:1990	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification Spec. 1170)	SVID Issue 4	Informational (Superseded)

3.8.2.1.2 Alternative specifications. The "dd" utility is useful for data copy with optional conversion that promotes portability, (e.g., ASCII to EBCDIC) or for record conversion with discrete record sizes, or multiple sector reads/writes to disk. The Berkeley Unix "dump" command is also available. The OSF's OSF/1 "tar" and "cpio" utilities and USG's System V Release 4 (SVR4) are also available.

3.8.2.1.3 Standards deficiencies. Although the "tar" and "cpio" commands can be used to back up disks, they are very limited in capability. "tar" and "cpio" are copy commands. These commands do not perform incremental backups. Furthermore, "tar" does not span multiple disks. No Ada bindings exist for distributed backup and restore standards.

3.8.2.1.4 Portability caveats. The "ustar" format is an extension of the historical "tar" archive format and, as such, may be read by historical implementation of the "tar" command. The POSIX.2 "pax" command has been developed as a replacement for both "tar" and "cpio" commands. It can read and write "ustar" and "cpio" archives, and most implementations have been extended to read historical "tar" format archives as well.

The "cpio" command can produce two different types of archives: "character"and "binary." The binary archives are non-portable, and cannot be read except on the same platform on which they were produced. POSIX documents only the character "cpio" format, and the "pax" command is only guaranteed to be able to read the character format.

The Berkeley Unix-based set of "backup" commands (e.g., "dump" and "rdump") are not the same as the backup commands based on System V (SVID) (e.g., "backup," "bkexcept,"). The two backup systems have different interfaces and do not work in a compatible manner.

3.8.2.1.5 Related standards. The following standards are related to backup and restore or backup and restore standards.

a. ISO/IEC 9595: CMIS.

b. ISO/IEC 9596: CMIP.

c. ISO/IEC DIS 11578.2: RPC.

d. Network Management Forum: OMNIPoint 1.

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

f. Internet RFC 1157: Simple Network Management Protocol.

g. Internet RFC 1158: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

3.8.2.1.6 Recommendations. ISO/IEC 9945-1 and ISO/IEC 9945-2 archiving services are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. "Pax" was commissioned for POSIX.2 because "tar" and "cpio" were considered

inadequate. "Pax" is similar to "tar" and "cpio." The "tar" and "cpio" formats are expected to be retired from a future version of POSIX.1 in favor of the newer "ustar" format.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.2.2 Floppy disk format and handling. (This BSA appears both in part 8 and part 9.) Floppy disk format and handling standards provide formats and interfaces for the exchange, backup, and restoration of data to or from floppy disks.

3.8.2.2.1 Standards. Table 3.8-18 presents standards for floppy disk format and handling.

TABLE 3.8-18 Floppy disk format and handling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, Commands and Utilities, Issue 5, Version 2	C604 (2/97)	Emerging (Approved)
CPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
IPC	IEEE	POSIX - Part 1: System API Supplement - Removable Media Support	P1003.1k	Emerging (Transitioning)
CPC	X/Open	Single UNIX Specification (Spec. 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C494 (9/94)	Informational (Superseded)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C Language], (as profiled by FIPS PUB 151-2:1993)	9945-1:1990	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.8.2.2.2 Alternative specifications. The following alternative specifications are also available:

a. Sun Microsystems' SunOS/Solaris command "bar"
b. OSF: OSF/1 "tar" and "cpio" utilities.

3.8.2.2.3 Standards deficiencies. POSIX and Unix have very poor floppy disk handling capabilities. Most standards related to floppy disks concern logical interfaces that permit the interconnection of floppy disk peripherals.

3.8.2.2.4 Portability caveats. The "bar" is not a standard. However, it is widely used because of Sun's large installed base. It is presented as an example of a capability needing to be standardized, as well as an example of the kind of capability that could be specified.

3.8.2.2.5 Related standards. No standards are related to floppy disk format standards.

3.8.2.2.6 Recommendations. ISO/IEC 9945-2 disk format services "pax" are expected to replace "tar" and "cpio" utilities in POSIX.1.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.2.3 POSIX tape labeling and tape volume processing. (This BSA appears both in part 8 and part 9.) Tape labels are a fixed portion of data stored on tape media and containing certain types of administrative information automatically readable by tape-handling software. Among the information typically stored on tape labels are the identification of the media content, ownership of the media content, access control information for the media content, and the format of the rest of the information on the media.

3.8.2.3.1 Standards. Table 3.8-19 presents standards for POSIX tape labeling and tape volume processing.

TABLE 3.8-19 POSIX tape labeling and tape volume processing standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ECMA	File Structure and Labeling of Magnetic Tapes for Information Interchange	13 (1985)	Informational (Approved)
IPC	ECMA	Magnetic Tape Cassette Labeling and File Structure for Information Interchange	41 (1973)	Informational (Approved)
IPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API [C Language]	P1003.1a	Emerging (Draft)
IPC	IEEE	POSIX - Part 1: System API Supplement - Removable Media Support	P1003.1f	Emerging (Formative)

3.8.2.3.2 Alternative specifications. The only other available specifications are proprietary.

3.8.2.3.3 Standards deficiencies. The P1003.1a draft standard does not address the issue of processing several files as if they were a single entity.

Traditional Unix systems do not provide mechanisms for protected access to devices or media, nor do they generally provide mechanisms for label processing or transparent volume switching.

3.8.2.3.4 Portability caveats. To provide tape handling portability, a standard must specify the handling of ANSI/ISO labeled tape and IBM labeled tape. IBM labeled tapes, although not a strict standard, represent vast numbers of labeled tapes already in existence. IBM labeled tapes are roughly analogous to the ANSI standard, except the labels are written with the EBCDIC character set rather than with ASCII.

It is not certain, even within the proposed standard, how to process information when some of it is on 9-track tape and some on 8mm (Exabyte) tape, or some on labeled and some on unlabeled tape. This may be a limitation of the standard.

3.8.2.3.5 Related standards. The following standards are related to POSIX tape labeling and tape volume processing standards:

a. ISO/IEC 9945-1:1996: POSIX Part 1: System Application Programming Interface.
b. ISO/IEC 9945-2:1992: POSIX Part 2: Shell and Utility.

c. IEEE 1003.5:1992: Ada Language Binding to POSIX.
d. IEEE P1003.1e: Security Interface Standards for POSIX.
e. IEEE P1387.1: POSIX System Administration - Part 1: Overview.
f. IEEE 1003.9:1992: Standard Fortran Language Bindings to POSIX.

3.8.2.3.6 Recommendations. There are no recommendations.

3.8.2.4 Data interchange format. Data interchange file format is the format of files to be copied from a medium to the file hierarchy and from the file hierarchy to a medium.

3.8.2.4.1 Standards. Table 3.8-20 presents standards for data interchange format.

TABLE 3.8-20 Data interchange format standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)

3.8.2.4.2 Alternative specifications. There are no alternative specifications.

3.8.2.4.3 Standards deficiencies. Standards deficiencies are unknown.

3.8.2.4.4 Portability caveats. The "ustar" format is an extension of the historical "tar" archive format and, as such, may be read by historical implementation of the "tar" command. The POSIX.2 "pax" command has been developed as a replacement for both "tar" and "cpio" commands. It can read and write "ustar" and "cpio" archives, and most implementations have been extended to read historical "tar" format archives as well.

The "cpio" command can produce two different types of archives: "character"and "binary." The binary archives are non-portable, and cannot be read except on the same platform on which they were produced. POSIX documents only the character "cpio" format, and the "pax" command is only guaranteed to be able to read the character format.

3.8.2.4.5 Related standards. There are no related standards.

3.8.2.4.6 Recommendations. ISO/IEC 9945-1:1996 which incorporates IEEE 1003.1b is recommended.

3.8.3 Shell and utilities. A user's shell is the interface to the operating system. Simple shells enable the user to control the environment and run programs. Traditionally, shells have been command-line oriented, and have provided simple programming facilities, allowing them to double as "job control languages." Recently, GUI and menu driven shells have become available, eliminating the need to learn complicated command lines to perform everyday tasks like reading mail or managing a calendar.

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

3.8.3.1 Commands and utilities used in applications and shell scripts. A shell script is a file of executable UNIX commands created by a text editor and made executable with the "chmod" command. These standards refer to the commands and utilities of the operating system used in the script.

3.8.3.1.1 Standards. Table 3.8-21 presents standards for commands and utilities used in applications and shell scripts.

TABLE 3.8-21 Commands and utilities used in applications and shell scripts standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Services and Applications	C323 (4/95)	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Definitions and Infrastructure	C324 (4/95)	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, Commands and Utilities, Issue 5, Version 2	C604 (2/97)	Emerging (Approved)
NPC	IEEE	POSIX - Part 1: Protocol independent interfaces	P1003.1g	Emerging (Draft)
NPC	IEEE	POSIX, Part 2: Shell and Utilities - (Additional Utilities)	P1003.2b	Emerging (Draft)
NPC	IEEE	POSIX Interactive Systems Application Environment Profile	P1003.13	Emerging (Draft)
CPC	X/Open	Single UNIX Specification (Spec. 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C434 (6/94)	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.8.3.1.2 Alternative specifications. The following specifications are also available:

a. Berkeley 4.2/4.3 Unix.

b. GNU Utilities (Public domain utilities from the Free Software Foundation).
c. OSF: OSF/1.

d. Mortice Kern Systems Inc.'s MKS Toolkit a toolkit with POSIX.2 and POSIX.2a compliant shell, tools, and utilities, as well as other traditional Unix language tools and utilities for Unix and DOS computers, which is being implemented widely on proprietary operating systems.

3.8.3.1.3 Standards deficiencies. POSIX.2 lacks many of the advanced commands and utilities present in XPG4, the SVID, and OSF/1, such as "chroot," "col," "cancel," "atq," "dircmp," "fmt," "egrep," "line," "mktemp," "nl," "passwd," and "curses".

POSIX.2 commands and utilities lack many of the options for the commands also present in XPG4, the SVID, and OSF/1.

3.8.3.1.4 Portability caveats. POSIX.2 is not quite compatible with many of the supposedly same utilities in XPG4, the SVID, or OSF/1, because even though the command names are the same, the commands have different options. The 1003.2 standard is not the same as the Bourne shell.

Since XPG4, version 2 (the Single Unix Specification) has been aligned with POSIX.2, POSIX.2 may be considered a "lowest common denominator" for future releases of proprietary Unix platforms like Solaris and HP-UX.

3.8.3.1.5 Related standards. The following standards are related to commands and utilities used in applications and shell scripts:

a. IEEE P1003.1e: Security Interface Standards for POSIX.
b. IEEE 1003.2d:1994: POSIX Batch Environment Amendments.

3.8.3.1.6 Recommendations. The interfaces to desired commands and utilities, which POSIX lacks, also must be identified and explicitly specified in procurements. The procurement's interface specification must include each command's options and syntax (e.g., order of the options, if applicable), in addition to the name of the command and the service it provides.

The following wording is recommended as part of the specification for these services:

"Commands and utilities offered as a result of the requirements of which this is a part shall conform to the requirements in the NIST FIPS 189 on POSIX Command and Utility Application Interface for Computer Operating System Environments, defined in ISO/IEC 9945-2 (POSIX: Part 2: Shell and Utilities)."

In many cases, it will be necessary to supplement the POSIX.2 commands and utilities to meet a procurement's needs. If possible, identify the most important commands and utilities lacking in POSIX.2, whose use is anticipated to be widespread across many procurements, and standardize

around these internally for all procurements. Otherwise, no backward compatibility will be present with systems not supporting these commands, and no portability across systems supporting these commands in different ways. If the commands required are part of XPG4, then conformance to Single Unix should be specified.

Aside from specifying GUI behavior and commands, XCDE also defines command line interfaces to this functionality (principally in order to "launch" the environment). XCDE is recommended for environments which require GUI functionality.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.3.2 Shell programming language. The shell programming language is a high-level programming language that can use operating system commands and utilities to build applications and shell scripts.

3.8.3.2.1 Standards. Table 3.8-22 presents standards for shell programming languages.

TABLE 3.8-22 Shell programming language standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Services and Applications	C323 (4/95)	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, Commands and Utilities, Issue 5, Version 2	C604 (2/97)	Emerging (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.3.2.2 Alternative specifications. The following specifications are also available:

a. Berkeley Unix.

b. GNU Bourne Again Shell (Korn Shell Imitation with job control) (Public Domain).

c. Mortice Kern Systems Inc.'s POSIX.2- and POSIX.2a-compliant MKS Toolkit.

d. OSF: OSF/1 C Shell (csh), Korn Shell (ksh), Remote Shell (rsh), Restricted Shell (rsh, Rsh).

3.8.3.2.3 Standards deficiencies. The System V Bourne shell lacks easy arithmetic and substring manipulation capabilities, the tilde expansion, and easy command substitution nesting.

3.8.3.2.4 Portability caveats. Shell scripts written under different shells are not portable to other shells. POSIX.2 extended the System V Bourne shell with features from the Korn shell to correct historical deficiencies (e.g., those listed under standards deficiencies), as well as extending it with the Korn shell's interactive features for command-line editing.

3.8.3.2.5 Related standards. The following standards are related to shell programming languages or shell programming language standards:

a. IEEE P1003.1e: Security Interface Standards for POSIX.
b. IEEE 1003.2d:1994: POSIX Batch Environment Amendments.

3.8.3.2.6 Recommendations. Several shell features are not required by FIPS 189. These are:

a. Operators (( ))

b. Reserved words [[ ]]

c. Substring expansions
   $name#pattern
   $name%pattern
   $name##pattern
   $name%%pattern

d. String length expansion $#name

e. Command substitution syntax $(command)

f. Multi digit positional parameters

g. Assigning values with "export" and "readonly"

h. Separation of positional parameters expanded from $* and $@ by the first character of the IFS. Only the capability to separate parameters by a space is required.

i. Functions

j. Function option "-f" for the "unset" command

k. The built-in commands "alias" (to define and display aliases) and "unalias" (to remove the aliases defined)

The following wording is recommended for specifying shell programming language services:

"Shell invocation primitives and built-in commands offered as a result of the requirements of which this is a part shall conform to the requirements in the NIST 189 FIPS on POSIX Command and Utility Application Interface for Computer Operating System Environments, defined in ISO/IEC 9945-2 (POSIX: Part 2: Shell and Utilities)."

Since portability is the goal, avoid the use of the multiple, historical shells in favor of the POSIX.2 shell.

X/Open Single Unix Specification provides additional utilities. XCDE is recommended for environments that require GUI functionality.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.3.3 User-oriented commands and utilities. User-oriented commands and utilities are miscellaneous facilities used by end-users, programmers, and system operators to perform an action on an immediate personal basis.

3.8.3.3.1 Standards. Table 3.8-23 presents standards for user-oriented commands and utilities.

TABLE 3.8-23 User-oriented commands and utilities standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Services and Applications	C323 (4/95)	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, Commands and Utilities, Issue 5, Version 2	C604 (2/97)	Emerging (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.3.3.2 Alternative specifications. The following specifications are also available:

a. Berkeley Unix.
b. GNU Utilities (Public Domain Programs from the Free Software Foundation).
c. Mortice Kern Systems Inc.'s POSIX.2- and POSIX.2a-compliant MKS Toolkit.
d. OSF: OSF/1.

3.8.3.3.3 Standards deficiencies. POSIX.2 lacks many of the utilities present in XPG4, SVID, and OSF/1, such as "banner," "calendar," "help," "learn," and "spell." POSIX.2 utilities lack many of the options present in XPG4, the SVID, and OSF/1.

3.8.3.3.4 Portability caveats. POSIX.2 is compatible with the utilities in XPG4, SVID, or OSF/1 when the commands are used with no options, otherwise, compatibility is not guaranteed. Since the Single Unix Specification (Spec 1170) has aligned the XPG4 Commands and Utilities with POSIX.2, it is possible to consider POSIX.2 a "lowest common denominator" among systems that conform to Spec 1170.

3.8.3.3.5 Related standards. The following standards are related to user-oriented commands and utilities:

a. ISO/IEC 9945-1: 1996 POSIX Part 1: System Application Programming Interfaces.

b. IEEE P1003.1e: Security Interface Standards for POSIX.

c. IEEE 1003.2d:1994: POSIX Batch Environment Amendments.

3.8.3.3.6 Recommendations. The interfaces with desired commands and utilities, which POSIX lacks, also must be identified and specified explicitly in procurements. The procurement's interface specification must include each command's options and syntax (e.g., order of the options, if applicable), in addition to the command name and the service it provides.

The following wording is recommended for specifying user-oriented commands and utilities:

"Commands and utilities offered as a result of the requirements of which this is a part shall conform to the requirements in the NIST FIPS 189 on POSIX Command and Utility Application Interface for Computer Operating System Environments, defined in ISO/IEC 9945-2 (POSIX: Part 2: Shell and Utilities)."

In many cases, the POSIX.2 commands and utilities will need to be supplemented to meet a procurement's needs. To maximize portability, identify the most important user portability extension commands lacking in POSIX.2 whose use is anticipated to be widespread across many procurements, and standardize around these internally for all procurements. Otherwise, there will be no backward compatibility with systems not supporting these commands, and no portability across systems supporting these commands in different ways.

Specifying Single Unix Specification rather than POSIX.2 will eliminate the problems of non-portable extensions to POSIX.2 by ensuring that all systems procured include the same extensions.

XCDE provides a variety of user-oriented utilities related to file management, printing, and editing. The "drag and drop" functionality specified by XCDE is a graphical method of providing arguments to programs. By dragging a GUI object and "dropping" it on another object, the user instructs the target object to operate on the dropped object in an appropriate manner. For example, dropping a file on a printer icon would cause the file to be printed, but dropping a file on a directory in the file manager would cause the file to be moved, or copied.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.3.4 File and program editing services. File and program editing services refer to interactive editors, stream editors, and utilities for editing files and programs, and specialized programming languages that often are used for editing.

3.8.3.4.1 Standards. Table 3.8-24 presents standards for file and program editing services.

TABLE 3.8-24 File and program editing services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Services and Applications	C323 (4/95)	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, Commands and Utilities, Issue 5, Version 2	C604 (2/97)	Emerging (Approved)
IPC	IEEE	POSIX Interactive System Application Environment Profile	P1003.1I	Emerging (Draft)
CPC	X/Open	Single UNIX Specification (Base), [illegible] Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C436 (6/94)	Mandated (Superseded)
CPC	X/Open	System V Interface Definition (SVID) replaced by Single UNIX Specification (Spec. 1170)	SVID Issue 4	Mandated (Superseded)

3.8.3.4.2 Alternative specifications. Dozens of proprietary editors are available, among the alternative specifications are the follwing :

a. GNU Emacs from the Free Software Foundation.

b. OSF: OSF/1's red (restricted line editor), view (read-only screen editor), vedit (beginner's version of editor).

3.8.3.4.3 Standards deficiencies. The editors are not deficient. Different users merely prefer different editors.

3.8.3.4.4 Portability caveats. The portability issue involving editors is a matter of user portability. Each editor has its own interface that users must learn as they move between editors. However, editors do not affect application portability.

3.8.3.4.5 Related standards. The following standards are related to file and program editing services standards:

a. IEEE P1003.1e: Security Interface Standards for POSIX.
b. IEEE 1003.2d:1994: POSIX Batch Environment Amendments.

3.8.3.4.6 Recommendations. ISO/IEC 9945-2 (as adopted by FIPS 189) is recommended for text and stream editors to obtain POSIX conforming editing services. (While this is not critical for application portability, the increase in user portability will save both time and money in (re)training.)

For GUI environments, XCDE is recommended as well as FIPS 189.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.3.5 Print management. (This BSA appears both in part 8 and part 9.) The print services are used by management and user applications to send a file to the printer, cancel the print job, and get printer status information. The printing systems program interface is used as the base for the POSIX printing management standard. Printing management standards also provide services and interfaces for transparent remote printing, output spooling, spool queue management, and scheduling.

3.8.3.5.1 Standards. Table 3.8-25 presents standards for print management.

TABLE 3.8-25 Print management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE): XCDE Services and Applications	C323 (4/95)	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, Commands and Utilities, Issue 5, Version 2	C604 (2/97)	Emerging (Approved)
IPC	ECMA	Method for Measuring Printer Throughput	132 (1991)	Informational (Approved)
IPC	ISO/IEC	Information Technology - Text and office systems - Document Printing Application (DPA), Part 1: Abstract service definition and procedures	10175-1:1996	Informational (Approved)
IPC	ISO/IEC	Information Technology - Text and office systems - Document Printing Application (DPA) - Part 2: Protocol specification	10175-2:1996	Informational (Approved)
IPC	IEEE	POSIX: System Administration - Part 4: Print Administration (former P1003.7.1)	P1387.4	Emerging (Draft)
CPC	X/Open	Single UNIX Specification (Spec 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C436 (6/94)	Informational (Superseded)
CPC	OSF	DME Print Service (PRS) (part of OSF Personal Computer Services)	DME PRS	Informational (Not Recommended (No commercial products))

3.8.3.5.2 Alternative specifications. The following specifications are also available:

a. MIT: Palladium (the basis for DME print management).

b. Berkeley 4.2/4.3 Unix.

c. Siemens/Nixdorf: Printing Management (the basis for UI's distributed printing management specification and USL's reference implementation).

3.8.3.5.3 Standards deficiencies. SVID, OSF/1, and Berkeley Unix have no features to control the formatting or scheduling of print jobs. The SVID, OSF/1, and Berkeley Unix are designed for centralized environments. No Ada bindings exist for print management standards. POSIX.2 specifies only a minimal "lp" command, suitable for submitting print jobs; no printer administration facilities are provided.

3.8.3.5.4 Portability caveats. The System V Unix "lp" printing system, from which the POSIX "lp" command is derived, is not compatible with the Berkeley Unix "lpr" printing system.

The OSF DME distributed print management is based on MIT's Palladium. It has a different interface from UI/USL's distributed print management, which is based on the Siemens-Nixdorf Xprint program and, therefore, is incompatible.

3.8.3.5.5 Related standards. The following standards are related to print management services or standards:

a. ISO/IEC 9945-1:1996: POSIX Part 1 - System Application Programming Interface.

b. ISO 8824:1990: Abstract Syntax Notation 1 (ASN.1).

c. ISO 8825:1990: Basic Encoding Rules for ASN.1.

d. ISO 9072:1989: Remote Operations Service Element (ROSE).

e. ISO/IEC 9595: Common Management Information Service (CMIS).

f. ISO/IEC 9596: Common Management Information Protocol (CMIP).

g. ISO/IEC DIS 11578.2: Remote Procedure Call.

h. IEEE P1003.1e: Security Interface Standards for POSIX.

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

j. Internet RFC 1157: Simple Network Management Protocol.

k. Internet RFC 1158: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

l. Network Management Forum: OMNIPoint 1.

3.8.3.5.6 Recommendations. The recommendation is to specify POSIX "lp" only for traditional, centralized systems for imminent procurements. Then look to ISO 10175 or IEEE 1387.4 in the long term.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.3.6 Batch scheduling. (This BSA appears both in part 8 and part 9.) Batch scheduling refers to the ability to submit jobs to be executed when the system load permits. The "at" command allows jobs to be executed at a predefined time. Batch queuing refers to the ability to place multiple jobs in a queue for processing, and to access and manage the queue.

3.8.3.6.1 Standards. Table 3.8-26 presents standards for batch scheduling.

TABLE 3.8-26 Batch scheduling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 2:Shell and Utilities - Amendment 1: Batch Environment	1003.2d:1994	Mandated (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 15: Scheduling Function	10164-15:1995	Informational (Approved)
CPC	X/Open	Single UNIX Specification, Commands and Utilities, Issue 5, Version 2	C604 (2/97)	Emerging (Approved)
CPC	OSF	OSF/1 Operating System	OSF/1 O.S.	Informational (Approved)
CPC	X/Open	Single UNIX Specification, Spec. 1170 Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C456 (5/94)	Informational (Superseded)

3.8.3.6.2 Alternative specifications. The Berkeley BSD 4.3 Unix "at" and "batch" commands are also available.

3.8.3.6.3 Standards deficiencies. The POSIX.2 and Unix "at" and "batch" commands are designed for a single machine, centralized environment. Traditional POSIX and Unix batch capabilities, such as "at" and "batch," are inadequate and inefficient for managing resources and scheduling jobs in many environments, particularly environments that manage expensive resources, because they are very limited. For example, "at" allows users only to schedule machines to run jobs at particular times. No Ada bindings exist for the POSIX.2d Batch Queuing Extensions.

3.8.3.6.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.8.3.6.5 Related standards. No standards are related to batch scheduling.

3.8.3.6.6 Recommendations. The mandated standards are recommended, but both provide only limited batch functionality. For international work, use the POSIX.2 standard's new "-t time" option for the "at" command to express a time for execution of the submitted job in a way to support other time conventions more easily.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.3.7 Language bindings to POSIX.2. These standards provide programming language interfaces to operating system shell & utilities.

3.8.3.7.1 Standards. Table 3.8-27 presents standards for language bindings to POSIX.2.

TABLE 3.8-27 Language bindings to POSIX.2 standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (8/94)	Emerging (Approved)

3.8.3.7.2 Alternative specifications. All other consortia or de facto specifications include C bindings.

3.8.3.7.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.8.3.7.4 Portability caveats. The interpretation of the C bindings for other programming languages probably will result in some misinterpretations, which in turn, will result in some portability problems due to different interpretations and assumptions in the original C language binding.

3.8.3.7.5 Related standards. The following standards are related to language bindings to POSIX.2:

a. IEEE 1003.5:1992: Ada Language Binding for POSIX.
b. IEEE 1003.9:1992: Standard Fortran Language Bindings to POSIX.

3.8.3.7.6 Recommendations. ISO/IEC 9945-2 (as adopted by FIPS 189) is recommended for its POSIX.2 language binding, although it is limited to C.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.3.8 User-oriented mail services. One of the most important services provided by a computer system is electronic mail.

3.8.3.8.1 Standard. Table 3.8-28 presents standards for user-oriented mail services.

TABLE 3.8-28 User-oriented mail services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Services and Applications	C323 (4/95)	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, Commands and Utilities, Issue 5, Version 2	C604 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, Version 2 (plus XPG4)	C436 (6/94)	Mandated (Approved)

3.8.3.8.2 Alternative specification. The following specifications are also available:

a. OSF: OSF/1

b. Berkeley BSD 4.3/4.4 Unix "Mail" command

c. Berkeley BSD 4.3/4.4 Unix, MH message handling system (not related to OSI MHS functionality)

3.8.3.8.3 Standard deficiencies. None of the standards listed explicitly discuss inter-machine communication. The ability to send mail to users on remote systems requires the appropriate network services standards (see "related standards" below).

3.8.3.8.4 Portability caveats. None

3.8.3.8.5 Related standards. The following standards are related to electronic mail services:

a. Internet STD-10: Simple mail transfer protocol (SMTP) (RFC 821).

b. Internet STD-11: Format for Electronic Mail Messages (RFC 822).

c. ISO/IEC 9594 (nine parts plus two draft parts): OSI - - The Directory.

d. ISO/IEC 10021 (nine parts): Text Communication - Message-oriented text interchange systems (MOTIS) and Message handling systems (MHS).

3.8.3.8.6 Recommendations. Because the user interface must properly interact with the network services, making recommendations in this area is difficult. For example, there are no known implementations of the POSIX.2 mailx command which will properly communicate with an OSI-based network mail service.

POSIX.2 is recommended for command-line based environments. XCDE Mail Services is recommended for GUI environments.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.3.9 Time management services. Time management services allow both individuals and groups of people to control their time more effectively by providing functions to schedule meetings via a simple browsable and updateable interface; access group members schedules; and create and edit individual, project, or departmental "todo lists". Advanced implementations will provide privacy and authorization to ensure that people cannot see more information than they're permitted and to restrict the ability to modify the schedules of other people.

3.8.3.9.1 Standard. Table 3.8-29 presents standards for time management services.

TABLE 3.8-29 Time management services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Services and Applications	C323 (4/95)	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); Calendaring and Scheduling API (XCS)	C321 (4/95)	Mandated (Approved)

3.8.3.9.2 Alternative specification. Proprietary software is available for MS-Windows which provides the same functionality; "Day-Timer" and "Maximizer" are two well-known examples. Interoperability between such proprietary packages is virtually nonexistent.

3.8.3.9.3 Standard deficiencies. No standard deficiencies are known at this time.

3.8.3.9.4 Portability caveats. None

3.8.3.9.5 Related standards. None

3.8.3.9.6 Recommendations. XCDE is recommended for GUI environments. XCS defines data structures and interfaces for developers wishing to make applications "calendar-aware." The XCDE "drag and drop" facility allows users to associate documents with meetings by dropping them on the calendar.

3.8.4 Real time extensions. Real time extension standards provide interfaces with a collection of services designed to support predictable responses to asynchronous events. In data processing or data communications, real time means the data is processed the moment it enters a computer, as opposed to BATCH processing where the information enters the system, then is stored and operated on at a later time.

3.8.4.1 Scheduling. (This BSA appears both in part 8 and part 9.) Scheduling services and interfaces provide different scheduling policies, such as time-sharing, priority-based, and user-defined. Scheduling services initiate and terminate jobs (programs) in the computer, maintain a list of jobs to be run, and allocate computer resources depending on priority. Each process is controlled by an associated scheduling policy and priority.

Priority and preemptive scheduling standards provide interfaces to scheduling services allowing the highest-priority process to run first and to completion. Preemptive multitasking shares processing time with all running programs. For example, background programs can be given recurrent CPU time no matter how heavy the foreground load. Priority bumping is the process during a link, trunk, or facility failure where lower priority user access to network services is interrupted to offer those services or bandwidth to a predesignated higher priority user.

3.8.4.1.1 Standards. Table 3.8-30 presents standards for scheduling.

TABLE 3.8-30 Scheduling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
OPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1a	Emerging (Draft)
OPC	NIST	POSIX Real Time Extensions	FIPS PUB (future)	Informational (Forecasted)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C language], (as profiled by FIPS PUB 151-2:1993)	9945-1:1990	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.8.4.1.2 Alternative specifications. There are no alternative specifications available.

3.8.4.1.3 Standards deficiencies. The POSIX.1 standard is not suitable for real time applications, because it supports only time-sliced time-sharing scheduling and does not allow scheduling based on the priority of a process.

The POSIX "nice" command for adjusting process priorities is not suitable for real time applications, because the "nice" function is merely a request to the operating system to favor a particular process for scheduling. However, in traditional Unix and POSIX.1, the effect of the "nice" command is tempered by degrading priorities based on CPU usage. In addition, the "nice" interface specifies an adjustment to a "nice" value, rather than setting it to an explicit value. Real time applications usually want to set priority to an explicit value. Finally, "nice()" does not allow for changing the priority of another process.

POSIX.1 scheduling is not based on absolute priorities. A process's scheduling priority degrades as it runs. POSIX.1 does not allow a system operator or real time application developer to tailor process scheduling.

POSIX.1b does not address the priorities of "system" processes. If system processes are not running in low priority ranges, conflicts with real time processes could result.

POSIX.1b does not address the interaction between priority and swapping because swapping and virtual memory paging-related issues are extremely dependent on the implementation and nearly impossible to standardize. However, the POSIX.1b scheduling paradigm fully describes the scheduling behavior of runnable processes, including the requirement for the working set to be resident in memory.

POSIX.1b does not address the temporary lending of priority from one process to another by the system (e.g., for the purposes of affecting the freeing of resources).

POSIX.1b does not define the effect of I/O interruptions and other system processing activities because the effect of I/O interruptions and system loading is intrinsically nondeterministic.

Influence levels (restrictions on a process's ability to affect other processes beyond a certain level) are defined by the implementation.

POSIX.1b does not address the mechanisms used to control access to scheduling facilities.

POSIX.1b does not address whether a process' handling of an event with a higher priority should have its priority boosted. This may be addressed later.

POSIX.1b provides a minimum of 32 priority levels. While this number conforms to the currently accepted scheduling theory requiring at least 32 priority levels for predictable responses with acceptable processor utilization, it is less than the 256 priority levels that many real time systems need.

3.8.4.1.4 Portability caveats. POSIX.1b supports a time-sharing scheduling policy, a real time scheduling policy, and a user-defined scheduling policy, but does not define the default scheduling policy. This could cause problems in porting the scheduling, and as a result, could cause problems in the response time behavior of real time applications.

POSIX.1b does not address resource preemption. The lack of resource preemption standardization could affect the ability to port real time applications so that they maintain the same behavior between systems. However, this does not affect source code portability, because resource preemption functions lie underneath the POSIX.1b interface.

The POSIX.1b priority-based scheduling functions are incompatible with the System V.4 SVID and SVR4 real time extensions' priority scheduling. The System V.4 "priocntl()" interface for priority scheduling violates POSIX.1b guidelines since it uses an argument to define the system call function. This increases the complexity of the "priocntl()" system call because it consolidates a large collection of related but logically separate functions into a single interface. Also, the "priocntl()" interface is less flexible than the POSIX.1b interface, because "priocntl()" does not permit separate disjointed or overlapping priority ranges between policies.

The specification of only 32 priority levels could reduce the behavior of some applications that depend on multiple priority levels to have reduced portability across conforming implementations.

In a conforming implementation, the priority ranges for the FIFO and Round Robin scheduling policies (SCHED_FIFO and SCHED_RR) defined in the header <sched.h> must be allowed to overlap, because these scheduling policies are identical except for the time interval. Because the third scheduling policy permitted by POSIX.1b (SCHED_OTHER) is defined by the user or implementation, any interactions among SCHED_OTHER and SCHED_FIFO or SCHED_RR also is defined by the implementation. Therefore, any application that depends on this interaction is not a strictly conforming application, and may not be portable across all systems.

3.8.4.1.5 Related standards. The following standard is related to priority and preemptive scheduling standards:

a. IEEE P1003.1e: Security Interface Standards for POSIX.

3.8.4.1.6 Recommendations. The mandated standards are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. IEEE 1003.1b standardized additional functions not in the original POSIX.1. FIPS 151-2 specifies many of the implementation-defined system limits and chooses among incompatible POSIX options.

Each real time functionality in the POSIX.1b standard is an option. If procurements do not call out the POSIX.1b Execution Scheduling option explicitly, vendors may provide a system conforming with POSIX.1b but not including this option.

Procurements should require implementations to document the priority ranges in which system processes run to check that conflicts will not exist between system processes and real time processes.

If a particular default scheduling policy is desired, a procurement should either specify the default explicitly or specify the ability for system operators to define one.

System processes always should execute in low priority ranges to avoid conflict with real time processes.

A portable, standardized interface for locking portions of a process in memory is necessary to ensure that paging behavior does not affect the scheduling of real time processes.

An organization-wide standard default scheduling policy should be established. Also, applications should make no assumptions about the default scheduling policy.

Although the POSIX.1b real time standard allows source code portable applications to be written, it does not guarantee that two such applications can coexist in a single system. To minimize conflicts, developers should adhere to certain programming guidelines to document the intent, rather than the syntax, of the standardization issues.

3.8.4.2 Kernel preemption. Kernel preemption provides support for the immediate preemption of running operating system kernel processes to dispatch a higher priority process as soon as possible.

3.8.4.2.1 Standards. Table 3.8-31 presents standards for kernel preemption.

TABLE 3.8-31 Kernel preemption standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[redacted]				

3.8.4.2.2 Alternative specifications. The following specifications are also available:

a. Proprietary real time Unix systems.

b. Proprietary real time executives.

c. "Home-grown" real time kernels.

d. OSF, working in conjunction with the Center for High Performance Computing, to develop a real-time Mach microkernel.

3.8.4.2.3 Standards deficiencies. Preemption of processes, particularly kernel processes (kernel preemption), is necessary for many critical real time applications. Kernel preemption is a function of an operating system implementation, not a standardized interface. Basic Unix does not support kernel preemption at all.

3.8.4.2.4 Portability caveats. The lack of a standard for kernel preemption can reduce the portability of real time application behavior across systems. However, it should not reduce real time application source code portability because the functions responsible for kernel preemption are underneath the real time operating system interface.
Recently, skinny microkernels have been discussed as the future of real time operating systems. A real time microkernel can be embedded in a POSIX/Unix system for general real time use. For critical real time applications, the microkernel can be used as a stand-alone, real time executive. Many people do not realize that the stand-alone microkernel is not compatible with POSIX or Unix. The source code of applications or parts of applications written directly to the microkernel are not portable across POSIX or Unix systems.

3.8.4.2.5 Related standards. The following standard is related to kernel preemption standards:

a. ISO/IEC 9945-1:1996: POSIX Part 1:System Applicatin Programming Interface.

3.8.4.2.6 Recommendations. There is no specific standard for kernel preemption, but kernel preemption must cooperate with IEEE 1003.1b. The following wording is recommended for specifying kernel preemption services:

"Real time systems offered as a result of the requirements of which this is a part shall provide as full as possible kernel preemption, as opposed to preemption via preemption points. At the same time, they shall conform to the requirements, services, and interfaces specified in the IEEE 1003.1b standard for all features and functionality specified elsewhere in this document."

3.8.4.3 Semaphore functions. Semaphore standards provide operating system synchronization. One type of semaphore is a message sent when a file is opened to prevent other users from opening the same file at the same time. Its purpose is to preserve the integrity of data (i.e., stop it from being unknowingly altered) during use. Semaphores can be implemented as follows:

a. Hardware or software flags used to indicate the status of some activity.

b. Shared space for interprocess communications (IPC) controlled by "wake up" and "sleep" commands. The source process fills a queue and goes to sleep until the destination process uses the data and tells the source process to wake up.

3.8.4.3.1 Standards. Table 3.8-32 presents standards for semaphore functions.

TABLE 3.8-32 Semaphore functions standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IEEE	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPC	Open	UNIX Specification, System Interface Definitions, Version 2, Issue 5	C605 (2/97)	Emerging (Approved)
CPC	X/Open	X Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) Amendment 2: Threads Extension [C Language]	1003.1c:1995	Informational (Approved)
NPC	IEEE	POSIX Ada Language Interfaces, Part 1: Binding for System API	1003.5:1992	Informational (Approved)
CPC	NIST	POSIX Real Time Extensions	FIPS PUB (Issue)	Informational (Formative)
NPC	IEEE	POSIX, Part 1: System API - Amend: Services for Reliable, Available, and Serviceable Systems (GRAES) [C Language]	P1003.1h	Emerging (Formative)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Informational (Superseded)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.8.4.3.2 Alternative specifications. The following specifications are also available:

a. Berkeley Unix Semaphores.
b. EventCounts Services and Interfaces (rather than semaphores).

c. OSF: OSF/1 Application Environment Specification, 1.1.

3.8.4.3.3 Standards deficiencies. POSIX.1b has no concept of ownership associated with a semaphore. One process may lock a semaphore, and a second process may unlock it. This lack of semaphore ownership has many advantages. However, it also means that it is not possible to implement a facility at the operating system or the library level, whereby the system could track the ownership of semaphores for error recovery, for example.
POSIX.1b lacks facilities to prevent "priority inversion," a situation occuring when a low priority process locks a semaphore, thus delaying a high priority process, then gets preempted by one or more medium priority processes. This can result in unpredictable response time for high priority processes. This problem usually is fixed by using a priority inheritance protocol. Such a protocol is not applicable to the general semaphore used in POSIX.1b, because there can be no assurance that the process unlocking the semaphore is the same one that locks it. Therefore, the implementation cannot determine who should inherit the higher priority.

The POSIX.1b group does not address a "mutex" facility that allows the process that locks a semaphore to become the owner of the semaphore; however, such an extension is being included in the POSIX.1c Threads standard.

The semaphores specified by the SVID, XPG4, OSF, and Berkeley 4.2/4.3 Unix are too complex to use for many real time applications. POSIX.1b specifies only semaphores whose persistence implies that a semaphore and its associated state remain valid until the last reference is released. This is a change from earlier drafts where nonpersistent semaphores could be specified. These would be unlocked if not actively referenced by a process, even though the name remains.

The sem_ifpost() function for posting to a binary semaphore has been removed (although it is standard practice in some contexts), because no convincing rationale was found for keeping it.

3.8.4.3.4 Portability caveats. The number of different, incompatible, nonportable semaphore specifications is almost equal to the number of different standards groups and consortia specifying semaphores.

The SVID, XPG4, OSF, and Berkeley 4.2/4.3 Unix specify and/or provide "resource" semaphores. The POSIX.1b real time extensions specify the simpler "binary" semaphores. Binary and resource semaphores are not compatible. Furthermore, the resource semaphores specified by the SVID and X/Open are not compatible with the resource semaphores specified by OSF/1 and Berkeley 4.2/4.3 Unix.

The POSIX.1b semaphore mechanism is unlike the proposed mutex and condition variable facility of POSIX.1c. Although this problem has been addressed through a substantial rewrite of semaphores retaining the 1003.1b binary semaphore functionality while closely matching the 1003.1c facilities, portability and incompatibility difficulties still may be present.

3.8.4.3.5 Related standards. The following standard is related to semaphore standards:

a. IEEE P1003.1c: Security Interface Standards for POSIX.

3.8.4.3.6 Recommendations. If the application in question is a critical real time application, specify ISO/IEC 9945-1:1996 which incorporates IEEE 1003.1b binary semaphores. First, the simpler binary semaphore is more suited to many critical real time applications. Second, developers write or customize their own semaphores for many critical real time applications, and the simpler binary semaphores are easier to learn and customize. The following wording is recommended for specifying real time semaphores:

"Real time systems offered as a result of the requirements of which this is a part shall provide as full as possible kernel preemption, as opposed to preemption via preemption points, and, at the same time, shall conform to the requirements, services, and interfaces specified in the IEEE 1003.1b standard for all of the features and functionality specified elsewhere in this document."

The more complex resource semaphores of System V Unix can be built on top of the POSIX.1b binary semaphores.

If nonpersistent semaphore behavior is needed, it may be emulated by removing the semaphore from the name space so that upon the last close of the semaphore, all resources associated with it will be released. If two unrelated processes want nonpersistent behavior, either they must synchronize up front, or they must provide for cleanup when they have no further use for the semaphore. Such methods of achieving nonpersistent semaphore behavior are complex and can cause portability of behavior problems.

Correctly written conforming implementations should not rely on either persistence or non-persistence, because persistence and system reboot are terms that mean different things to different people.

Currently, semaphores cannot be implemented using POSIX.1c "mutexes" and condition variables because these are not usable between processes. A reasonably efficient implementation based on mutexes and condition variables would not be safe enough for the signal handler invocations to post to semaphores used outside of signal context.

Applications using POSIX.1b semaphores must be careful of their robustness because no facility exists for determining whether one of the cooperating processes suddenly has become uncooperative.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.4.4 Memory management. Memory management services provide ways to optimize, protect, and control memory. These services include shared memory, memory locking and memory mapping.

Shared memory is the portion of memory accessible to multiple processes. When two or more processes share some memory, that memory is in two (or more) places at once. It's mapped into the address spaces of all processes concerned. If one process writes a value into a particular byte of shared memory, the other processes see it almost immediately (depending on the physical characteristics of the underlying hardware memory coherence system). Virtual memory combines physical memory and a swap space, which is the disk space used for memory overflow. Use of virtual memory allows different processes to appear to share the same physical page, and it makes the computer appear to have more memory than it actually does.

Process memory locking standards provide services via an interface allowing a programmer to lock a program, or part of a program or process, in main memory instead of letting it be moved to a disk.

Memory mapped I/O refers to the ability of a system to have its data transferred by transferring pointers to areas of memory.

3.8.4.4.1 Standards. Table 3.8-33 presents standards for memory management.

TABLE 3.8-33 Memory management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, System Interface Definitions, Version 2, Issue 5	C605 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amend: Services for Reliable, Available, and Serviceable Systems (SRASS) [C Language]	P1003.1h	Emerging (Formative)
OPC	NIST	Portable Operating System Interface (POSIX) - Real Time Extensions: Memory Mapped Files Option	FIPS PUB (future)	Informational (Formative)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Informational (Superseded)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Informational (Superseded)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)

3.8.4.4.2 Alternative specifications. The following specifications are also available:

a. Berkeley: Berkeley Software Distribution (BSD) Unix.
b. OSF: OSF/1 (product implementation).

3.8.4.4.3 Standards deficiencies. The SVID, XPG4, OSF/1, and Berkeley Unix consider shared memory a basic, general purpose, system capability. However, shared memory is not specified in the POSIX.1 kernel interfaces, and requires the specification of POSIX.1b real time extensions for non-real time procurements.

POSIX.1b leaves the behavior of "read()," "write()," and "lseek()" on shared memory unspecified. However, implementations using file mapping can use these functions.

POSIX.1b specifies only persistent shared memory objects. This reduces the complexity resulting from specifying nonpersistent objects. However, for processes to share memory, the mechanism supporting nonpersistent shared memory objects must be emulated by processes sharing memory, an additional complexity.

The memory mapping functions in POSIX.1 include the main memory allocation and deallocation functions, which are applicable only to the C programming language. POSIX.1 memory mapping functions cannot map pages of memory. No de jure or de facto standard Fortran binding for the POSIX.1b memory mapping is either approved or in progress.

POSIX.1b memory locking does not support "lock stacking," which makes it impractical to use locking transparently in library functions or opaque modules. POSIX.1b supports no specific interface for preallocating stack space and locking it down -- a common real time requirement that prevents page faults from allowing the stack to grow during real time operation. Many architectures support system-managed stacks that grow automatically when their current extent is exceeded. A real time application is required to be able to "preallocate" sufficient stack space and lock it down, so it will not suffer page fault to allow the stack to grow during critical real time operation.

3.8.4.4.4 Portability caveats. Although shared memory functionality is supported in POSIX.1b, and the SVID, the process is not quite the same. The shared memory facilities are the same across OSF, X/Open, and the SVID, but their shared memory semantics are different from POSIX.1b's. The POSIX.1b standard uses pathnames, while System V Unix uses a separate numeric name space for shared memory.

POSIX.1b specifies interfaces with designated separate commands to perform individual functions (e.g., separate commands to remove a shared memory segment, change the shared memory segment's access permissions, and change its owner). In contrast, the SVID tends to provide a single command for shared memory (e.g., "shmctl()") and use different variables and flags to indicate different functions.

POSIX.1b's process memory locking requires the behavior of the following POSIX.1 function calls to be modified to support the memory locking mechanisms: "exec()," "_exit()," "fork()," and "sysconf()."

Although POSIX.1b has adopted the SVID's "mlockall()" and "munlockall()" interfaces for process memory locking, POSIX.1b has extended the semantics of the SVID interfaces to ensure that the locked pages are resident when the locking functions return. This is not specified in the SVID. Besides "mlockall()," the SVID still supports the System V original "plock()" command because of the many existing applications using it. Applications using the "plock()" command for memory locking are not compatible with POSIX.1b's memory locking.

POSIX.1b process memory locking does not apply to POSIX.1b shared memory regions, and the "MEMLOCK_FUTURE" argument to "memlockall()" can be relied upon to cause new shared memory regions to be locked automatically.

POSIX.1b does not specify the SVID's "memcntl()" interfaces for memory locking control because the "memcntl()" function associates a multitude of functions with a single command, a practice POSIX.1b shuns.

The POSIX.1b interface can support extensions, such as mapping objects other than memory or files, more easily than the System V shared memory interface.

Only systems with hardware supporting protection of mapped data from certain classes of access can support the POSIX.1b Memory Protection option. POSIX.1b does not address how implementations that choose to implement memory objects directly would treat them with standard utilities such as "ls," on the grounds that utilities are not within the charter of the POSIX.1b standard.

POSIX.1b memory mapped I/O cannot be mapped literally into Fortran-77 in a portable way because POSIX.1b mem y mapped I/O implementations return a process' address by means of a pointer, and Fortran-77 does not support pointer data types. No POSIX.1b language binding to Fortran-77 exists to map the shared memory constructs in a standardized manner.

The POSIX.1b "mmap()" and "munmap()" definitions for mapping objects into process address spaces, and subsequently unmapping them, were adopted from SVR4, and the semantics of the POSIX.1b and SVR4 system calls are the same. The OSF Application Environment Specification (AES) contains a nearly identical interface. The "mmap()" and "munmap()" system calls are part of X/Open's "Single Unix Specification" (Spec. 1170).

The "mmap" and related interfaces in the OSF Application Environment Specification (AES) are trial-use interfaces and, therefore, subject to change, causing potential incompatibilities among applications written to the trial-use and changed interfaces. The history of "mmap()," which is printed in Draft 12 of the POSIX.1b standard, does an excellent job of pointing out some of the portability problems that users may run into with different specifications and implementations. Therefore, this history is reprinted here.

"Berkeley invented and documented, but never built, mmap(). Sun and Berkeley partially redesigned the mmap() interface, which Sun then implemented. SVR4 picked up the Sun mmap(). Meanwhile, Berkeley changed their minds about what some of the mmap() parameters should be; they changed the manual page; they didn't implement this either. Now enter POSIX.4, POSIX.4 essentially took SVR4's mmap(), called it "shmmap()," and added the new "default exact mapping" feature to it. They did this by overloading the address NULL to do something different. The problem with this is that zero is a valid address on many machines. This effectively precluded mapping memory at address zero. Furthermore, it has been recognized that this feature added no new semantic capabilities, and has since been dropped from POSIX.4 entirely. Meanwhile, enter OSF. The OSF originally picked up the SVID's mmap(), but added the old POSIX.4 NULL address treatment to "follow POSIX's lead." It is assumed they will now change the (trial use) AES mmap() definition to match the rest of existing practice. (Note: This change is particularly important for program loaders, which may need to map code or data at location zero.)"

Procurement specifications should require that a system not allow default exact mapping to a "NULL" address, because it may conflict with the ability to map memory to address zero.

3.8.4.4.5 Related standards. The following standards are related to memory management or memory management standards:

a. IEEE P1003.1a: POSIX - System API Extensions, Language Independent.
b. IEEE 1003.1e: Security Interface Standards for POSIX.
c. IEEE R1003.5:1992: ADA Language Binding for POSIX. (Being revised)
d. IEEE 1003.9:1992: Standard FORTRAN Language Bindings to POSIX.

3.8.4.4.6 Recommendations. ISO/IEC 9945-1:1996 is recommended. It incorporates IEEE 1003.1b which standardizes additional functions not in the 1990 version of 9945-1.

The following wording is recommended for use in specifying shared memory services:

"Systems offered as a result of the requirements of which this is a part shall provide shared memory capabilities conforming to the requirements, services, and interfaces specified in the IEEE 1003.1b standard which is incorporated in ISO 9945-1:1996, for all the features and functionality specified elsewhere in this document."

Most of the System V shared memory functionality can be emulated on top of the POSIX.1b interface. An example of how to do this is given in draft 12 of the P1003.1b standard.

Pointer problems also exist with shared memory in the SVID, SVR4, and XPG4. In these systems, shared memory control operations require the use of a pointer to the shared memory address space. This pointer operation must be mapped into the non-pointer oriented Fortran-77, and no portable mapping exists.

When a mapping is established, an implementation may need to map more than is requested into the process' address space because of hardware requirements. However, an application cannot and should not count on this behavior. Implementations not using a paged architecture simply may allocate a common memory region and return its address. Such implementations probably will not allocate any more than is necessary.

To use POSIX.1b memory mapped I/O with Fortran-77, choose one of the following alternatives. The first is to use the Fortran-77 binding in P1003.9. The second is to move to Fortran-90, which does support pointer data types, thereby making it easier to map POSIX.1b shared memory constructs to Fortran. The third alternative, particularly important for Fortran-77 legacy systems in the absence of a standardized binding mapping the shared memory constructs, is to make public the name of a COMMON, and then bind the name of the COMMON (make it equivalent) to a locally defined COMMON area. Such implementations probably will have to place restrictions on the size and alignment of such structures, or will have to map a suitable region of the process' address space into the memory object, and thus into other processes.

The following wording is recommended for specifying real time process memory locking:

"Real time systems offered as a result of the requirements of which this is a part shall provide memory locking capabilities conforming to the requirements, services, and interfaces specified in the IEEE 1003.1b standard which is incorporated in ISO 9945-1:1996."

The older "plock()" function for process memory locking can be implemented on top of the optional address range locking, provided the implementation has the means to locate the address space ranges corresponding to "text," "data," and "stack" segments. The plock() interface in not specified by XPG4 or the Single Unix Specification.

Although memory mapped I/O is a standard part of the SVID and OSF/1, it is an option in the recommended POSIX.1 standard. If procurements do not specify the IEEE P1003.1b Standard's Memory Mapped Files option, vendors may provide a POSIX.1b conformant system not including this option. In a procurement specification, require that a system not allow default exact mapping to a "NULL" address, because it may conflict with the ability to map memory to address zero.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.4.5 Asynchronous I/O. Asynchronous I/O standards provide the ability to overlap currently executing processes and I/O operations initiated by the application.

3.8.4.5.1 Standards. Table 3.8-34 presents standards for asynchronous I/O.

TABLE 3.8-34 Asynchronous I/O standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.4.5.2 Alternative specifications. For true asynchronous I/O, only proprietary products will suffice. For nonblocking I/O: System V's "poll() and terminal driver settings, Berkeley 4.3 Unix's "select()" and "[SIGIO]" features can be used. Both Berkeley's "select()" and System V's "poll()" are required by X/Open's Single Unix Specification (Spec. 1170).

3.8.4.5.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.8.4.5.4 Portability caveats. Mixing existing nonblocking I/O with the newer asynchronous I/O can cause portability problems.

The unwise use of signals with the POSIX.1b asynchronous I/O interfaces can cause a problem whose cause is difficult to determine, because the blocking function can return with a particular symbolic error number when another error caused the problem.

3.8.4.5.5 Related standards. The following standards are related to asynchronous I/O standards:

a. IEEE P1003.1e: Security Interface Standards for POSIX.
b. IEEE 1003.10:1995: POSIX - Supercomputing Applications.

3.8.4.5.6 Recommendations. The following wording is recommended for specifying real time asynchronous I/O:

"Real time systems offered as a result of the requirements of which this is a part shall provide asynchronous I/O capabilities conforming to the requirements, services, and interfaces specified in the IEEE 1003.1b standard which is incorporated in ISO/IEC 9945-1:1996."

System V's shared memory and semaphores may be used, albeit at high cost, to perform asynchronous I/O. Since the POSIX.1b asynchronous I/O supplements but does not replace the functions of the existing nonblocking interfaces available on most Unix systems, building the older Unix functions on the new POSIX asynchronous I/O function is not easy.

3.8.4.6 Asynchronous event notification. Asynchronous event notification is a facility that notifies a process of different types of events concerning it in a consistent and reliable manner.

3.8.4.6.1 Standards. Table 3.8-35 presents standards for asynchronous event notification.

TABLE 3.8-35 Asynchronous event notification standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
NPC	IEEE	POSIX Part 1: System API - Amendment 1: System API Extensions (C language)	POSIX.1c	Emerging (Draft)
QPC	NIST	POSIX Real Time Extensions	NIST FIPS (Status)	Informational (Transitive)

3.8.4.6.2 Alternative specifications. No other consortia or de facto specifications are available.

3.8.4.6.3 Standards deficiencies. The ISO/IEC 9945-1:1996 standard now includes POSIX.1b real time signals and supports many functions not in the 1990 version of 9945-1. These include reliable delivery of event notification, prioritized delivery of event notifications, and the differentiation among multiple signals of the same type.

Many people consider the POSIX.1b asynchronous event notification to be overly detailed and complex because it is implemented as part of the signals mechanism. Using a single signals mechanism to handle ordinary signals and asynchronous event notification requires system developers to deal with a large amount of complex signals flags, variables, and other details. Having one interface handle multiple functionalities is contrary to POSIX.1b's usual approach of defining a separate, clearly-understood interface for each functionality (e.g., one interface for signals and another one for asynchronous event notification). In this case opponents of the separate interface for each functionality approach argued that the separate interface approach would require the implementation and maintenance of interfaces with different names.

3.8.4.6.4 Portability caveats. If POSIX.1b real time signals providing reliable asynchronous event notification is integrated with the more common unreliable asynchronous event notification, system behavior cannot be guaranteed to be portable.

3.8.4.6.5 Related standards. The following standards are related to asynchronous event notification standards:

a. IEEE P1003.1e: Security Interface Standards for POSIX.

b. IEEE P1003.1g: Protocol Independent Interfaces.
c. OSF: Distributed Computing Environment (DCE).

3.8.4.6.6 Recommendations. ISO/IEC 9945-1:1996 which incorporates IEEE 1003.1b is recommended. Because reliable asynchronous event notification is such an important capability for real time, networking, distributed management, and transaction processing, procurements should specify the POSIX.1b Real Time Signals option; otherwise, vendors probably will not provide it.

3.8.4.7 Synchronized I/O. Synchronized I/O (also known as synchronous I/O) refers to the ability of a system to have transferred its data to nonvolatile media by the time the system signals completion.

3.8.4.7.1 Standards. Table 3.8-36 presents standards for synchronized I/O.

TABLE 3.8-36 Synchronized I/O standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, System Interface Definitions, Version 2, Issue 5	C605 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
NPC	IEEE	POSIX Part 1: System API - Amendment 1: System API [Extensions (C language)]	P1003.1a	Emerging (Draft)
CPC	NIST	POSIX Real Time Extensions	FIPS PUB (Future)	Informational (Formative)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Informational (Superseded)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec.	SVID Issue 4	Informational (Superseded)

3.8.4.7.2 Alternative specifications. The following specifications are also available:

a. Berkeley 4.2/4.3 Unix.
b. OSF: OSF/1 Application Environment Specification (AES) 1.1.

3.8.4.7.3 Standards deficiencies. Although the POSIX.1b "fsync()" function has been adapted from the emerging P1003.1a standard, the POSIX.1b specifiers and many balloters consider the loosely defined POSIX.1a "fsync()" function to be unacceptable for real time applications.

3.8.4.7.4 Portability caveats. The POSIX.1b Synchronized I/O interface is similar to but not exactly like the one described in the Single Unix Specification (Spec 1170). Berkeley Unix systems include an "fsync()" operation, which causes synchronization for file data and file attributes. The Berkeley Unix "fsync()" operation has been incorporated into Spec 1170; thus both the System V and Berkeley Unix styles of synchronous I/O are availa. . The POSIX.1b Synchronized I/O interface supports two levels of integrity for output operations, using an

"O_SYNC" and an "O_DSYNC" flag. The POSIX.1b "O_SYNC" flag is essentially the same as the "O_SYNC" flag described in the Spec 1170, so the "O_SYNC" flag of Spec 1170 and SVR4's "open()" system call maps directly onto the POSIX.1b "O_SYNC" flag. Subsequent output operations of "write()" will behave identically in System V and POSIX.1b. The POSIX.1b also has an "O_DSYNC" flag, which specifies a less stringent form of integrity.

The SVID does not impose synchronized I/O on input operations. The POSIX.1b Synchronized I/O facility extends the SVID's facility to include input operations.

POSIX.1a (the POSIX.1 revision) has defined an "fsync()" function abstractly to force a physical write of data from the buffer cache and synchronize a file's state. The POSIX.1b "fsync()" function is more specifically and rigorously defined to meet real time application requirements. The behavior of the more rigorous POSIX.1b "fsync() function cannot be counted on to be portable to the less rigorous POSIX.1a "fsync()" function.

Not all file systems may support or need to support synchronized I/O. Consequently, when synchronized I/O is specified on the "open()" or "fcntl()" functions, the function may fail due to the fact that the file system cannot support synchronized I/O for the specified file.

The operating system cannot protect users from themselves if they bypass the operating system's protection mechanism and use raw I/O (directly address the I/O device). Although users may provide their own mechanisms for ensuring data and file integrity if they use raw I/O, neither the protection mechanisms nor the raw I/O can be counted on to be portable to any other platform.

3.8.4.7.5 Related standards. The following standard is related to synchronized I/O standards:

a. IEEE P1003.1e: Security Interface Standards for POSIX.

3.8.4.7.6 Recommendations. ISO/IEC 9945-1:1996 which incorporates IEEE 1003.1b is recommended. Procurements involving programs requiring a file to be in a known state, for example, procurements for transaction facilities, should use the more rigorous POSIX.1b "fsync()" functions to ensure that all modifications to a file or files caused by a transaction are recorded.

If the less rigorous POSIX.1a synchronized I/O facility is used, look to the conformance document to specify what behavior can be expected from the system. If procurements do not specify the POSIX.1b Synchronized I/O option, vendors probably will provide either a different and nonportable synchronized (synchronous) I/O facility, or they may provide a POSIX.1b conformant system not including this option.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.4.8 Real time file system. A real time file system is a high-performance file system (e.g., contiguous I/O or preallocated I/O) that optimizes data storage on a disk to minimize the disk access time when retrieving or writing data on the disk. Real time files refer to the ability to specify various characteristics regarding how normal file requests, such as "read()" and "write()," are handled. File management functions include create, get and set attributes, get cache and buffer capabilities, and allocate and release data buffers. Real time files are associated most commonly with contiguous files and preallocated files minimizing disk access time when reading or writing data on a disk.

3.8.4.8.1 Standards. Table 3.8-37 presents standards for real time file systems.

TABLE 3.8-37 Real time file system standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
NPC	IEEE	POSIX Part 1: System API - Amendment 1: System API Extension (C language)	P1003.1b	Emerging (Draft)
GPC	NIST	POSIX Real Time Extensions	FIPS PUB (future)	Informational (Formative)

3.8.4.8.2 Alternative specifications. No other consortia or de facto specifications are available.

3.8.4.8.3 Standards deficiencies. Data are not guaranteed to be delivered to the underlying storage media. This issue should have been discussed in Section 6.6 of the POSIX.1b standard.

POSIX.1b lacks an interface that allows the specification of bounded performance. POSIX.1b does not address files of a fixed size whose contents are written in a circular fashion. For example, after reaching the file's size limit, subsequent "write()" functions would overwrite the beginning of the file. Such a capability is needed primarily for logging types of operations.

POSIX.1b lacks a specification for a real time file system, such as contiguous files or preallocated files, which are needed for most real time applications. A generic real time file specification was included in Draft 12 of the standard, but was dropped subsequently due to controversy. The group is working on real time files for the POSIX.1b revision.

3.8.4.8.4 Portability caveats. Real time files are associated most commonly with contiguous files and preallocated files that minimize disk access time when reading and writing data on a disk. POSIX.1b supports attributes for contiguous files, preallocated files, direct I/O, cache usage,

sequential access, aligned transfers, and the transfer granularity. Thus, it is possible to have two applications compliant with POSIX.1b with incompatible file systems.

The requirements for real time file usage differed in the areas of performance, guaranteed access to resources, and guaranteed delivery of data to a nonvolatile media (not memory). These differences influence the underlying behavior of existing interfaces. Application developers typically employ "tricks" to achieve a higher level of performance than a system delivers through the normal interface. This behavior is not portable.

One of the areas of common practice with the greatest variation between vendors and the greatest resulting incompatibility is the persistence of file attributes. The POSIX.1b standard does not alleviate this problem. POSIX.1b requires persistence of file attributes on an open instance basis. It allows, but does not require, more persistent implementations. This specification does not require vendors to change their existing systems to ensure multivendor compatibility.

3.8.4.8.5 Related standards. The following standard is related to real time file system standards:

a. IEEE P1003.1e: Security Interface Standards for POSIX.

3.8.4.8.6 Recommendations. If capabilities are needed to address fixed size files written in a circular fashion, procurements should require such a facility to be implemented as library functions using functions defined in ISO/IEC 9945-1:1996 which incorporates IEEE 1003.1b:1993.

If procurements do not specify the POSIX.1b Real-Time Files option, the recommended standard, vendors may not provide it.

Currently, nothing can be done about the nonportability of performance behavior except wait. Because the POSIX.1b specifiers have found that many of the techniques for achieving bounded levels of performance are common to many implementations, they may be able to standardize an interface to these techniques.

The POSIX.1b real time files interface uses constant names prefixed with ATC_ or ATB_, and structure members prefixed with either atc_ or atb_. Applications should avoid using identifiers of this form to preclude name conflicts with the standard.

3.8.4.9 Embedded real time. Embedded real time capabilities provide services to support embedded real time applications with demanding determinism and response times. An embedded system is a specialized computer used to control a device. It implies software that integrates operating system and application functions.

3.8.4.9.1 Standards. Table 3.8-38 presents standards for embedded real time.

TABLE 3.8-38 Embedded real time standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.4.9.2 Alternative specifications. The following specifications are also available:

a. Proprietary real time Unix systems.
b. Proprietary real time executives.
c. "Home grown" real time kernels.
d. Future: Mach microkernel with real time extensions.

3.8.4.9.3 Standards deficiencies. The P1003.13 standardized profile for embedded real time applications contains too many high overhead POSIX.1 operations (e.g., "fork()"). To meet the response time and real estate requirements of embedded real time applications, the P1003.13 Group must be allowed to subset POSIX.1 as well as POSIX.1b. However, IEEE and ISO rules do not allow the subsetting of a base standard. Until this problem is solved, a practical embedded real time POSIX standard cannot exist.

3.8.4.9.4 Portability caveats. If software companies producing real time operating systems choose different functionalities from POSIX.1b, which is possible because each functionality is an option, portability will be reduced.
If software companies producing real time operating systems eliminate different high-overhead parts of POSIX.1 to meet demanding determinism and response time requirements and implement their own nonstandard functions to replace those eliminated from POSIX.1, their POSIX.1b- or POSIX.13-conformant operating systems will be different. They also will not support portable real time applications across other vendors' POSIX.1b- or POSIX.13-conformant systems.

3.8.4.9.5 Related standards. The following standard is related to embedded real time standards:

a. ISO/IEC 9945-1:1996: POSIX Part 1: System Application Programming Interface (Includes Realtime and Threads Amendments).

b. IEEE P1003.1e: Security Interface Standards for POSIX.

3.8.4.9.6 Recommendations. This problem needs to be resolved. Broad-based, active participation is needed to force a decision allowing the subsetting of a base standard such as POSIX.1 in a standardized way for special purposes.

3.8.4.10 Symbolic real time debugging aids. Symbolic real time debugging aids refer to a variety of real time specific development and debugging tools. A debugger lets you stop the program at a specified statement, step through it one statement at a time, as well as capture and view system data and program variables. Modern debuggers link source and object code so that the programmer can step through the source program while instructions are being executed.

3.8.4.10.1 Standards. Table 3.8-39 presents standards for symbolic real time debugging aids.

TABLE 3.8-39 Symbolic real time debugging aids standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
N.A.	N.A.	None	N.A.	- (N.A.)

3.8.4.10.2 Alternative specifications. The only other available specifications are proprietary (e.g., Harris Computer, Encore Computer, Concurrent Computer, Modcomp, Wind River Systems, Silicon Graphics, Hewlett-Packard, Sun Microsystems, Digital Equipment Corp.)

3.8.4.10.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.8.4.10.4 Portability caveats. This is a high portability risk area because no standards exist.

3.8.4.10.5 Related standards. The following standards are related to symbolic real time debugging aids:

a. NIST: ISEE.

b. European Computer Manufacturers' Association (ECMA): Portable Common Tools Environment (PCTE).

3.8.4.10.6 Recommendations. No standards are available to recommend.

3.8.4.11 Real time POSIX.1b language bindings. These standards provide a language interface to the POSIX.1b real time standard.

3.8.4.11.1 Standards. Table 3.8-40 presents standards for real time POSIX.1b language bindings.

TABLE 3.8-40 Real time POSIX.1b language bindings standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
NPC	IEEE	POSIX Ada Language Interfaces - Part 1:Binding for Realtime Extensions	1003.5b:1996 (former 1003.20)	Informational (Approved)
NPC	IEEE	Test Methods for Measuring Conformance to POSIX - System Interfaces	2003.1:1992	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.4.11.2 Alternative specifications. There are no alternative specifications available.

3.8.4.11.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.8.4.11.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.8.4.11.5 Related standards. There are no related standards.

3.8.4.11.6 Recommendations. ISO/IEC 9945-1:1996 which incorporates the 1003.1b Realtime amendment is recommended.

3.8.5 Operating system security. Security services present standards, guidelines, models, frameworks, and other documents related to the control and validation of information in an open system. Security services can be placed at various layers within the OSI architecture. The selection of the appropriate layers to place security services within a system depends upon the architecture and functional requirements.Therefore, the system architecture and functional requirements will influence the selection of standards within a subservice area. The selection of subservice areas depends on the selected architecture and required functionality. DOD policy covering the accreditation process must be adhered to to obtain approval to process classified data.

3.8.5.1 Operating system security. (This BSA appears in both part 8 and part 10.) Operating system security services provide basic reference monitor services. These security mechanisms control the flow of data and use of applications to ensure the system security policy is adhered to.

3.8.5.1.1 Standards. Table 3.8-41 presents standards for operating system security.

TABLE 3.8-41 Operating system security standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	NIST	Password Usage	FIPS PUB 112: 1985	Mandated (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Guidelines on Evaluation of Techniques for Automated Personal Identification	FIPS PUB 48:1977	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 7: Security Alarm Reporting Function (same as ITU-T X.736)	10164-7:1992	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment n: Protection, Audit, and Control Interfaces (C Language), Draft 15	P1003.1e: 1995	Emerging (Draft)
NPC	IEEE	POSIX Part 2: Shell and Utilities - Amendment n: Protection and Control Utilities, Draft 15	P1003.2c: 1995	Emerging (Draft)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
NPC	IEEE	Guide to the POSIX Open Systems Environment - A Security Framework	P1003.22: 1995	Informational (Draft)
NPC	SAE	Avionics Operating System API Requirements for the Society of Automotive Engineers	ARD 50067: 1996	Informational (Draft)
NPC	IEEE	Portable Operating System (POSIX), Part 1: System API/C Language (same as ISO 9945-1:1990)	1003.1:1990	Informational (Superseded)

3.8.5.1.2 Alternate specifications. No alternative specifications are available.

3.8.5.1.3 Standards deficiencies. General operating systems for personal computers are inherently insecure and should not be used in DOD acquisitions without an assurance of "add-on"

security features and an approved security risk analysis providing at least a C2 level of trust per DOD Directive 5200.28.

The DGSA stresses the need for separation mechanisms, such as a separation kernel, to maintain strict isolation, that is, information domains must be completely isolated from each other. The DGSA concept requires that information transfers between domains may occur if, and only if, a relationship is explicitly defined in each information domain's security policy. There are no current or emerging standards for design and implementation of separation kernels nor for programming interfaces for separation kernels.

Due to its age, FIPS 48 does not include information on modern security concepts.

3.8.5.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.8.5.1.5 Related standards. ISO/IEC 9945-1 as profiled by FIPS 151-2 is related to IEEE P1003.1e and IEEE P1003.2c.

The following Compartmented Mode Workstation (CMW) specifications are related to operating system security:

a. DDS-2600-5502-87, Security Requirements for System High and Compartmented Mode Workstations

b. DDS-2600-6243-92, Compartmented Mode Workstation (CMW) Evaluation Criteria

c. DDS-2600-6216-91, Compartmented Mode Workstation (CMW) Labeling: Encoding Format

d. DDS-2600-6243-91, Compartmented Mode Workstation (CMW) Labeling: Source Code and User Interface Guidelines, Revision 1

3.8.5.1.6 Recommendations. The mandated standards are recommended.

3.8.5.2 Electronic hashing. (This BSA appears in part 5, part 7, part 8, and part 10.) Electronic hashing services compute a condensed representation of a message or a data file, often used as a measure of data integrity checking.

3.8.5.2.1 Standards. Table 3.8-42 presents standards for electronic hashing.

TABLE 3.8-42 Electronic hashing standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180-1:1995	Mandated (Approved)
IPC	ISO	Hash Functions, Part 1: General Model	10118-1:1994	Informational (Approved)
IPC	ISO	Hash Functions, Part 2: Hash Functions Using an N-Bit Block Cipher Algorithm	10118-2:1994	Informational (Approved)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180:1993	Informational (Superseded)
IPC	ISO	Hash Functions, Part 3: Dedicated Hash Functions	WD 10118-3 JTC1/SC27 N993 (Project 1.27.09.03)	Informational (Draft)
IPC	ISO	Hash Functions, Part 4: Hash Functions Using Modular Arithmetic	WD 10118-4 JTC1/SC27 N994 (Project 1.27.09.04)	Informational (Draft)

3.8.5.2.2 Alternate specifications. There are no alternative specifications.

3.8.5.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.8.5.2.4 Portability caveats. Portability problems with the existing specifications are unknown.

3.8.5.2.5 Related standards. FIPS PUB 180-1 supersedes FIPS PUB 180 and is required for use with FIPS PUB 186, Digital Signature Standard.

3.8.5.2.6 Recommendations. The mandated standard is recommended. FIPS PUB 180-1 specifies SHA, which can be used to generate a message digest. SHA is required for use with the DSA as specified in FIPS PUB 186 and whenever an SHA is required for federal applications.

3.8.5.3 Entity authentication. (This BSA appears in part 8, part 9, part 10, and part 11.) Entity authentication standards address data, processes, systems, and enterprises.

3.8.5.3.1 Standards. Table 3.8-43 presents standards for entity authentication.

TABLE 3.8-43 Entity authentication standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
GPC	NIST	Computer Data Authentication	FIPS PUB 113:1985	Informational (Approved)
GPC	NIST	Entity Authentication Using Public Key Cryptography	FIPS PUB 196:1996	Emerging (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO	Financial Transactions - Retail Banking Security Requirements for Message Authentication	9807	Informational (Approved)
IPC	ISO	Entity Authentication Mechanisms - Part 1: General Model	9798-1:1991	Informational (Approved)
IPC	ISO	Entity Authentication Mechanisms - Part 3: Entity Authentication Using a Public Key Algorithm	9798-3:1993	Informational (Approved)
GPC	NIST	Guideline for Use of Advanced Authentication Technology Alternatives	FIPS PUB 190:1994	Informational (Approved)
IPC	ISO	Entity Authentication - Part 2: Mechanisms Using Symmetric Encipherment Algorithms	9798-2:1994	Informational (Approved)
IPC	ISO	Entity Authentication - Part 4: Mechanisms Using a Cryptographic Check Function	9798-4:1995	Informational (Approved)
CPC	X/Open	Security Interface Specification: Auditing and Authentication	S020: 1990	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
CPC	IETF	The Kerberos Network Authentication Service (V5)	RFC 1510:1993	Informational (Draft)
IPC	ISO	Entity Authentication Mechanisms - Part 5: Entity Authentication Using Zero Knowledge Techniques	9798-5:1995	Informational (Draft)

3.8.5.3.2 Alternate specifications. There are no alternative specifications.

3.8.5.3.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.8.5.3.4 Portability caveats. OSF DCE Version 1.1's authentication service is based on Kerberos Version 5 (RFC 1510), but is not totally compatible with RFC 1510. DCE 1.2.2 adds testing and official support for Kerberos Version 5.

3.8.5.3.5 Related standards. The following standards are related to entity authentication:

a. DOD NCSC-TG-017, Version 1, September 1991, Guide to Understanding Identification and Authentication in Trusted Systems.

b. FIPS PUB 196, 11 October 1996.

FIPS PUB 196 becomes effective 6 April 1996. It is based on ISO/IEC 9798-3:1993 and specifies two challenge-response protocols by which entities in a computer system may authenticate their identities to one another. FIPS PUB 196 is for use in public key based challenge-response and authentication systems at the application layer within computer and digital telecommunications systems.

3.8.5.3.6 Recommendations. The mandated standards are recommended.

3.8.5.4 Security management. (This BSA appears in part 7, part 8, part 9, and part 10.) Security management is a particular instance of information system management. Security management provides supporting services that contribute to the protection of information and resources in open systems in accordance with information domain and information security policies. The basic elements that must be managed are users, security policies, information, information processing systems that support one or more security policies, and the security functions that support the security mechanisms (automated, physical, personnel, or procedural) used to implement security services. For each of these elements, the managed objects that constitute them must be identified and maintained. For example, users must be known and rec[illegible], security policies must be represented and maintained and information objects must be iden[illegible] and maintained. Security policies, security services and security mechanisms are the first classes of managed objects.

3.8.5.4.1 Standards. Table 3.8-44 presents standards for security management.

TABLE 3.8-44 Security management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Network Interpretation	NCSC-TG-005, Version 1: 1987	Mandated (Approved)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
IPC	ITU-T	The Directory: Procedures for Distributed Operation (X-ref: ISO 9594-4)	X.518: 1993	Informational (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) - Part 1: Specification (Includes amendment 1 and 2 of ISO/IEC 9596-1:1990)	9596-1:1991	Informational (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 7: Security Alarm Reporting Function (same as ITU-T X.736)	10164-7:1992	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 8: Security Audit Trail Function (same as ITU-T X.740)	10164-8:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 9: Objects and Attributes for Access Control	10164-9:1995	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.5.4.2 Alternate specifications. There are no alternative specifications.

3.8.5.4.3 Standards deficiencies. Deficiencies exist in standardization of security policy rule representation; key management, including generation, distribution, and accounting; audit information formats; exchange of security management information; and remote security management.

The DGSA principle of decision and enforcement separation requires that the functions determining how to enforce a security policy and the actual enforcement of the policy be implemented independently. That is, the enforcement mechanisms do not need any knowledge of security policy. Standards are needed for object class definitions for classes of managed objects and for methods of representing security policy.

The DGSA calls for a separation mechanism, such as separation kernel, to mediate all calls to security critical functions to ensure that strict isolation is maintained. Standardization of object class definitions for management of critical functions used within the separation kernel is needed.

The present ISO/IEC 10164-7 "Security Alarm Reporting Function," and 10164-8, "Security Audit Trail Function," standards were designed with network security in mind. Little work has been done, either in standards groups or in products, on how to use these standards for general system management (e.g., computer systems and software).

FIPS PUB 179-1 supersedes FIPS PUB 179. The present GNMP specifications require ISO CMIS/CMIP to communicate management information and ISO OSI networking protocols. Plans are for the GNMP eventually to provide a capability to integrate the present GNMP with SNMP. One reason for this goal is the widespread use of SNMP.

No Ada bindings exist for any of the ISO or consortia system management specifications.

The IEEE POSIX Security Working Group (formerly P1003.6) is defining security extensions to the base POSIX interface standard (ISO 9945-1), to include support for audit, privilege, discretionary and mandatory access control, and information labels. These have been redesignated IEEE P1003.1e and IEEE P1003.2c. The draft standards are still incomplete, and the specifications may change.

The POSIX/Unix permission bits are inadequate for fine-grained control over exactly which users can perform specified actions to particular files.

In the IETF, efforts to develop an acceptable security standard for SNMPv2 have been on hold since September 1995 when the IETF SNMP Working Group failed to agree on the proposals submitted. Since then, two sets of proposals for providing SNMPv2 security have emerged. The first set of proposed specifications, the User-based Security Model (USEC), also referred to as SNMPv2u, consists of two documents: RFC 1909, "An Administrative Infrastructure for SNMPv2" and RFC 1910, "The User-based Security Model for SNMPv2." Both RFCs were issued 28 February 1996 and are classified by the IETF as experimental RFCs. The other proposal is known as SNMPv2*, which its proponents claim is heavily based on USEC. Neither USEC nor SNMPv2* has been approved for a standards track by IETF.

3.8.5.4.4 Portability caveats. The structure of certain traditional UNIX directories, such as the familiar "/tmp," "/usr/spool," and "/usr/spool/mail" directories will have to change to accommodate the P1003.1e and P1003.2c security standards. This is because these are directories to which all users have access and to which many programs write. A change in the way programs write to directories has the potential for causing software portability and systems administrator portability problems.

The traditional UNIX permission bits that have been carried into POSIX are inadequate for defining exactly which user can perform specific actions on specific files. Eliminating the permission bits in favor of Access Control Lists could make the secure POSIX systems incompatible with non-POSIX compliant systems and many applications.

OSF DCE Version 1.1's authentication service is based on Kerberos Version 5 (RFC 1510), but is not totally compatible with RFC 1510. DCE 1.2.2 adds testing and official support for Kerberos Version 5.

3.8.5.4.5 Related standards. ISO/IEC 9945-1 as profiled by FIPS PUB 151-2 is related to IEEE P1003.1e and IEEE P1003.2c.

3.8.5.4.6 Recommendations. The mandated standards are recommended.

All IEEE P1003.1e and IEEE P1003.2c security systems should incorporate Access Control Lists as an optional feature in addition to permission bits (not "in place of" permission bits). The incompatibilities between the two access control methods (permission bits and access control

lists) are not resolvable. The best method for resolving the overall problems seem to be incorporation Access Control Lists as an optional feature on top of permission bits. The permission bits would represent the lowest common denominator of security, showing the maximum amount of openness possible in a system. Organizations needing only the lowest level of security could continue to use the familiar permission bits and associated "chmod" command. Use of access control lists will require a change in security policy such that access is granted if and only if permission is granted and access control permits it.

3.8.5.5 Operating system security labeling. (The BSA appears in part 8 and part 10.) Operating system security labeling provides a security labeling service in support of end system processing. This service is required to support similar or shared service for all other MSAs having security labels. This service includes any translation services to support other MSAs, achieve host system independence, or protect host identity.

3.8.5.5.1 Standards. Table 3.8-45 presents standards for operating system security labeling.

TABLE 3.8-45 Operating system security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.5.5.2 Alternate specifications. There are no alternative specifications.

3.8.5.5.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.8.5.5.4 Portability caveats. Portability problems with the existing standards are unknown.

3.8.5.5.5 Related standards. DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

3.8.5.5.6 Recommendations. The mandated standard is recommended.

3.8.6 Distributed system services. Distributed system management services allow systems and/or enterprises to be managed from any node in the enterprise. In some cases an enterprise may be managed as a single unit, but management tasks can be performed at any node. In other cases, the enterprise may be split into multiple domains, each having its own management system, but the different management systems can cooperate with each other and exchange and use each others' management information.

3.8.6.1 Distributed file services. (This BSA appears in part 8 and part 11.) Distributed file services (DFS) is a distributed client/server application, built on the underlying DCE services. It takes full advantage of the lower-level DCE services (such as RPC, Security, Threads, and Directory) and the distributed computing system. DFS provides many advantages over centralized systems. It provides a higher availability of data and resources, the ability to share information throughout a very large heterogeneous system, and efficient use of special computing functionality. Files are made highly available through replication, or caching, making it possible to access a copy of a file even when one of the machines on which a file is stored goes down. Further, users are able to work with unfamiliar file systems without having to know the unique commands for each system.

File Transfer, Access, and Management (FTAM) allows for the effective transfer, access, and management of different file types on remote systems by creating a virtual filestore that emulates the file services offered by existing file service systems.

Remote file access is the ability to access and/or change a file type or content at a location other than the user's. Remote file access is associated with distributed processing/client-server architectures, and is not used in host-terminal architectures.

3.8.6.1.1 Standards. Table 3.8-46 presents standards for distributed file services.

TABLE 3.8-46 Distributed file services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Distributed File Service (DFS)	DCE 1.1 DFS:1994	Mandated (Approved)
GPC	DOD	DoD Standardized Profiles - File Transfer, Access and Management (FTAM) - Parts 1,4, and 5 (References ISO 8571 parts 1-5)	MIL-STD-2045-17508 - Parts 1,4, and 5: 7/94	Informational (Approved)
CPC	X/Open	Protocols for X/Open PC Interworking: SMB, Version 2	C209 (10/92)	Informational (Approved)
CPC	X/Open	Protocols for X/Open Interworking: XNFS, Issue 4	C218 (10/92)	Informational (Approved)
NPC	IEEE	OSI API - File Transfer, Access, and Management (FTAM) (C Language)	1238.1:1994	Informational (Approved)
NPC	IEEE	POSIX, Part 1: Network-Transparent File Access	P1003.1f	Emerging (Draft)
CPC	IETF	NFS: Network File System Protocol Specification	RFC 1094:1989	Informational (Not Recommended)

3.8.6.1.2 Alternative specifications. The only other available specifications are proprietary.

3.8.6.1.3 Standards deficiencies. Limited-Purpose File Transfer, Access and Management (FTAM) subsets do not provide file access capabilities. Only Full-Purpose FTAM subsets provide such capabilities. Limited-Purpose FTAM subsets cannot interoperate fully with Full-Purpose FTAM subsets.

IEEE Transparent File Access (TFA) addresses the POSIX.1 refinements needed for file access, but ignores the behavior of other facilities needed for file access between nodes, such as signals.

The Remote File System (RFS) is associated mostly with Unix-based systems rather than with heterogeneous operating systems on legacy systems as the Network File System (NFS) is.

NFS security uses the not very secure traditional Unix authentication and permissions. Secure NFS is not as secure as it could be because it ships security information around the network.

Although the Andrew File System (AFS) can provide good networked performance because it supports client caching, this requires large amounts of memory and disk buffer space, as well as a potentially long time for the first remotely accessed data to be downloaded.

3.8.6.1.4 Portability caveats. The SVID provides facilities for getting file system information about a mounted file system, but none of the SVID functions ("statvfs()," "sftatvfs()," and "ustat()") are compatible with OSF/1's comparable functions ("statfs()," "fstatfs()," and "ustat()"). X/Open specifies enhancements to the "popen" and "pclose" system calls.

Because TFA does not go beyond the POSIX.1 refinements needed for file access and address the behavior of other facilities (e.g., signals) between nodes, a portability risk exists in using TFA between nodes. The TFA has two specifications, full TFA (which provides all of the file access services specified in ISO 9945-1) and Subset TFA (which defines file access semantics, which are less stringent than POSIX requires. Subset TFA also is designed for use with non-P1003.1 file systems. Consequently, it is possible to have two systems compliant with TFA, which are not compatible with each other, and which also may not be totally compatible with the core POSIX.1 file system.

The AFS is a superset of NFS, and IEEE TFA is a superset of AFS and NFS. Thus, a little backward compatibility exists between TFA and AFS and between AFS and NFS.

Systems using different FTAM subsets cannot be assured of portable applications or interoperability.

3.8.6.1.5 Related standards. The following standards are related to distributed files or distributed file standards:

a. ISO 9945-1:1996: (POSIX.1) System Interfaces.
b. IEEE 1224:1993: OSI Abstract Data Manipulation - API.

c. IEEE P1351: Association Control Service Element (ACSE) API.
d. RFC 1057: ONC Remote Procedure Call (RPC).
e. OSF:DCE RPC.

3.8.6.1.6 Recommendations. The OSF Distributed Computing Environment (DCE) Distributed File System is recommended for distributed computing environments based on TCP/IP.

MIL-STD-2045-17508 is recommended for legacy systems interoperability. Parts 1, 3, and 6 of the MIL-STD support only the Limited-Purpose FTAM (simple file transfer and management) system. This system does not provide file access capabilities. The MIL-STD-2045-17508, parts 4 and 5 support Full-Purpose FTAM (Positional file transfer, simple file access, and management)) system. Users requiring remote file access capabilities, based on OSI standards, should use parts 1, 4, and 5 of the MIL-STD.

An API to FTAM is provided by IEEE 1238.1.

3.8.6.2 Remote login. (This BSA appears in part 8 and part 11.) Remote login is the ability of a user from a local machine to be an authorized user and access a remote machine.

3.8.6.2.1 Standards. Table 3.8-47 presents standards for remote login.

TABLE 3.8-47 Remote login standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	TELNET Protocol	Standard 8/RFC-854/RFC-855	Mandated (Approved)
IPC	IAB	Host Requirements	Standard 3/RFC-1122/RFC-1123	Mandated (Approved)
IPC	ISO	Open Systems Interconnection-Protocol Specification for the Association Control Service Element (ACSE)	8650:1988	Informational (Approved)
GPC	DOD	DoD Standardized Profile - Internet Remote Login Profile for DoD Communications (References IAB Std 8 (RFC 854 and RFC 855 - Telnet Protocol:1983) and IAB Std 3 (RFC 1123 - Requirements for Internet hosts:1989))	MIL-STD-2045-17506:7/94	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Virtual Terminal Basic Class Protocol	9041:1990	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Basic Connection Oriented Presentation Service Definition	8822:1988	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Connection-Oriented Presentation Protocol	8823:1988	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Connection-Oriented Session Protocol	8327:1987	Informational (Approved)

3.8.6.2.2 Alternative specifications. None

3.8.6.2.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.8.6.2.4 Portability caveats. A procurement may specify Simple Systems or Forms-Capable Systems or both. However, the two systems cannot interoperate, and applications are not portable from one system to another. Each system is distinguished by the VT profile it supports: a Simple System supports the TELNET profile, and a Forms-Capable System supports the Forms profile. The Basic Class VT protocol is required in all cases; it operates independently of the Simple or Forms-Capable Systems.

3.8.6.2.5 Related standards. None

3.8.6.2.6 Recommendations. All new systems and systems undergoing major upgrades should use the Internet Architecture Board (IAB) STD 8 (RFC 854 and 855) and IAB STD 3 (RFC 1123). Those persons conducting procurements that involve IAB standards should review the latest version of the IAB official protocol standards list to ensure that the appropriate RFCs are specified.

The OSI Virtual Terminal (VT) standard is recommended for legacy systems interoperability. A clear migration path to page, scroll, graphics, and mixed mode virtual terminal profiles that are being defined by the OSE Implementors' Workshop (OIW)/NIST should be required. Otherwise, systems capable of employing only TELNET and Forms will not interoperate with future VT systems. The "rlogin" facilities are delivered with Berkeley BSD-based UNIX operating systems. Those facilities are not in the System V Interface Definition (SVID).

Currently, a Simple VT and a Forms-Capable VT exist. Few vendors have implemented a simple version of VT. Procurements need to determine if Simple or Forms-Capable VT Systems are sufficient for the application. No tests have been developed for VT to test conformance. Remote login is associated with distributed processing/client-server architectures. It is not used in host-terminal architectures.

No standards exist for VT API. A procurement for a VT final system must include a vendor's offering of virtual terminal API. This API should accommodate as many VT types as possible.

3.8.6.3 Remote shell execution. Remote shell execution services are facilities to execute an operating system shell remotely.

3.8.6.3.1 Standards. Table 3.8-48 presents standards for remote shell execution.

TABLE 3.8-48 Remote shell execution standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPN-C	Berkeley	Berkeley rsh/rshl	Berkeley Unix-TCP/IP	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.6.3.2 Alternative specifications. Alternatives include any implementation of Berkeley Unix with the Transmission Control Protocol/Internet Protocol (TCP/IP) and OSF/1's "rsh" and "rshl" functions.

3.8.6.3.3 Standards deficiencies. IEEE 1003.2 does not include "rsh/rshl."

3.8.6.3.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.8.6.3.5 Related standards. No standards are related to remote shell execution standards.

3.8.6.3.6 Recommendations. The only standards available are consortia and de facto specifications; they are equally attractive options. Selection may be based on the use of other specifications from the same source.

The "rsh/rshl" is one of the "remote" commands (often called the "r" commands) developed for Berkeley Unix 4.2. The "r" commands are not specified by any consortia specification and have been removed from X/Open products.

3.8.6.4 Remote procedure call. (This BSA appears in part 8 and part 11.) Remote procedure call (RPC) is a communication service to transfer procedure calls to a remote server and return results, errors, or associated call backs (ECMA 127). The RPC extends the local procedure call to a distributed environment. In a RPC, a process can invoke a remote procedure as if it were invoking a local procedure. SC21/WG6 proposes to address RPC using Interface Definition Notation (IDN) that is based on abstract data types rather than on a union of programming language-specific data types.

3.8.6.4.1 Standards. Table 3.8-49 presents standards for remote procedure call.

TABLE 3.8-49 Remote procedure call standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Remote Procedure Call (RPC)	DCE 1.1 RPC:1994	Mandated (Approved)
CPC	X/Open	X/Open DCE: Remote Procedure Call	C309 (8/94)	Informational (Approved)
CPC	IETF	Open Network Computing (SUN ONC) Remote Procedure Call (RPC)	RFC 1057:1988	Informational (Approved)
RPC	ISO	OSI Remote Procedure Call (RPC) Protocol DIS 11578 PT 1, Then PT 0	11578.2	Informational (Draft)
RPC	IEEE	POSIX - Part 1: Protocol Independent Interfaces	P1003.1g	Emerging (Draft)
RPC	IEEE	POSIX - Part 1: System API Amendment: Real Time Distributed Systems Communications	P1003.21	Emerging (Draft)

3.8.6.4.2 Alternative specifications. There are no alternative specifications.

3.8.6.4.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.8.6.4.4 Portability caveats. All the indicated RPCs are unique. They do not interoperate. Systems using different RPCs are not interoperable, nor are their applications portable across different RPCs. No RPC conformance tests are available.

3.8.6.4.5 Related standards. The following standards are related to RPC:

a. Common Language Independent Data Types (CLID) (ISO 11404).

b. Common Language Independent Procedure Call Mechanism (CLIP or CLIPCM). SC22/WG11 has recommended that there should be a cross reference between the standards.

c. NIST FIPS 146-1:1991: Government Open Systems Interconnection Profile (GOSIP), ISO 8822, ISO 8823 (SIA-5.8) Presentation (Layer 6), Session (Layer 5) ISO 8327 (SIA-5.9).

d. NIST FIPS 146-2 POSIT: May 1995.

3.8.6.4.6 Recommendations. The Open Software Foundation (OSF) Distributed Computing Environment (DCE) is recommended. A migration path to the ISO RPC also should be required as soon as that standard is in final form.

The IEEE P1003.21 draft standard includes interfaces for the support of request/response services.

3.8.6.5 Protocol-independent transport service. This defines a protocol-independent application interface to enable one process to communicate with another local or remote process over a network.

3.8.6.5.1 Standards. Table 3.8-50 presents standards for protocol-independent transport service.

TABLE 3.8-50 Protocol-independent transport service standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Single UNIX Specification, Networking Services, Version 2, Issue 5	C523 (2/97)	Emerging (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.6.5.2 Alternative specifications. The following specification is available:

a. SAE ARD 50067 Draft: Avionics Operating System API Requirements.

3.8.6.5.3 Standards deficiencies. The IEEE P1003.1g draft standard is an API for process-to-process communications, utilizing the X/Open Transport Interface (XTI) or the Berkeley Sockets interface. Although IEEE P1003.1g will be sufficient for many application domains, the standard does not address many of the functions required by many real-time applications. Among these are multicast services, heterogeneous communication, message priorities, typed messages, lightweight directory services, explicit buffer management, asynchronous interactions, bounded blocking, and event management, all of which are addressed in the IEEE P1003.21 standard.

3.8.6.5.4 Portability caveats. IEEE P1003.1g addresses two existing interfaces: the X/Open Transport Interface (XTI) and the Berkeley Sockets interface. In order to maintain the portability of existing applications in XTI and Sockets, both interfaces are required to be supported in any conformant implementation. In addition, IEEE P1003.1g is limited to transport protocols that are compatible with XTI and Sockets. The IEEE P1003.21 draft standard includes mappings to additional protocols, including XTP and SCI.

3.8.6.5.5 Related standards. The following standards are related to protocol-independent service standards:

a. ISO/IEC 9945-1:1996: POSIX Part 1 - System Application Program Interface (Includes realtime and threads).

b. IEEE 1224:1993: OSI Abstract Data Manipulation - API.

c. IEEE 1224.2:1993: Directory Services - API.

d. IEEE 1238.1:1994: OSI Applications Program Interface - FTAM.

e. IEEE 1351:1994: Association Control Service Element (ACSE) and Presentation Layer Services - API.

3.8.6.5.6 Recommendations. The IEEE P1003.1g draft standard is composed of a common language-independent specification with two C-language bindings: one compatible with the X/Open Transport Interface (XTI), and one compatible with the Berkeley Sockets interface. The IEEE P1003.5c draft standard is the corresponding Ada language binding for XTI and Sockets.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.7 System management services. Centralized system management services refer to services that allow systems and/or enterprises to be managed from a single, centralized point. Distributed system management services refer to services that allow systems and/or enterprises to be managed from any node in the enterprise, in a variety of ways. In some cases an enterprise may be managed as a single unit, but management tasks can be performed at any node. In other cases, the enterprise may be split into multiple domains, each having its own management system, but the different management systems can cooperate with each other and exchange and use each others' management information.

3.8.7.1 System administration and management APIs. (This BSA appears in part 8 and part 9.) Operating system-based system administration standards provide interfaces to traditional, centralized operating system administration services and utilities. System management APIs refer to standardized Application Programming Interfaces that can be used by system and network managers and application developers to manage a system or network. They also are used to develop a system or network management application, without having to resort to writing third-generation language code or UNIX/POSIX shell scripts to perform the same functions on different machines. In this sense, system and network management APIs are considered productivity tools for system managers and system management application developers.

3.8.7.1.1 Standards. Table 3.8-51 presents standards for system administration and management APIs.

TABLE 3.8-51 System administration and management APIs standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Management Protocol Profiles (XMPP)	C206 (11/93)	Adopted (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
NPC	IEEE	Open Systems Interconnection (OSI) Abstract Data Manipulation - Application Program Interface (API) (Language Independent)	1224:1993	Adopted (Approved)
NPC	IEEE	POSIX System Administration - Part 2: Software Administration (former P1003.7.2)	1387.2:1995	Informational (Approved)
NPC	IEEE	POSIX: System Administration - Part 3: User and Group Administration	1387.3:1996	Informational (Approved)
NPC	IEEE	POSIX System Administration - Part 1: Overview (formerly 1003.7)	P1387.1	Informational (Draft)
NPC	IEEE	POSIX System Administration - Part 4: Print Administration (former P1003.7.1)	P1387.4	Informational (Draft)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.8.7.1.2 Alternative specifications. The following specifications are also available:

a. Groupe Bull: Consolidated Management Architecture (CMA), on which X/Open's XMP and OSF's CM-API are based.

b. Tivoli Systems: Objcall API, which is incorporated in MRB which is based on Tivoli. NOTE: A high-level API, such as the Tivoli Systems' "objcall" API is more suited for application development and integration than for management tasks such as long-term monitoring of system devices.

c. Tivoli Systems: Application Programming Interface (API) to objects.

d. Berkeley Unix.

e. OSF: OSF/1.

3.8.7.1.3 Standards deficiencies. All traditional Unix system administration is difficult. Neither System V system administration facilities nor Berkeley Unix system administration facilities were designed for a distributed networked environment. Traditional Unix system administration is not object-based and is not easily extendable.

3.8.7.1.4 Portability caveats. The traditional AT&T/USL system administration facilities are largely different from and incompatible with the traditional Berkeley Unix system administration facilities.

UI specifies the AT&T/USL system administration for the SVID. OSF provides the Berkeley Unix system administration facilities for OSF/1, except for the System V accounting facilities. The SVID and OSF/1 system administration interfaces, configuration files, and procedures are incompatible. Most of the shell scripts written for SVID-based Unix will not be portable to OSF/1 systems. The many system administration configuration files required by POSIX and Unix are not portable across different machines.

3.8.7.1.5 Related standards. The following standards are related to traditional operating system administration:

a. ISO IS 9595/9596/CCITT X.710/711: CMIS/CMIP (Common Management Information Service/Protocol).

b. ISO IS 7498:1986/CCITT X.700: Management Framework.

c. ISO IS 10040:1991: Systems Management Overview.

d. ISO IS 10164-1:1993/CCITT X.730: Object Management Function.

e. ISO IS 10164-2:1993/CCITT X.731: State Management Function.

f. ISO IS 10164-3:1993/CCITT X.732: Attributes for Representing Relationships.

g. ISO IS 10164-4:1992/CCITT X.733: Alarm Reporting Function.

h. ISO IS 10164-5:1993/CCITT X.734: Event Report Management Function.

i. ISO IS 10164-6:1993:Log Control Function.

j. ISO IS 10164-7:1992/CCITT X.736: Security Alarm Reporting Function.

k. ISO IS 10164-8:1993 Security Audit Trail Function.

l. ISO IS 10164-12:1994 Test Management Function.

m. ISO IS 10165-1:1993/CCITT X.720: Structure of Management Information.

n. ISO IS 10165-2:1992/CCITT X.721: Definition of Management Information.

o. ISO IS 10165-4:1992/CCITT X.722: Guidelines for the Definition of Managed Objects

p. ISO DIS 10181-2.2:1993: Authentication Framework.

q. ISO 8824:1990: (Edition 2) Specification of Abstract Syntax Notation 1 (ASN.1).

r. ISO 8825:1990: Specification of Basic Encoding Rules for ASN.1 (BER).

s. NIST FIPS 146-2: POSIT (for ASN.1 and BER (related to ISO 8824 and 8825)).

t. NIST FIPS 158-1: X Window System (X11 Version 5).

u. NIST FIPS 179-1: Government Network Management Profile (GNMP).

v. IEEE P1003.1e: Security Interface Standards for POSIX.

w. X/Open: G207:9/93: Systems Management Reference Model

x. X/Open: G303:9/93: Systems Management: Managed Object Guide (XMOG).

3.8.7.1.6 Recommendations. The PM should plan to use X/Open's XMPP as a common API to CMIP and SNMP. X/Open, Unix International, and OSF specify the same API, although they call them by different names (XMP and CM-API). The XMP and CM-API hide some of the differences between CMIP and SNMP and eliminate the need to learn two different syntaxes to access both protocols.

The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications. It replaces FIPS 179 (GNMP) in Version 3.0 of the NIST Application Portability Profile.

3.8.7.2 User/group identification. (This BSA appears both in part 8 and part 9.) User/group identification services provide traditional system administration interfaces for administering users and groups. These services are mechanisms for system and network administrators to use when implementing a management policy across a system. Administrators can use the services to establish domains and policies for management throughout the system. They can provide the ability for applications to access group and user databases. Users can set up their own areas of management and policies or use system defaults that are included in management services.

3.8.7.2.1 Standards. Table 3.8-52 presents standards for user/group identification.

TABLE 3.8-52 User/group identification standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
NPC	IEEE	POSIX: System Administration - Part 3: User and Group Administration	1387.3:1996	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
GPC	NIST	Computer Security Guidelines for Implementing the Privacy Act of 1974	FIPS PUB 41:1975	Informational (Approved)
GPC	NIST	Guidelines on Evaluation of Techniques for Automated Personal Identification	FIPS PUB 48:1977	Informational (Approved)

3.8.7.2.2 Alternative specifications. The following specifications are also available:

a. Berkeley Unix: Centralized User and Group Management.
b. OSF/1 O.S.: Centralized User and Group Management.

3.8.7.2.3 Standards deficiencies. User and group management in the SVID, OSF/1, and Berkeley Unix is designed for a centralized, single machine environment. No Ada bindings exist for user and group management standards.

3.8.7.2.4 Portability caveats. System V Unix and the SVID use the commands "useradd" and "groupadd" to add a new user or group to the system. The OSF and Berkeley Unix use the commands "adduser" and "addgroup" to do the same thing.

Although the functionality defined by P1387.3 is based on historical user and group administration practice, no commercial products which conform to the (draft) standard are available as yet.

3.8.7.2.5 Related standards. The following standards are related to user and group management or user and group management standards:

a. ISO/IEC 9595:1991: CMIS.

b. ISO/IEC 9596:1991: CMIP.

c. ISO/IEC DIS 11578.2: RPC.

d. Network Management Forum: OMNIPoint 1.

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

f. Internet RFC 1157: Simple Network Management Protocol.

g. Internet RFC 1213: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

3.8.7.2.6 Recommendations. The mandated standards are recommended.

3.8.7.3 Accounting management. (This BSA appears in part 8 and part 9.) Accounting management services provide the ability to cost services for charging and reimbursement. An effective cost management system should contribute to the development of a sound investment strategy that recognizes and evaluates cost and alternatives. The services should also provide for the ability to measure and prioritize resource usage and to monitor assets and maintain costing records for chargeback purposes. Costs of information technology services should be capable of being apportioned to users, and reports of those costs should be capable of being provided to management and customers.

3.8.7.3.1 Standards. Table 3.8-53 presents standards for accounting management.

TABLE 3.8-53 Accounting management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	OSI Systems Management, Part 10: Usage Metering Function for Accounting Purposes	10164-10:1995	Adopted (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 13: Summarization Function	10164-13:1995	Adopted (Approved)
GPC	NIST	Guideline for Developing and Implementing a Charging System for Data Processing Services	FIPS PUB 96:1982	Adopted (Approved)

3.8.7.3.2 Alternative specifications. The following specifications are also available:

a. OSF/1 O.S.: Centralized Accounting Mgmt.
b. Berkeley BSD 4.3 Unix.

3.8.7.3.3 Standards deficiencies. A variety of different chargeback systems are using different metrics and methods that are causing compatibility problems within agencies and services. The Unix accounting functions are designed for a single machine environment.

The present ISO 10164-10, "Accounting Metering Function," and 10164-13, "Summarization Function," standards were designed with a networked system configuration in mind. Little work has been done in standards groups or products to determine how to use these standards for host configuration management.

Although several standard libraries of object classes that allow a common view of network resources are planned, few are currently available or sufficiently complete. For example, these library specifications have incomplete object definitions for modems, OSI routers, and transport connections.

The ISO standards require ISO CMIS/CMIP for the communication of management information and ISO OSI networking protocols, and do not interoperate with TCP/IP.

No Ada bindings exist for any of the ISO or consortia system management specifications.

3.8.7.3.4 Portability caveats. OSF/1 uses the System V Unix accounting facilities. Although the OSF/1 and System V accounting systems differ, and each operating system has extra accounting functions, the use of the same accounting facilities eliminates one source of incompatibility.

3.8.7.3.5 Related standards. The following standards are related to accounting management or accounting management standards:

a. ISO/IEC 7498:1986: Management Framework.

b. ISO/IEC 8571:1988: FTAM, as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if FTAM functionality are required.

c. ISO/IEC 8650:1988: ACSE, as specified in GOSIP Version 2, Section 4.2.7.1, as modified by the NMSIG agreements in Part 18 of the OIW Implementors Agreements.

d. ISO/IEC 8824:1990: Specification of Abstract Syntax Notation 1 (ASN.1).

e. ISO/IEC 8825:1990: Specification of Basic Encoding Rules for ASN.1.

f. ISO/IEC 9041:1990 (OSI Virtual Terminal), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if virtual terminal functionality is required.

g. ISO/IEC 9072:1989: ROSE, as specified in the Remote Operations Part 1: Model Notation and Service Definition (ROSES), and the Remote Operations Part 2: Protocol Specification (ROSEP), and as modified by the NMSIG agreements clause 6.5.

h. ISO/IEC 9595:1991 CMIS.

i. ISO/IEC 9596:1991 CMIP.

j. ISO/IEC 10165-1:1993: SMI.

k. ISO/IEC 10165-2:1992: DMI.

l. ISO/IEC 10165-4:1992: Guidelines for the Definition of Managed Objects (GDMO).

m. ISO/IEC DIS 11578.2: RPC.

n. CCITT X.400 Message Handling System (MHS), as specified in GOSIP Version 2 Sections 4.2.7.3 and 5.3.2, if message handling functionality is required.

o. IEEE 1224:1993: OSI Abstract Data Manipulation (Object Management) API - Language Independent Specification.

p. IEEE 1327:1993: OSI Abstract Data Manipulation (Object Management) API - C Language Binding.

q. NIST OSI Implementors Workshop (OIW) Implementor Agreements relating to the Presentation and Session layers, as specified in Part 5 (Upper Layer Agreements), clause 13.7 of the OIW Stable Implementation Agreements for OSI Protocols Version 3 (NIST Special Publication 500-224).

r. Internet RFC 1155: Structure and Identification of Management Information for Internets based on TCP/IP.

s. Internet RFC 1157: Simple Network Management Protocol.

t. Internet RFC 1213: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

u. Network Management Forum: OMNIPoint 1.

v. X/Open: OSI-Abstract-Data Manipulation API (XOM) (Object Management).

3.8.7.3.6 Recommendations. To build or procure account management applications, users must identify the system management functions that are applicable to their requirements. Then they must identify the various specifications within the ISO 10164 and 10165 standards that are related to these requirements. Finally, they must explicitly include the requirements and the related standards in the RFP.

In the future, the NIST plans to provide a capability in the GNMP to integrate the present GNMP with SNMP.

3.8.7.4 System configuration. (This BSA appears both in part 8 and part 9.) System configuration services is a representation of the components and component parameters of a computer system (e.g., memory boards, amounts of memory, memory addresses, particular interrupts, networks, network addresses, and specific peripherals such as keyboards, disk drives, terminals, mice or other input devices, and specialized instruments). Clearly, every computer must have a way to do this. System configuration also refers to the automation of this procedure (i.e., automated system configuration) and the ability to configure the system on-line. On-line configuration refers to the ability for system administrators to make dynamic configuration changes, while users are working on-line, rather than having to take the system down.

3.8.7.4.1 Standards. Table 3.8-54 presents standards for system configuration.

TABLE 3.8-54 System configuration standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 1: Object Management Function	10164-1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 2: State Management Function	10164-2:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 3: Attributes for Representing Relationships	10164-3:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 12: Test Management Function	10164-12:1994	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)

3.8.7.4.2 Alternative specifications. No other consortia or de facto specifications are available.

3.8.7.4.3 Standards deficiencies. The present ISO 10164-3, "Attributes for Representing Relationships," and 10164-12, "Test Management Function," standards were designed with network configuration in mind. Theoretically, these standards should be able to be used for configuration management of any computer system. Until now, very little work has been done in this area, either in standards groups or in products. Exactly how these standards should be used in host management is undetermined.

Versions 1.0 and 2.0 of the GNMP specify only network management capabilities. Not until Version 3.0 is available will the GNMP specify the management information required for general system management, such as host computer configuration and management, operating systems management, and database management systems.

The present ISO standards and GNMP specifications require ISO CMIS/CMIP for the communication of management information and ISO OSI networking protocols. Plans are for the

GNMP to provide a capability to integrate the present GNMP with SNMP also. One reason for this goal is the widespread use of SNMP.

No Ada bindings exist for the configuration management standards or consortia specifications.

3.8.7.4.4 Portability caveats. Unknown

3.8.7.4.5 Related standards. The following standards are related to system configuration or system configuration standards:

a. ISO/IEC 7498-4:1989: Management Framework.

b. ISO/IEC 8571:1988: File Transfer, Access, and Management (FTAM), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if FTAM functionality are required.

c. ISO/IEC 8650:1988: ACSE, as specified in GOSIP Version 2, Section 4.2.7.1, as modified by the Network Management SIG (NMSIG) agreements in Part 18 of the OSI Implementors' Workshop (OIW) Implementors Agreements.

d. ISO/IEC 8824:1990: Specification of Abstract Syntax Notation 1 (ASN.1).

e. ISO/IEC 8825:1990: Specification of Basic Encoding Rules for ASN.1.

f. ISO/IEC 9041:1990: (OSI Virtual Terminal), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if virtual terminal functionality is required.

g. ISO/IEC 9072:1989: Remote Operations Service Element (ROSE), as specified in the Remote Operations Part 1: Model Notation and Service Definition (ROSES), and the Remote Operations Part 2: Protocol Specification (ROSEP), and as modified by the NMSIG agreements clause 6.5.

h. ISO/IEC 9595:1991: CMIS.

i. ISO/IEC 9596:1991: CMIP.

j. ISO/IEC 10165-1:1993: Structure of Management Information (SMI).

k. ISO/IEC 10165-2:1992: Definition of Management Information (DMI).

l. ISO/IEC 10165-4:1992: Guidelines for the Definition of Managed Objects (GDMO).

m. ISO/IEC DIS 11578.2: Remote Procedure Call.

n. IEEE 1224:1993: OSI Abstract Data Manipulation (Object Management) API - Language Independent Specification.

o. IEEE 1327:1993: OSI Abstract Data Manipulation (Object Management) API - C Language Binding.

p. Comite Consultatif International de Telegraphique et Telephonique (CCITT) X.400 Message Handling System (MHS), as specified in GOSIP Version 2 Sections 4.2.7.3 and 5.3.2, if message handling functionality is required.

q. NIST OSI Implementors Workshop (OIW) Implementor Agreements relating to the Presentation and Session layers, as specified in Part 5 (Upper Layer Agreements), clause 13.7 of the OIW Stable Implementation Agreements for OSI Protocols Version 3 (NIST Special Publication 500-224).

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

s. Internet RFC 1157: Simple Network Management Protocol.

t. Internet RFC 1213: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

u. X/Open: C315:5/94: OSI-Abstract-Data Manipulation API (XOM) (Object Management).

3.8.7.4.6 Recommendations. OMNIPoint 1 is recommended. The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications.

To build or procure configuration management applications, users must identify the system management functions that are applicable to their requirements. Then they must identify the various ISO 10164 and 10165 standards whose specifications are related to these requirements. Finally, they must include their explicit requirements and the related standards in the RFP.

3.8.7.5 Communication of management information. (This BSA appears in part 8 and part 9.) Communication of management information refers to a mechanism and protocol with extensions specifically geared to the communication of data and information used by system management and network management applications for monitoring and controlling resources. This management information may be shared between management processes and structured according to the requirements of those processes.

3.8.7.5.1 Standards. Table 3.8-55 presents standards for communication of management information.

TABLE 3.8-55 Communication of management information standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	Simple Network Management Protocol (SNMP)	Standard 15/RFC-1157	Mandated (Approved)
GPC	DOD	DoD Standardized Profiles - Internet Network Management Profile for DoD Communications	MIL-STD-2045-17507:7/94	Informational (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) - Part 1: Specification (Includes amendment 1 and 2 of ISO/IEC 9596-1:1990)	9596-1:1991	Informational (Approved)
IPC	ISO/IEC	Elements of Management Information Relating to OSI Network Layer Standards	10733:1993	Informational (Approved)
IPC	ISO/IEC	Elements of Management Information Related to OSI Data Link Layer Standards	10742:1994	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
CPC	X/Open	Management Protocol Profiles (XMPP)	C206 (11/93)	Informational (Approved)
CPC	IETF	Protocol Operations for Simple Network Management Protocol, version 2 (SNMPv2)	RFC 1448:1993	Informational (Approved)
IPC	ISO	OSI Remote Procedure Call (RPC) (Replaces DIS 11578 PT 1 Thru PT 4)	11578:2	Informational (Draft)
IPC	IAB	Simple Management Protocol (SMP)(Developed in response to an IETF request for an improved SNMP)	SMP	Informational (Draft)

3.8.7.5.2 Alternative specifications. Hewlett-Packard's Postmaster, on which the OSF DME's CMIP and Simple Network Management Protocol (SNMP) implementations are based, is also available.

3.8.7.5.3 Standards deficiencies. With its object-oriented approach, CMIS/CMIP has a relatively expensive initial application implementation cost. This flaw is offset by a low maintenance cost, because CMIS/CMIP allows objects to be added, and an associated level of management to be

provided, at a small incremental cost. There is no standard API to CMIS/CMIP. Only a limited number of narrowly focused applications are implemented with it. It lacks a complete set of associated object definitions needed for network management and sufficient associated security standards.

The SNMP is a simple request-and-reply protocol. It performs all its operations using a fetch-and-store paradigm, rather than defining a large set of commands. Effectively, the SNMP network manager is restricted to only two commands that are performed on Management Information Base (MIB) data items: "set" and "get." Variables are retrieved (get) or modified (set). All other operations are defined as side-effects of the "set" operation.

The SNMP's chief disadvantage is the fact that its simplicity severely limits the protocol's ability to satisfy users' requirements for event reporting, sufficient control, and extensibility. Because SNMP is so simplistic and limited, it provides more of a monitoring and data gathering capability than a management function.

The SNMP accommodates only limited event reporting by means of the "trap" mechanism. Other events must be discovered by the managing node by means of periodic polling. Its simplicity compromises its ability to support consistent or extensive addressing. It has limited security capabilities, and does not support threshold-driven performance notification except indirectly through side effects or "set" operations on MIB items. SNMP cannot be extended easily.

The SNMP has a high maintenance cost. Although the first implementation of SNMP is relatively inexpensive, SNMP's simplicity so severely limits its extensibility that future SNMP developments are more likely to occur in the form of new proprietary and standard Management Information Bases (MIBs) rather than as SNMP enhancements. Each additional MIB will require changes and additions to its existing specific applications to support new functions. New MIBs also will require a unique application code to be developed, modified, documented, and supported. MIB development and maintenance can result in a high cost to users and vendors and present a major SNMP concern.

The SNMP lacks an object-oriented approach to network management. The lack of object orientation is a major factor limiting the SNMP's extensibility and its ability to support legacy systems, support system and network management, and make complex distributed system management more intuitive.

It lacks the ability to manage a network of networks in which different managers must interact on a peer-to-peer basis.

Because the SNMP cannot be extended easily, and extensions require changes to SNMP applications, developing new SMP products rather than retooling existing ones probably will be less costly.

The future of SMP is uncertain because it is unclear whether vendors will want to develop new products for a protocol that is incompatible with the major systems management standards today (e.g., from ISO, NMF, X/Open, and OSF). SMP is still less functional than CMIS/CMIP.

The SMP is not an Internet standard. Although developed in response to a request issued by the Internet Engineering Task Force (IETF) for an improved SNMP, SMP was developed outside the IETF. Furthermore, the SMP developers do not plan to submit it as a proposed Internet standard. They feel that submitting SMP to a committee would subject it to alteration and a lengthy review, and would slow down development of a coherent technology.

SMP is not accepted by groups such as the Network Management Forum (NMF), X/Open, OSF, and the National Institute of Standards and Technology (NIST). These groups are resistant to SMP because it lacks an object-oriented approach to network management. Despite the improvements, without object orientation, SMP is still incompatible with the ISO and NMF network management model, as well as with the OSF's Distributed Management Environment (DME) and X/Open's systems management specifications. Vendors moving from SNMP to SMP may find it more cost effective to develop new SMP products.

SMP is not easily extensible, and like SNMP, is expensive to extend. This is largely due to SMP's lack of an object-oriented approach to network management.

3.8.7.5.4 Portability caveats. Nonstandard SNMP MIB definitions have proliferated. The SNMP MIB is tailored to accommodate only Internet equipment. Despite the X/Open, OSF, and former UI (now X/Open) consolidated interface to CMIP and SNMP (X/Open Management Protocol (XMP) and CM-API), without object-orientation SNMP is still incompatible with the ISO and NMF network management model, as well as with the OSF's Distributed Management Environment (DME) and X/Open's systems management specifications.

SNMP's design does not lend itself to migration from and coexistence with legacy systems. For example, SNMP does not support the ability to send the same operation to different classes of objects (an important concept known in this context as "polymorphism," which CMIS/CMIP supports).

3.8.7.5.5 Related standards. The following standards are related to management information communication standards:

a. ISO/IEC 7498:1986: Management Framework.

b. ISO/IEC 8326:1987 and 8327:1987: Connection-Oriented Session Service and Connection-Oriented Session Protocol, respectively.

c. ISO/IEC 8326 AD 2: Connection-Oriented Session Service - Incorporation of Unlimited User Data.

d. ISO/IEC 8327 AD 2: Connection-Oriented Session Protocol - Incorporation of Unlimited User Data.

e. ISO/IEC 8571:1988: FTAM, as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if File transfer, Access, and Management functionality are required.

f. ISO/IEC 8649:1988 and 8650:1988: Association Control Service Element (ACSE) and Association Control Protocol (ACP), as specified in GOSIP Version 2, Section 4.2.7.1, as modified by the NMSIG agreements in Part 18 of the OIW Implementors Agreements.

g. ISO/IEC 8822:1988 and 8823:1988: Connection-Oriented Presentation Service and Connection-Oriented Presentation Protocol, respectively.

h. ISO/IEC 8824:1990: Abstract Syntax Notation 1 (ASN.1).

i. ISO/IEC 8825:1990: Basic Encoding Rules (BER) for ASN.1 .

j. ISO/IEC 9041:1990: (OSI Virtual Terminal), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if virtual terminal functionality is required.

k. ISO/IEC 9072-1:1989 and 9072-2:1989: ROSE and Remote Operations Protocol (ROP), as specified in the Remote Operations Part 1: Model Notation and Service Definition (ROSES) and the Remote Operations Part 2: Protocol Specification (ROSEP), and as modified by the NMSIG agreements clause 6.5.

l. ISO/IEC 10165-1:1993: SMI.

m. ISO/IEC 10165-2:1992: DMI.

n. ISO/IEC 10165-4:1992: Guidelines for the Definition of Managed Objects (GDMO).

o. CCITT X.400 Message Handling System (MHS), as specified in GOSIP Version 2 Sections 4.2.7.3 and 5.3.2, if message handling functionality is required.

p. NIST OSI Implementors Workshop (OIW) implementor Agreements relating to the Presentation and Session layers, as specified in Part 5 (Upper Layer Agreements), clause 13.7, of the OIW Stable Implementation Agreements for OSI Protocols Version 3 (NIST Special Publication 500-224).

q. Open Software Foundation Distributed Computer Environment (DCE): Remote Procedure Call (RPC) Service Definition.

r. Plan to use IEEE 1327 Object Management API, or X/Open's XOM (on which 1327 is based) to simplify the management of networked managed resources in a CMIP environment. (See system management APIs BSA in part 8 for more information.)

s. RFC 1006:1987: ISO transport services on top of the TCP: version 3 (IAB Std 35).

3.8.7.5.6 Recommendations. All new systems and systems undergoing major upgrades should use the Internet Architecture Board (IAB) STD 15, SNMP (RFC 1157). Those persons conducting procurements that involve IAB standards should review the latest version of the IAB official protocol standards list to ensure that the appropriate RFCs are specified.

The PM should plan to use CMIS/CMIP for OSI/GOSIP networks and existing TCP/IP networks, because SNMP does not have the required functionality to manage distributed networks and is very expensive to maintain.

Until environments become distributed, SNMP is a suitable solution for stand-alone local area networks.

The PM also should plan to use either X/Open's XMP or OSF's CM-API (they are the same) as a common API to CMIP and SNMP. (See the system administration and management APIs BSA in part 8 for more information).

The CMOT users, vendors, and applications should be aware of some of the functional differences between OSI managed systems and Internet agents because CMIS/CMIP's more sophisticated and additional features may be difficult to map reliably to TCP/IP and SNMP.

A common protocol API should be used to access CMIP and SNMP. X/Open, Unix International, and OSF specify the same API. X/Open and Unix International call the API "XMP" (X/Open Management Protocol); OSF calls the same protocol CM-API (Consolidated Management API). Although XMP and CM-API provide an extra call specific to SNMP, because the SNMP "GetNext" function call does not work in an OSI environment, the consolidated management protocol API provides the union of the CMIP and SNMP protocols and service primitives consistently. It hides some of the differences between CMIP and SNMP. For most work, programmers and system managers need to learn only a single syntax to access both protocols.

3.8.7.6 Error and event logging. (This BSA appears both in part 8 and part 9.) Error logging is the automatic logging of errors and events to a log (special file) to avoid system or network faults (by detecting that the operation of a component is approaching the edge of its operational range) and to provide a historical record that can be studied to diagnose faults after their occurrence and perhaps prevent their happening in the future.

On the detection of events of interest, the operating system may automatically write the encoded event to the system log and/or may notify a process of the occurrence. This is certainly the case when an error with a high severity level is detected. Logging or notification may occur at any time in the operation of a system. They may occur when an application or the operating system has detected an error, when an event has been generated during event classification (especially if the event is indicative of imminent failure of a component), or when an event is severe and requires the immediate attention of a process and when a corrective action is taken, such as when a processor(hardware) or process(software) is being registered for service.

3.8.7.6.1 Standards. Table 3.8-56 presents standards for error and event logging.

TABLE 3.8-56 Error and event logging standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
CPC	X/Open	Single UNIX Specification, System Interface Definitions, Version 2, Issue 5	C605 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 4: Alarm Reporting Function	10164-4:1992	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 5: Event Report Management Function	10164-5:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 6: Log Control Function	10164-6:1993	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendc Services for Reliable, Available, and Serviceable Systems (SRASS) [C Language]	P1003.1h	Emerging (Formative)
CPC	X/Open	Single Unix Specification Spec. 1170, System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Informational (Superseded)
CPC	X/Open	Single Unix Specification Spec. 1170, System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Informational (Superseded)

3.8.7.6.2 Alternative specifications. The following specifications are also available:

a. Banyon Systems' Network Event Logger (NeL) (from Wang Laboratories) on which OSF's Event Notification Component is based.

b. Banyon Systems' PC library for the Network Event Logger (NeL), which filters and logs PC events locally and sends them to a Network Event Logger server on a host system for further processing.

3.8.7.6.3 Standards deficiencies. No Ada bindings are available for any of the consortium's system management Error Logging Components.

3.8.7.6.4 Portability caveats. Portability problems related to the existing standards are unknown.

3.8.7.6.5 Related standards. The following standards are related to error logging standards:

a. ISO/IEC DIS 11578.2: OSI - RPC (Replaces DIS 11578 PT 1 Thru PT 4).
b. NIST APP - Special Pub. 550-230:1995.
c. OSF: DCE RPC Component.
d. USL/Sun Microsystems: Open Network Computing (ONC) RPC Component.

3.8.7.6.6 Recommendations. OMNIPoint 1 is recommended. The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.7.7 Subsystem management. (This BSA appears both in part 8 and part 9.) Subsystem Management Service (SMS) is a product that controls the execution of system processes (usually daemons). It ensures that related processes are started (or stopped) in the proper sequence. It also provides a standard systems administration command syntax to start/stop these processes, and the specification for an RPC interface that could be embedded into daemons to allow administrator interaction. Without SMS, the commands to start these processes are embedded in the system startup file. There is no mechanism to ensure that one daemon is ready before starting a related one. To stop a daemon, the administrator needs to know the syntax of the appropriate command, and needs to know which other related daemons also need to be stopped. If a daemon dies, the administrator needs to know which related processes to stop, and the proper sequence to restart them.

3.8.7.7.1 Standards. Table 3.8-57 presents standards for subsystem management.

TABLE 3.8-57 Subsystem management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.7.7.2 Alternative specifications. There are no alternative specifications available.

3.8.7.7.3 Standards deficiencies. There are no products currently using the OSF DME SMS specifications. The software available from the OSF could be used as-is, although it is intended to be used by third-party vendors as the basis for products.

There are also no daemons that implement the SMS RPC interface, except for the ones that come with OSF DME. Therefore the SMS is required to use Signals to stop daemons, which may have unpredictable results if the daemon does not catch the signal correctly.

3.8.7.7.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.8.7.7.5 Related standards. The following standard is related to subsystem management.

a. OSF DCE Remote Procedure Call (RPC)

3.8.7.7.6 Recommendations. There are no recommendations.

3.8.7.8 Event management. Event management and notification services allow system managers and system administrators to be informed that a predefined system or network event of interest (e.g., additional resources needed) has occurred, so that the event may be managed in a predefined way that prevents network or system problems. Event management is related closely to fault and performance management, in that each of these services could make use of event management to log, track, and provide alerts based on relevant events.

3.8.7.8.1 Standards. Table 3.8-58 presents standards for event management.

TABLE 3.8-58 Event management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
GPC	NIST	Stable Implementation Agreements for Open System Environments, Ver. 8, Ed. 1	Special Pub. 500-224:12/94	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 5: Event Report Management Function	10164-5:1993	Informational (Approved)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Informational (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amend: Software for Reliable, Available, and Serviceable Systems (RASS) [C Language]	P1003.1b	Informational (Transitional)

3.8.7.8.2 Alternative specifications. The following specifications are also available:

a. Banyon Systems' Network Event Logger (from Wang Laboratories) on which OSF's Event Notification Component is based.

b. Banyon Systems' PC library for the Network Event Logger, which filters and logs PC events locally and sends them to a Network Event Logger server on a host system for further processing. The OSF DME's PC Error Logging Component is based on this Banyon Systems' PC library.

3.8.7.8.3 Standards deficiencies. None of the event notification components in any of the consortia management systems are compatible with the IEEE P1003.1b specifications for event notification. OSF DME event management is intended to be used as the basis for commercial management systems, but is not currently supported by any products.

3.8.7.8.4 Portability caveats. Portability problems with the existing specifications are unknown.

3.8.7.8.5 Related standards. The following standards are related to event management and notification standards:

a. ISO/IEC DIS 11578.2: RPC (Replaces DIS 11578 PT 1 Thru PT 4.)

b. NIST APP - Special Pub. 500-230: 1995.

c. OSF: Distributed Computing Environment (DCE) Remote Procedure Call Component.

d. USL/Sun Microsystems: Open Network Computing (ONC) Remote Procedure Call (RPC) Component.

e. NIST FIPS 179-1:1995: Government Network Management Profile (GNMP).

f. ISO/IEC 9596-1:1991: OSI CMIP, Part 1: Specification.

g. IAB: RFC 1157: SNMP.

3.8.7.8.6 Recommendations. OMNIPoint 1 is recommended. The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications.

3.8.7.9 Performance management. (This BSA appears in part 8 and part 9.) Performance management provides services and interfaces for tuning systems and subnetworks to meet individual performance requirements. Performance management enables the behavior of resources and the effectiveness of communication activities to be evaluated. It includes functions to: gather statistical information; maintain and examine logs of system state histories; determine system performance under natural and artificial conditions; and alter system modes of operation for the purpose of conducting performance management activities. Performance management may make use of event management facilities.

3.8.7.9.1 Standards. Table 3.8-59 presents standards for performance management.

TABLE 3.8-59 Performance management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Data Communications Systems and Services -User Oriented Performance Parameters (adopts ANSI X3.102-1983/R1990)	FIPS PUB 144:1985	Adopted (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 11: Metric Objects and Attributes	10164-11:1994	Informational (Approved)
GPC	NIST	Guideline on Computer Performance Management: An Introduction	FIPS PUB 49:1977	Informational (Approved)
GPC	NIST	Guidelines for the Measurement of Interactive Computer Service Response Time and Turnaround Time	FIPS PUB 57:1978	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
GPC	NIST	Guidelines for Measurement of Remote Batch Computer Service	FIPS PUB 72:1980	Informational (Approved)

3.8.7.9.2 Alternative specifications. No other consortia or de facto specifications are available.

3.8.7.9.3 Standards deficiencies. The present 10164-11 ("Workload Monitoring Function) and generic 10165-xx standards were designed with network configuration in mind. Theoretically, they should be able to be used for configuration management of any computer system. Little work has been done in this area, either in standards groups or in products. Exactly how these standards should be used in host management is undetermined. Standards for system performance measurement are needed.

Although several standard libraries of object classes that allow a common view of network resources and support performance management of network resources are planned, few are currently available or sufficiently complete. For example, these library specifications have incomplete object definitions for modems, OSI routers, and transport connections. Based on needs of the U.S. Federal Government (as shown by NIST surveys), the GNMP added more object class specifications and definitions. These include the following objects: LANs, X.25 WANs, ISDN, FDDI, modems, bridges, links, and a rudimentary capability to manage OSI

routers and transport connections. Phase 2 GNMP objects also will include protocol software (layers 3-7), routers, terminal servers, MTAs, PBXs, and circuit switches.

Versions 1.0 and 2.0 of the GNMP currently specify only network management capabilities. Not until Version 3.0 will the GNMP specify the management information required for general system management, such as host computer configuration and management, operating systems, and database management systems.

The present ISO standards and GNMP specifications require ISO CMIS/CMIP for the communication of management information and ISO OSI networking protocols. Plans are for the GNMP eventually to provide a capability to integrate the present GNMP with SNMP. One reason for this goal is the widespread use of SNMP.

No Ada binding is available for the ISO system management standards.

Performance management could make use of generalized event management facilities, but most products currently implement their own event management.

3.8.7.9.4 Portability caveats. Portability problems related to the existing specific [illegible] are unknown.

3.8.7.9.5 Related standards. The following standards are related to performance management or performance management standards:

a. ISO/IEC 7498-4:1989: Management Framework.

b. ISO/IEC 8571:1988: FTAM, as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if FTAM functionality are required.

c. ISO/IEC 8650:1988: Association Control Service Element (ACSE), as specified in GOSIP Version 2, Section 4.2.7.1, as modified by the NMSIG agreements in Part 18 of the OIW Implementors Agreements.

d. ISO/IEC 8824:1990: Specification of Abstract Syntax Notation 1 (ASN.1).

e. ISO/IEC 8825:1990: Specification of Basic Encoding Rules for ASN.1.

f. ISO/IEC 9041:1990: (OSI Virtual Terminal), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if virtual terminal functionality is required.

g. ISO/IEC 9072:1989: ROSE, as specified in the Remote Operations Part 1: Model Notation and Service Definition (ROSES), and the Remote Operations Part 2: Protocol Specification (ROSEP), and as modified by the NMSIG agreements clause 6.5.

h. ISO/IEC 9595:1991: CMIS.

i. ISO/IEC 9596:1991: CMIP.

j. ISO/IEC 10165-1:1993: SMI.

k. ISO/IEC 10165-2:1992: DMI.

l. ISO/IEC 10165-4:1992: GDMO.

m. ISO/IEC DIS 11578.2: RPC.

n. CCITT X.400 Message Handling System (MHS), as specified in GOSIP Version 2 Sections 4.2.7.3 and 5.3.2, if message handling functionality is required.

o. IEEE 1224:1993: OSI Abstract Data Manipulation (Object Management) API - Language Independent Specification.

p. IEEE 1327:1993: OSI Abstract Data Manipulation (Object Management) API - C Language Binding.

q. NIST OSI Implementors Workshop (OIW) Implementor Agreements relating to the Presentation and Session layers, as specified in Part 5 (Upper Layer Agreements), clause 13.7, of the OIW Stable Implementation Agreements for OSI Protocols Version 3 (NIST Special Publication 500-224).

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

s. Internet RFC 1157: Simple Network Management Protocol.

t. Internet RFC 1158: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

u. X/Open: C315:5/94: OSI-Abstract-Data Manipulation API (XOM) (Object Management).

3.8.7.9.6 Recommendations. To procure performance management applications, users must identify the system management functions that are applicable to their requirements. Then they must identify the various specifications in the ISO 10164 and 10165 standards related to these requirements. Finally, they must include their requirements and the related standards in the RFP.

The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications. It replaces FIPS 179 (GNMP) in

Version 3.0 of the NIST Application Portability Profile. OMNIPoint adopts the ISO 10164 and 10165 series of standards.

FIPS 144 is a mandatory standerd according to the Federal ADP and Telecommunications Standards Index and shall be used if it satisfies the user's requirements.

3.8.8 Fault management services. A fault condition arises whenever a malfunction or abnormal behavior results or may result in an error, outage, or degradation of services. Fault Management services allow a system to minimize the impact of faults on a system. These services are designed to detect events of interest, namely, errors, events indicative of imminent failures, and events associated with recovery from the effects of faults. This is accomplished by providing services to detect events of interest, collect the associated state of these events, encode the events, log the encoded events together with their associated states, provide notification of such events, classify such events, recover from errors, and reconfigure the system. The services have two aspects to them, those that support system recovery from errors while it is running, and those that support the maintainability of the system. For example when a disk read retry threshold has been exceeded this may indicate a pending disk failure. In order that the system maintain its fault tolerant characteristics and maintain high availability a spare or backup contingency should be available. Fault management has four main functional areas, detection, logging and notification, diagnosis, and corrective action.

Faults in a system are not detected directly, they are inferred from their effects, namely the errors and / or anomalous events that arise as a result of these faults. The following definitions of fault, error and failure are used in the discussion that follows. A failure results when the service that a system delivers no longer complies with the system specification, which is assumed to be authoritative. An error is that part of the system state which may lead to failure. Finally, a fault is the assigned or hypothesized cause of an error. Faults are managed in two ways. One way is to continue processing in the face of errors in the system, and the other is to diagnose and passivate a fault (that is to prevent it from being reactivated) or to diagnose and isolate the fault, so that the faulty component may be repaired.

3.8.8.1 Fault management. (This BSA appears in part 8 and part 9.) Fault management services allow a system to react to the loss or incorrect operation of system components. Fault management services encompass services for fault detection, isolation, diagnosis, recovery, and avoidance. Fault management may make use of event management facilities. In practice, fault management and performance management products often incorporate event management functions.

3.8.8.1.1 Standards. Table 3.8-60 presents standards for fault management.

TABLE 3.8-60 Fault management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 4: Alarm Reporting Function	10164-4:1992	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	OSI Systems Management, Part 5: Event Report Management Function	10164-5:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 6: Log Control Function	10164-6:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 12: Test Management Function	10164-12:1994	Informational (Approved)
NPC	SAE	General Open Architecture (GOA) Framework	AS 4893 (Committee AS-5)	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.8.1.2 Alternative specifications. The following specifications for network fault reporting are available:

a. Banyon Systems's Network Event Logger (originally developed by Wang Laboratories), on which OSF's DME event services and logging services are based.

b. Gradient Technologies: PC Event system integrated with a Banyon Systems-based Network Event Logger PC library and a PC Ally server on which OSF has based its PC event and logging component.

3.8.8.1.3 Standards deficiencies. The present ISO 10164-4, "Alarm Reporting Function," 10164-6, "Log Control Function," 10164-5, "Event Report Management Function," 10164-12, "Test Management Function," and 10164-14, "Confidence and Diagnostic Testing Service" standards were designed with network configuration in mind. Theoretically, these standards should be able to be used for configuration management of any computer system. Little work has been done in this area, either in standards groups or in products. Therefore, exactly how these standards should be used in host management is undetermined.

Although several standard libraries of object classes that allow a common view of network resources and fault management of network resources are planned, few are available or sufficiently complete. For example, these library specifications have incomplete object definitions for modems, OSI routers, and transport connections. Based on U.S. Federal Government needs (as shown by NIST surveys), the GNMP added more object class specifications and definitions. These include the following objects: LANs, X.25 Wide-Area-Networks (WANs), Integrated Services Digital Network (ISDN), Fiber Distributed Data Interface (FDDI), modems, bridges, links, and a rudimentary capability to manage OSI routers and transport connections.

Phase 2 GNMP objects also will include protocol software (layers 3-7), routers, terminal servers, Message Transfer Agents (MTAs), Private Branch Exchange (PBXs), and circuit switches.

Versions 1.0 and 2.0 of the GNMP currently specify only network management capabilities. Not until Version 3.0 will the GNMP specify the management information required for general system management, such as host computer configuration and management, operating systems, and database management systems.

The present ISO standards and GNMP specifications require ISO CMIS/CMIP for the communications of management information and ISO OSI networking protocols. Plans are for the GNMP eventually to provide a capability to integrate the present GNMP with SNMP also. One reason for this goal is the widespread use of SNMP.

No Ada bindings exist for any of the ISO or consortia system management specifications.

Fault management should make use of general event management such as OSF DME event services, but most products currently implement their own event management facilities.

Finally, standards are needed for problem reporting and tracking, diagnostic standards for hardware and software, and fault isolation.

3.8.8.1.4 Portability caveats. Portability problems with the existing specifications are unknown.

3.8.8.1.5 Related standards. The following standards are related to fault management or fault management standards:

a. ISO/IEC 7498-4:1989: Management Framework.

b. ISO/IEC 8571:1988: File Transfer, Access, and Management (FTAM), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if File transfer, Access, and Management functionality are required.

c. ISO/IEC 8650:1988: Association Control Service Element (ACSE), as specified in GOSIP Version 2, Section 4.2.7.1, as modified by the NMSIG agreements in Part 18 of the OIW Implementors Agreements.

d. ISO/IEC 8824:1990: Specification of Abstract Syntax Notation 1 (ASN.1).

e. ISO/IEC 8825:1990: Specification of Basic Encoding Rules for ASN.1.

f. ISO/IEC 9041:1990: (OSI Virtual Terminal), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if virtual terminal functionality is required.

g. ISO/IEC 9072:1989: Remote Operations Service Element (ROSE), as specified in the Remote Operations Part 1: Model Notation and Service Definition (ROSES),

and the Remote Operations Part 2: Protocol Specification (ROSEP), and as modified by the NMSIG agreements clause 6.5.

h. ISO/IEC 9595:1991: Common Management Information Service (CMIS).

i. ISO/IEC 9596:1991: Common Management Information Protocol (CMIP).

j. ISO/IEC 10165-1:1993: Structure of Management Information (SMI).

k. ISO/IEC 10165-2:1992: Definition of Management Information (DMI).

l. ISO/IEC 10165-4:1992: Guidelines for the Definition of Managed Objects (GDMO).

m. ISO/IEC DIS 11578.2: Remote Procedure Call.

n. CCITT X.400 Message Handling System (MHS), as specified in GOSIP Version 2 Sections 4.2.7.3 and 5.3.2, if message handling functionality is required.

o. IEEE 1224:1993: OSI Abstract Data Manipulation (Object Management) API - Language Independent Specification.

p. IEEE 1327:1993: OSI Abstract Data Manipulation (Object Management) API - C Language Binding.

q. NIST OSI Implementors Workshop (OIW) Implementor Agreements relating to the Presentation and Session layers, as specified in Part 5 (Upper Layer Agreements), clause 13.7 of the OIW Stable Implementation Agreements for OSI Protocols Version 3 (NIST Special Publication 500-224).

r. Internet RFC 1155: Structure and Identification of Management Information for Internets based on TCP/IP.

s. Internet RFC 1157: Simple Network Management Protocol.

t. Internet RFC 1158: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

u. X/Open: OSI-Abstract-Data Manipulation API (XOM) (Object Management).

3.8.8.1.6 Recommendations. To build or procure fault management applications, users must identify the system management functions that are applicable to their requirements. Then they must identify the various specifications within the ISO 10164 and 10165 standards related to these requirements. Finally, they must specify the requirements and the related standards in the RFP.

The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications. It replaces FIPS 179 (GNMP) in Version 3.0 of the NIST Application Portability Profile.

3.8.8.2 Core dump. Core dump APIs allow the process to specify the location where the core dump file is written. Many times as a last resort a core dump may be initiated at termination. This is useful as a debug aid. This API allows an analyst to find the core file and post process it.

3.8.8.2.1 Standards. Table 3.8-61 presents standards for core dumps.

TABLE 3.8-61 Core dump standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

3.8.8.2.2 Alternative specification. There are no alternative specifications.

3.8.8.2.3 Standard deficiencies. Standard deficiencies are unknown.

3.8.8.2.4 Portability caveats. Portability problems are unknown.

3.8.8.2.5 Related standards. There are no standards related to core dumps.

3.8.8.2.6 Recommendations. There are no adopted standards to recommend.

3.8.8.3 Hardware error and event conditions. (This BSA appears in both part 8 and part 9.) An event is an unsolicited communication from a hardware device to a computer operating system, application, or driver. Events are generally attention-getting messages, allowing a process to know when a task is complete or when an external event occurs. Error conditions (e.g., system failures, unauthorized access attempts, or strange glitches) must be detected and reported so corrective action can be taken to minimize system or network problems. (See the BSA on error and event logging for more information on tracking errors.)

Offline diagnosis of events which have been written in encoded form to the system log is termed event classification. Encoded events which are written to the system log for later analysis form the raw material for algorithms designed to diagnose and passivate faults, that is to prevent them from being reactivated. Offline classification of errors or events which are indicative of the potential failure of a component can be conducted only when the required information has been saved. Algorithms designed to improve system maintenance and to shorten the duration of outages generally scan the system event log for patterns of event types. Such algorithms can be used to predict imminent failure of software or hardware components. This analysis of logged events could also be processed in parallel while the main system continues to perform.

Services for the detection of events come in two basic forms: active and passive. Events come in two types, those which are anomalous and those which are not. Anomalous events may be classified into two categories: errors, and events which are indicative of a fault which is not yet producing errors, but is the cause of some degradation in system performance. P1003.1h is already addressing passive errors in their draft standard.

3.8.8.3.1 Standards. Table 3.8-62 presents standards for hardware error and event conditions.

TABLE 3.8-62 Hardware error and event conditions standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, System Interface Definitions, Version 2, Issue 5	C605 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1a	Emerging (Draft)
NPC	IEEE	POSIX, Part 1: System API - Amend: Services for Reliable, Available, and Serviceable Systems (SRASS) [C	P1003.1h	Emerging (Formative)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)

3.8.8.3.2 Alternative specification. The OSF's OSF/1 (product implementation) is also available.

3.8.8.3.3 Standard deficiencies. POSIX.1 has limited error and event condition capabilities. To address this deficiency, P1003.1h is including event detection. Active event detection consists of functions which request information on the occurrence of events that may not normally be reported to an application. Passive event detection occurs when other applications or the underlying system services provide event signaling to an application. Events to be detected include:

-- Software and Hardware errors during operation,
-- Processes that failed or almost failed to meet scheduled deadlines,
-- Times when the system operated in extreme environmental conditions,
-- Errors reported during startup self-testing and,
-- Attempts to violate the security policy of the system

Upon the detection of an error the operating system may raise an exception, signal an exception, abort a process, or take other actions. The action taken by the operating system depends on the level of severity of the error. These actions include the collection of relevant parts of the system state, and the encoding of events for logging and notification by operating system services.

3.8.8.3.4 Portability caveats. Symbolic error numbers are a set of names defined for error numbers set by the "exec" functions to indicate the nature of an error condition that has occurred. Symbolic error numbers have been around for a long time and are reasonably stable. However, many implementations, especially the newer ones, use symbolic error numbers that are different from one another. Applications using such new, different symbolic error numbers are not portable except to implementations using the same error number set.

POSIX, X/Open, and SVID support many of the same symbolic error numbers, with some exceptions. For example, POSIX does not support the error symbols "EIDRM" (indicating an identifier has been removed from the system), "ENOMSG" (required message not in the message queue), and "ETXTBSY" (attempt to overwrite active procedure), even though X/Open, and

SVID support them. Other differences in symbolic error numbers occur in the following error symbols: "EBADMSG," "ENOSR," "ENOSTR," "EPROTO," "ERESTART," and "ETIME."

Symbolic error numbers provide portability only if programmers and vendors implement programs using them. Implementations using numeric numbers instead of symbolic error names and numbers are not portable.

POSIX, X/Open, and SVID allow additional implementation-defined symbolic error names to be created. Such implementation-defined symbolic error numbers may be a necessity for a particular application. These values are usually returned by extended functionality, not defined by POSIX.1. The SVID, for example, defines the symbolic errors "EBADMSG", "ENOSR", and "ENOSTR" which are returned by the kernal "STREAMS" subsystem. These new symbolic error numbers should be portable among all systems which provide the underlying functionality. The longest of the symbolic error number names is "ENAMETOOLONG."

X/Open's Single Unix Specification (Spec 1170) has aligned XPG4 with POSIX in the areas where they overlap. Thus any XPG4 or Single Unix conforming system is guaranteed to respond with the same symbolic error value although, as discussed above, the actual error number may vary.

3.8.8.3.5 Related standards. The following standards are related to hardware error conditions:

a. IEEE 1003.2:1992: POSIX - Shell and Utility Application Interface.

b. IEEE R1003.5:1992: Ada Language Binding for POSIX (under revision).

c. IEEE P1003.1e: Security Interface Standards for POSIX.

d. IEEE P1387.1: POSIX System Administration - Part 1: Overview.

e. IEEE 1387.2:1995: POSIX System Administration - Part 2: Software.

f. IEEE P1387.3: POSIX System Administration - Part 3: User and Group Administration.

g. IEEE P1003.1g: Protocol Independent Interfaces.

h. IEEE 1224.2:1993: Directory Services API - Language Independent.

i. IEEE 1224.1:1993: X.400 Based Electronic Messaging API.

j. IEEE P1238.1: OSI Applications Program Interface - FTAM.

k. IEEE P1351: OSI Application Interfaces - ACSE.

3.8.8.3.6 Recommendations. The mandated standards are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. IEEE 1003.1b added asynchronous event notification to the original IEEE 1003.1. FIPS 151-2 specifies the read/write return options. SUS supports additional error symbols.

To get the better event management capabilities needed for networking, communications, transaction processing, and real time applications, explicitly specify the IEEE 1003.1b standard's real time signals option for asynchronous event notification. For U.S. Federal Government procurements, the NIST Application Portability Profile (APP) and FIPS 151-2 have some special file and directory requirements:

a. The APP and FIPS 151-2 require support for the error message "ENAMETOOLONG" for the open command.

b. The APP and FIPS 151-2 require read() calls and write() calls that are interrupted by a signal after they have successfully read or written data shall return the number of bytes the system has read. POSIX allows the return of either the number of bytes read or written or a return of -1 with "errno" set to [EINTR] after a successful read or write.

To get greater functionality than POSIX provides, establish the error management interfaces provided by X/Open as an internal standard. The problem is that in implementations compliant with POSIX, many specific system calls have differences in their error messages and exception management handling. These system call commands must be analyzed to see which error messages to specify for certain critical commands, as the NIST did in developing FIPS 151-1. A second problem occurs because X/Open, the SVID, and OSF specify more functionalities than POSIX. Even where these functionalities are the same, X/Open's, the SVID's, and OSF/1's error messages are often different. In general, X/Open's error messages for specific system calls tend to be the same, but they differ from OSF/1's, which is the same as Berkeley UNIX's.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.8.4 State collection. Before diagnosis can occur, the relevant parts of the state of a system must be preserved. In those cases where the operating system returns control to an application after the occurrence of an error, the application must decide what action to take. One possible action is a dump of the process state to memory or stable storage. In those cases where the operating system retains control after an error is detected the operating system may save parts of the system state for later analysis.

For those detected events which are classified as anomalous, an application may wish to communicate its interest to the operating system in the event by means of registering for and specifying the extent of the state collection required. The parts of the state preserved are application specific. The checkpointing of a process is an example of a fault tolerance method which requires the process state be saved. Parts of the process state which are candidates for preservation (as determined by the application) examples are process memory, process data segments, process stacks, process states, process status, program counters, pointers and contents of the all CPU registers.

3.8.8.4.1 Standards. Table 3.8-63 presents standards for state collection.

TABLE 3.8-63 State collection standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.8.4.2 Alternative specification. There are no alternative specifications.

3.8.8.4.3 Standard deficiencies. Standard deficiencies are unknown.

3.8.8.4.4 Portability caveats. Portability problems are unknown.

3.8.8.4.5 Related standards. There are no standards related to state collection.

3.8.8.4.6 Recommendations. There are no adopted standards to recommend at this time.

3.8.8.5 Error recovery and reconfiguration. There are two main types of corrective actions to take when error conditions are detected. Error recovery occurs while the system is operational, while reconfiguration may occur when the system is operational or while it is inoperable.

Error recovery methods are based on hardware redundancy, information redundancy and a combination of the two (hybrid redundancy methods). These methods include N modular redundancy with voters, error detection / correction codes, and combinations of the two. Another type of error recovery is temporal redundancy. A technique which is classified under this category is retry. Forward and backward recovery in real-time systems is classified as a hybrid method. Backward recovery generally involves saving the state of a process at intervals, so that the process may be restarted at a point at which its state is valid.

System reconfiguration is a means of providing or improving the fault tolerance of a system. When a faulty component which has been causing errors to occur is isolated and switched offline, a reconfiguration has occurred. In some systems, it is not possible to repair a component. In these systems the fault tolerance characteristics are permanently degraded, whenever a component is removed from operation. For systems which contain redundant reparable components, the fault tolerance characteristics of the system are temporarily degraded.

3.8.8.5.1 Standards. Table 3.8-64 presents standards for error recovery and reconfiguration.

TABLE 3.8-64 Error recovery and reconfiguration standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.8.5.2 Alternative specification. There are no alternative specifications.

3.8.8.5.3 Standard deficiencies. Standard deficiencies are unknown.

3.8.8.5.4 Portability caveats. Portability problems are unknown.

3.8.8.5.5 Related standards. There are no standards related to error recovery and reconfiguration.

3.8.8.5.6 Recommendations. There are no adopted standards to recommend at this time.

3.8.8.6 Diagnosis. Diagnosis of events entails analysis of the state of the system this is where each indiviual fault management application can build in their unique intelligence and knowledge of the system. This may be performed online or offline. In some cases an event may be encoded so that the operating system can take immediate action to deal with an event, a process can register for notification upon the occurance of an event while in others the diagnosis may take place offline. All but the most severe error conditions are usually written in an encoded form into the system log. In some cases these events will also generate a notification message to system management control.

Diagnosis occurs in error recovery though a variety of mechanisms. In an N-modular redundancy error recovery scheme, diagnosis can be performed in real-time. It occurs when the voter(s) detect an inconsistency in the output of N hardware modules. In this case an error is detected and recovery initiated when the output from one (or possibly more) modules is discarded. In more elaborate schemes, the system will then initiate fault diagnosis on the apparently faulty component.

Offline diagnosis of events which have been written in encoded form to the system log is termed event classification.

3.8.8.6.1 Standards. Table 3.8-65 presents standards for diagnosis.

TABLE 3.8-65 Diagnosis standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.8.6.2 Alternative specification. There are no alternative specifications.

3.8.8.6.3 Standard deficiencies. Standard deficiencies are unknown.

3.8.8.6.4 Portability caveats. Portability problems are unknown.

3.8.8.6.5 Related standards. There are no standards related to diagnosis.

3.8.8.6.6 Recommendations. There are no adopted standards to recommend at this time.

3.8.8.7 Shutdown/Reboot services. The intent of these APIs is to provide a means of recovering a system by brute force reinitialization. The same APIs can be used to completely disable a system which is deemed to be faulty in some manner.

3.8.8.7.1 Standards. Table 3.8-66 presents standards for shutdown/reboot.

TABLE 3.8-66 Shutdown/Reboot services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)

3.8.8.7.2 Alternative specification. There are no alternative specifications.

3.8.8.7.3 Standard deficiencies. Standard deficiencies are unknown.

3.8.8.7.4 Portability caveats. Portability problems are unknown.

3.8.8.7.5 Related standards. There are no standards related to shutdown/reboot services.

3.8.8.7.6 Recommendations. More work is needed to fully define these APIs. There is some interest in interfaces to enable orderly system startup and shutdown.

3.8.8.8 Process and event trace services. The trace work within the SRASS Project Authorization Request (PAR) has enjoyed the combined efforts of the SRASS working group and the Realtime working group. Trace is important to both groups because it allows the developer of applications to build a reliable system and it allows the application writer to tell what processes are doing without substantially affecting the intended behavior. This is important in realtime systems since it is not invasive and does not affect critical timing and it is important to reliable systems since it can be used to determine reliability problems. Trace points can be coded and inserted into the application program code with specific triggers which when activated put events of interest quickly into a trace buffer. This information can be used later with the aid of automated tools to help in the analysis of performance problems, behavior problems, detect programming mistakes, or process timing mismatches and randomly exceeded time budgets.

Tracing should be distinguished from on-line debugging in which no special programmatic changes are required in the program, and in which analysis is done at the time the events of interest happen, and from logging, in which the events of interest can be processed by other programs, possibly in realtime.

3.8.8.8.1 Standards. Table 3.8-67 presents standards for process and event trace.

TABLE 3.8-67 Process and event trace services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.8.8.2 Alternative specification. There are no alternative specifications.

3.8.8.8.3 Standard deficiencies. Standard deficiencies are unknown.

3.8.8.8.4 Portability caveats. Portability problems are unknown.

3.8.8.8.5 Related standards. There are no standards related to trace services.

3.8.8.8.6 Recommendations. There are no adopted standards to recommend at this time.

3.8.8.9 Built-in Test . Built-in Test (BIT) is a fault management function that provides a capability to access unique hardware configurations supporting the built-in test functions for operational status of computer components.

3.8.8.9.1 Standard. Table 3.8-68 presents standards for built-in test.

TABLE 3.8-68 Built-in Test standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.8.9.2 Alternative specification. There are no alternative specifications.

3.8.8.9.3 Standard deficiencies. ARD 50067 is domain specific - oriented toward support of avionics applications.

3.8.8.9.4 Portability caveats. Portability problems are unknown because of the immaturity of the specification.

3.8.8.9.5 Related standards. There are no standards related to built-in test.

3.8.8.9.6 Recommendations. There is no approved standard available to recommend at this time.

3.8.9 Clock/calendar services. These are services for maintaining and synchronizing system clocks and triggering events based on the passage of time.

3.8.9.1 Clocks and timers. A clock is a mechanism for measuring the passage of time and maintaining the system time. Timers are used to start or stop processes based on the passage of a specific amount of time. A timer can work together with a clock by sending a start or expiration signal when an associated clock reaches or exceeds a specified time.

3.8.9.1.1 Standards. Table 3.8-69 presents standards for clocks and timers.

TABLE 3.8-69 Clocks and timers standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)

3.8.9.1.2 Alternative specifications. The following specification is available:

a. SAE ARD 50067 Draft: Avionics Operating Syste... API Requirements.

3.8.9.1.3 Standards deficiencies. Deficiencies in the existing standard are unknown.

3.8.9.1.4 Portability caveats.

3.8.9.1.5 Related standards. There are no related standards.

3.8.9.1.6 Recommendations. ISO/IEC 9945-1:1996 is recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996.

3.8.9.2 Real time timers. Real time timers are high resolution timers that allow for fixed, periodic, offset, absolute, and relative schedules, and track elapsed time very accurately to support the highest priority processes and event notifications in real time applications. They also may provide timing signals for timesharing operations.

3.8.9.2.1 Standards. Table 3.8-70 presents standards for real time timers.

TABLE 3.8-70 Real time timers standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPC	X/Open	Single UNIX Specification, System Interface Definitions, Version 2, Issue 5	C605 (2/97)	Emerging (Approved)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
CPC	X/Open	Single UNIX Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (Part of XPG4)	C034 (9/94)	Informational (Superseded)
CPC	X/Open	Single UNIX Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2 (Part of XPG4)	C035 (9/94)	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.8.9.2.2 Alternative specifications. The following specification is also available:

a. Berkeley 4.2/4.3 Unix.

3.8.9.2.3 Standards deficiencies. POSIX.1b timer facilities lack the Berkeley Unix virtual and profiling interval time functions. The POSIX.1b real time timer service, with its requirement for nanosecond resolution timers, is better suited for real time applications than industry standards. For example, the granularity of ISO/IEC 9945-1 timer functions (seconds), Berkeley Unix (seconds and microseconds) the SVID Issue 4 (microseconds), and System V Release 4 (microseconds) is not sufficient for critical real time applications. Also, some real time applications need to have more than one outstanding time interval on the same time base (clock_id) to trigger different functions. Berkeley Unix, ISO/IEC 9945-1:1990, and System V Release 4 do not allow this.

3.8.9.2.4 Portability caveats. System V Release 4 and Berkeley Unix timers are identical to each other. They are not compatible with POSIX.1b timer functions however, because they use signals not existing in POSIX.1b.

The Berkeley Unix "adjtime" function has no POSIX.1b equivalent.

Berkeley Unix does not provide programmatic calls to obtain a timer's resolution or support the ability to request "absolute" timer expirations.

3.8.9.2.5 Related standards. The following standards are related to real time timer standards:

a. None.

3.8.9.2.6 Recommendations. The following wording is recommended for specifying real time timers:

"Real time systems offered as a result of the requirements of which this is a part shall conform to the timer requirements established by the IEEE 1003.1b standard incorporated into ISO/IEC 9945-1:1996 and shall implement nanosecond resolution timers and all of the timer functions specified in the 1003.1b standard, as well as the additional real time features specified elsewhere in this document."

POSIX.1b timer calls can be mapped to System V timer functions. Examples of how to do this are published in draft 12 of the IEEE P1003.1b standard.

The POSIX.1b time functions can be mapped to the Berkeley time functions, although not with the POSIX.1b nanosecond resolution for the timers. The mapping is shown in draft 12 of the POSIX.1b standard.

The Berkeley Unix "adjtime()" function can be implemented as a library function on top of the POSIX.1b "clock_setdrift()" function.

Berkeley Unix's virtual and profiling interval timing functions can be implemented as extensions using new clock_id values.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.9.3 Distributed timing service. (This BSA appears in part 8 and part 11.) Distributed timing service (DTS) guarantees synchronization among all system clocks in a distributed network. Synchronized timing is necessary to maintain scheduling of activities and sequencing of events. DTS uses RPC in the communications between DTS clients and DTS servers. It also uses RPC in the protocol between a Time Server and a Time Provider. Since DTS is based on DCE RPC, which uses DCE Threads, DTS also uses Threads. DTS depends on CDS to find Time Servers and their locations. GDS may be used indirectly if a Global Time Server is registered in a foreign cell registered in the X.500 namespace. DTS uses the DCE Security Service to authenticate its interactions.

3.8.9.3.1 Standards. Table 3.8-71 presents standards for distributed timing service.

TABLE 3.8-71 Distributed timing service standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Distributed Time Service (DTS)	DCE 1.1 DTS:1994	Mandated (Approved)
CPC	IETF	Network Time Protocol (V3)	RFC 1305:1992	Mandated (Approved)
CPC	X/Open	X/Open DCE: Time Services	C310 (11/94)	Informational (Approved)
NPC	IEEE	POSIX - Part 1: Advanced Real-time System API Extension (C Language Binding)	P1003.1j	Emerging (Draft)
NPC	IEEE	POSIX - Part 1: System API Amendment: Real-Time Distributed System Communications	P1003.21	Emerging (Draft)

3.8.9.3.2 Alternative specifications. The following specification is available:

a. SAE ARD 50067 Draft: Avionics Operating System API Requirements.

3.8.9.3.3 Standards deficiencies. ISO/IEC 9945-1:1996 which incorporates IEEE 1003.1b contains time services related to high resolution real time timers, but internationalization and highly functional, system-wide clocks are beyond its scope. The IEEE P1003.1j draft standard extends the model of 1003.1b Clocks and Timers to include access to a monotonic clock and a synchronized clock; however, like 1003.1b, the actual implementation of these clocks is beyond the scope of the standard.

To date, there is no standardized API for the management of distributed time services. However, the IEEE P1003.21 working group intends to develop an API for time management serices, which would include such time management protocols as NTP and DTS.

3.8.9.3.4 Portability caveats. If the time services are to be used in building internationalized programs, portability is unlikely. Behavior is not portable across systems in which one supports the nanosecond-resolution timers specified by the SVID and Berkeley Unix. However, the IEEE P1003.1j draft standard provides applications with explicit access to a synchronized clock,

utilizing the portable standard interfaces provided in IEEE 1003.1b (incorporated in ISO 9945-1:1996).

When several applications are executed simultaneously, problems may occur when remote application components are out of time synchronization with each other. DCE takes care of this by synchronizing all the host clocks on the system through its DTS.

One component of the DTS clerk reads the clocks for a certain time interval on each of the host machines through software called the DTS server. The DTS clerk then computes the midpoint between all the time intervals to determine a new average time and resets the clocks of each host. The DTS also can read time from an outside source, such as the Universal Coordinated Time Standard through a telephone or radio, then set host clocks to this time.

3.8.9.3.5 Related standards. IEEE 1003.1b is related to this service.

3.8.9.3.6 Recommendations. Procurements should use the time services corresponding to the operating system being specified in the procurement. OSF DCE Timing should be specified for distributed systems.

3.8.9.4 Year 2000 problem/fixes. For years programmers have stored date information in "mm/dd/yy" format to conserve space in disk storage and computer memory. They adjusted computations to take the two-digit year into consideration when computing time periods, ending dates, etc. Calculations based on the year value in its two digit format are likely to yield unspecified results once the value rolls over to "00" in the year 2000. Semantics in operating system commands have been changed to allow for use of a four digit field.

3.8.9.4.1 Standards. Table 3.8-72 presents standards for the Year 2000 problem.

TABLE 3.8-72 Year 2000 problem/fixes standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Single UNIX Specification, System Interfaces and Headers, Version 2, Issue 5	C606 (2/97)	Emerging (Approved)

3.8.9.4.2 Alternative specification. There are no alternative specifications.

3.8.9.4.3 Standard deficiencies. Many current standards are unable to handle four-digit year codes. Hardware will also cause difficulties for system admistrators and chief information officers. System clocks on virtually every personal computer will wind up with corrupted dates on January 1, 2000. Some workstations, minicomputers, mainframes, elevators, and automobile central computers will fall victim to the problem. In most cases, software patches can alleviate the problem, but in some cases, the date issue can be resolved only by replacing the hardware.

3.8.9.4.4 Portability caveats. Application programs will have serious portability problems moving among platforms with different date structures.

3.8.9.4.5 Related standards. There are no standards related to the Year 2000 problem.

3.8.9.4.6 Recommendations. Organizations must get executive management to acknowledge the problem and take serious action. According to the March 1996 Computer Systems Laboratory Bulletin from NIST, the Federal Information Resources Management Policy Council (FIRMPOC) has a work group in place to identify issues and recommend actions concerning the Year 2000 problem. The group provides agencies with a definition of Year 2000 compliance and issues a recommendation on contract wording to that effect. The Office of Management and Budget has also taken an active interest in the Year 2000 problem. The Defense Information Systems Agency (DISA) Chief Information Officer (CIO) will oversee DISA's year 2000 program while the Center for Computer Systems Engineering (CFCSE) will be providing support assistance to the DOD.

Peter de Jager, a Toronto-based consultant has established the Year 2000 Information Center on the World Wide Web at "http://www.year2000.com/". Links to other articles and publications on the Year 2000 phenomenom are available at that site.

X/Open has addressed the Year 2000 problem and provided utilities to handle it in the latest release of the Single Unix Specification. X/Open is also drafting a White Paper on the subject and advises implementors to define %y such that values in the range 69-99 refer to the twentieth century and values in the range 00-68 refer to the twenty-first century. This is consistent with the touch command within the X/Open CAE specifications. Programmers are advised to use the %y field descriptor which defines year as a four digit field (ccyy). The latest version of the X/Open CAE specification denotes the interpretation of the ranges in this advice to implementors, and adds the %C specifier to the interface to denote the century.

Issue 5 of the Single UNIX Specification includes the following changes: interfaces previously defined in the ISO POSIX.2 standard; C Language Binding; Shared Memory; the addition of Threads and a Realtime Threads Feature Group to align with POSIX; Multibyte Support Extension (MSE) to align with ISO/IEC; Large File Summit (LFS) Extensions for support of 64-bit or larger files and file systems; X/Open-specific Threads extensions and dynamic linking.

3.8.10 Operating system object services. These services define the rules for creating, deleting, and managing objects.

3.8.10.1 Object request broker. (This BSA appears both in part 8 and in part 11.) The Object Request Broker (ORB) provides a mechanism for accessing objects anywhere in a distributed computing environment. It provides a method for defining objects and their interfaces. In operation, the ORB provides routing, address resolution, and authentication services, as well as parameter marshaling and conversion if necessary.

3.8.10.1.1 Standards. Table 3.8-73 presents standards for object request brokers.

TABLE 3.8-73 Object request broker standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OMG	Common Object Request Broker Architecture (CORBA) Version 2.0 (includes CORBAservices and CORBAfacilities)	CORBA 2.0:1995	Mandated (Approved)
CPC	X/Open	Common Object Request Broker: Architecture and Specification	C432 (8/94)	Informational (Approved)
CPC	X/Open	Common Object Services, Vol 1 & 2	P432/P502	Informational (Approved)
CPC	OMG	Common Object Request Broker Architecture (CORBA) Version 1.2, (Same as X/Open C432)	CORBA Specification Ver. 1.2 93-12-43	Informational (Approved)
CPC	OSF	Distributed Computing Environment (DCE)	DCE 1.1:1994	Informational (Approved)
CPC	TOG	Distributed Common Object Model/Annex X	DCOM/Annex X	Informational (Draft)
CPC	X/Open	Common Object Request Broker Architecture (CORBA), Version 1.0 (IIOP), (Same as C432 specification w/ 12.1)	P235	Informational (Superseded)

3.8.10.1.2 Alternative specifications. There are no alternative specifications available.

3.8.10.1.3 Standards deficiencies. At present, there is no independent test for conformance to any version of the CORBA specification.

CORBA 1.2 (also called CORBA 1.X) includes a standard Interface Definition Language (IDL) for defining objects. The IDL is not the same as OSF DCE Remote Procedure Call IDL, although there are similarities. CORBA 1.2 also defines a standard API for accessing ORB services, such as those needed to declare that an object is available for use, or to access an object.

CORBA 1.2 does not include a specification for interoperability between ORB's, therefore ORB's from different vendors are likely to be incompatible. This is a major feature of the new CORBA 2.0. OMG's CORBA 2.0 specification allows for two types of RPC mechanisms: (1) a mandatory General Inter-ORB Protocol (GIOP), and an optional DCE RPC protocol. ORB's that use different methods will still not be interoperable. CORBA 2.0 does not specify other types of distributed computing services (e.g. remote procedure call(RPC), security, directory, time,

threads, file system, and administration). Therefore, while CORBA 2.0 ORBs will interoperate, higher level distributed services (security, directory, etc.) may not.

CORBA requires a "mapping" of IDL into each application programming language that is used. Mappings exist for C, C++, and Smalltalk, and an Ada95 mapping is under development.

3.8.10.1.4 Portability caveats. Applications developed for one ORB are likely to be portable to a different ORB. However, the lack of interoperability specifications means that an object implemented on one ORB can usually not be accessed from a different ORB. In order to be interoperable, a system must select a single vendor's ORB for use across the enterprise.

All vendor claims for conformance to CORBA 2.0 should be matched by product demonstrations in the target environment before final contract award is made. If no such demonstration is made, serious interoperability and security problems could result, particularly in multi-vendor environments.

3.8.10.1.5 Related standards. The following standards are related to ORBs or their standards:

a. Component Integration Laboratories Inc. (CILabs):OpenDoc
b. Taligent Inc.:CommonPoint
c. Next Computer Inc.:OpenStep

3.8.10.1.6 Recommendations. Users buying distributed object technology from multiple vendors must be cautious. The use of ORB technology should be limited to pilot projects and programs with a limited number of sites. If an ORB is used, the Object Management Group (OMG) CORBA (Common Object Request Broker Architecture) Version 2.0 is recommended. The vendor must provide a plan to migrate to CORBA 2.0 with the DCE RPC as soon as possible. The vendor should also be required to state his proposed solutions to the other distributed computing services listed above, and to identify how these solutions relate to the distributed computing services already in the user's inventory.

Because of the lack of ORB interoperability, OSF DCE is the preferred solution to distributed computing requirements in the near term. OSF DCE provides the following distributed computing services: RPC, security, directory, time, threads, file system, and administration.

3.8.11 Compound document services. Compound documents are structured documents containing subdocuments of varying types of data (spreadsheets, graphics, text, etc.) and links to other documents or parts of other documents. Updating a document which has been linked into others causes the linking documents to be updated as nesessary. Compound documents are closely associated with "component software" technology, which allows for editing of parts of the compound document by that editor best suited to manipulating the type of data which it contains.

Although compound document systems usually have a strong GUI requirement, the document embedding, linking, and storage functionality which are the defining attributes of compound documents are independent of the display format.

3.8.11.1 Document linking. Document linking ensures that data stored in one document and required by another (such as financial numbers in a spreadsheet which are required in a year-end report) are always up-to-date in the second by inserting into the dependent document a pointer to the original source of the data, rather than a copy of the current value of the data.

3.8.11.1.1 Standard. Table 3.8-74 presents standards for document linking.

TABLE 3.8-74 Document linking standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	IETF	HyperText Markup Language (HTML) v.2.0	RFC 1866:1995	Informational (Approved)
CPC	CI Labs	OpenDoc	OpenDoc	Informational (Formative)

3.8.11.1.2 Alternative specification. The only other specifications are proprietary.

3.8.11.1.3 Standard deficiencies. None known.

3.8.11.1.4 Portability caveats. OpenDoc is presently available only on proprietary operating systems, but development of a reference port to Unix is ongoing.

3.8.11.1.5 Related standards. The following standards are related to document linking:

a. ISO 8879:1986 - Standard Generalized Markup Language (SGML).
b. OMG Common Object Request Broker Architecture (CORBA) ver 2.

3.8.11.1.6 Recommendations. There are no approved standards to recommend at this time.

3.8.11.2 Document embedding. Where document linking creates links between separate documents, document embedding collects data of various types into one document. This has the advantage that moving the file maintains the relationships between the contained data elements, but it requires the user to explicitly manage the consistency of data among several different copies.

3.8.11.2.1 Standard. Table 3.8-75 presents standards for document embedding.

TABLE 3.8-75 Document embedding standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.11.2.2 Alternative specification. Microsoft's proprietary specification OLE provides document embedding. Fujitsu's "Fresco" project has been submitted to the Object Management Group for consideration as an OMG specification.

3.8.11.2.3 Standard deficiencies. None known.

3.8.11.2.4 Portability caveats. OpenDoc is presently available only on proprietary operating systems, but development of a reference port to Unix is ongoing.

3.8.11.2.5 Related standards. None

3.8.11.2.6 Recommendations There are no approved standards to recommend at this time.

3.8.11.3 Compound document editing. Editing of compound documents requires careful coordination to ensure that links to other documents are maintained and that the correct data editor is used to manipulate embedded document components.

3.8.11.3.1 Standard. Table 3.8-76 presents standards for compound document editing.

TABLE 3.8-76 Compound document editing standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)

3.8.11.3.2 Alternative specification. Microsoft's proprietary specification, OLE, provides compound document editing abilities.

3.8.11.3.3 Standard deficiencies. None known.

3.8.11.3.4 Portability caveats. OpenDoc is presently available only on proprietary operating systems, but development of a reference port to Unix is ongoing.

3.8.11.3.5 Related standards. The following standards are related to compound document editing:

a. OMG Common Object Request Broker Architecture (CORBA) ver. 2.

3.8.11.3.6 Recommendations. There are no approved standards to recommend at this time.

3.8.11.4 Compound document storage. Document embedding implies a certain structure to the "container" document. Ensuring that applications which operate on compound documents can quickly and properly access the appropriate subdocuments requires agreement on this internal structure.

3.8.11.4.1 Standard. Table 3.8-77 presents standards for compound document storage.

TABLE 3.8-77 Compound document storage standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	IETF	HyperText Markup Language (HTML) v.2.0	RFC 1866:1995	Informational (Approved)
CPC	IETF	Multipurpose Internet Mail Extensions (MIME): Mechanisms for Specifying and Describing the Format of Internet Message Bodies	RFC 1521:1993	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.11.4.2 Alternative specification. Microsoft's proprietary specification, OLE, defines a compound document storage format.

3.8.11.4.3 Standard deficiencies. HTML provides for document linking only, while MIME specifies just an embedded document storage format. Unfortunately there is no standard way to combine the two specifications which provides the use with both abilities.

3.8.11.4.4 Portability caveats. OpenDoc is presently available only on proprietary operating systems, but development of a reference port to Unix is ongoing.

3.8.11.4.5 Related standards. The following specification is related to compound document storage:

a. ISO 8879:1986 - Standard Generalized Markup Language (SGML).

3.8.11.4.6 Recommendations Although MIME is listed as a "draft internet standard", it is in widespread use and has been generally accepted by the Internet community. MIME is recommended for multi-part structured document storage and exchange on those systems which require interoperability with the larger Internet community.

3.8.11.5 Compound document interoperability. The ability to access compound documents created in conformance to one specification, or on a particular operating system, by the document editors of a different specification, or by the same standard, but on a different operating system, is critical to the success of compound document technology in the workplace.

3.8.11.5.1 Standard. Table 3.8-78 presents standards for compound document interoperability.

TABLE 3.8-78 Compound document interoperability standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.11.5.2 Alternative specification. Microsoft's OLE specification makes no provision for interoperability with other compound document formats. Fujitsu's Fresco project provides facilities which allow it to interoperate with OLE documents.

3.8.11.5.3 Standard deficiencies. None known.

3.8.11.5.4 Portability caveats. OpenDoc is presently available only on proprietary operating systems, but development of a reference port to Unix is ongoing.

3.8.11.5.5 Related standards. The following standard is related to compound document interoperability:

a. OMG Common Object Request Broker Architecture (CORBA) ver. 2.

3.8.11.5.6 Recommendations. There are no approved standards to recommend at this time.

3.8.12 Portable device driver environment. Operating systems access I/O devices through the use of device-specific software modules called device drivers. Device driver interface standards limit the interaction between a device driver and the rest of the system (i.e. the operating system, the applications, the processor architecture, and the interconnecting busses and/or channels) to well-defined interfaces. This enables highly portable device drivers to be developed independent of the target platform, operating system, or interconnect scheme. For commercial systems, where device drivers are written by Independent Hardware Vendors (IHVs), this permits a single driver, delivered with a hardware board or device, to be utilized in whatever system the device is installed by the end user. In military systems, many devices are not off-the-shelf, but are highly specialized and developed specifically for the military market; more often than not, the burden of device driver development falls on the application developer, because the device vendor has neither the resources nor the market to supply device drivers for all possible targets; the ability to develop and maintain a single portable driver, whether written by the device vendor or the application developer, clearly reduces the cost of supporting the device.

Device driver code is typically quite complex; the complexity of device driver design and coding often strongly affects the overall performance of a system. Further, the consequences of bugs in device drivers are far more severe than those of bugs in applications programs: device drivers run with much greater privilege, directly manipulate hardware resources, and often must comply with severe time constraints. Historically, drivers have needed to be modified for each hardware platform and operating system version; also, driver updates are frequently required to provide new capabilities or to utilize hardware upgrades. Given their complexity, this becomes a considerable maintenance burden requiring significant development resources. As the number of devices, operating systems, and platforms grows dramatically, as is the trend today, the number of different device drivers becomes unmanageable. Portable device driver interface standards are a way to reduce this burden, resulting in a one device - one driver approach which allows developer resources to be devoted to quality of implementation, not quantity of drivers.

Portable interfaces for device drivers must allow any application request for an I/O action (open, close, read, write, control, status, synchronous, asynchronous, synchronized, etc.) to be honored by the appropriate driver; for a driver to deal with multiple applications contending for the same device; for both programmed and Direct Memory Access data transfers between the device and the application's data area; for servicing hardware interrupts; and for a driver to implement a layer of protocol between a higher level driver (or the application) and a lower level driver (or hardware entity). Yet, the interfaces must remain operating system neutral in spite of variations in the underlying OS memory management, synchronization models, kernel premptibility, multi-threading, and dynamic loading capabilities. Likewise, the interfaces must remain platform neutral in the presence of proprietary I/O busses, cached and buffered I/O data paths, alignment constraints, mixed byte ordering, and variations in processor I/O and interrupt architecture.

Currently, the only known effort which meets these criteria is Project UDI (Uniform Driver Interface), initiated by a multi-vendor working group comprised of several systems vendors and IHVs. This group first documented a set of 40 functional requirements for an environment to support portable device drivers, then prepared a specification of the interfaces between such an environment and the device drivers themselves. In addition, the group conceived a Metalanguage

concept to account for special interfaces from application to driver or between drivers for each specific class of device (e.g. all pointer devices might require a special calibrate interface, while all removable media devices might require an unload/eject interface); a number of standard Metalanguages, and their associated interface specifications, were developed by the UDI group. Having specified a draft UDI environment and set of standard Metalanguages, the group has embarked on an aggressive prototyping effort designed to demonstrate proof-of-concept and to further refine the specifications. It is anticipated that this prototyping effort will lead to wide-spread industry adoption of UDI technology and inclusion of UDI compliant environments and drivers in future product releases. The de-facto industry standard based on the UDI specifications will then be ready to be turned into a national and/or international standard through an IEEE (or similar) standards process.

The UDI specifications have been developed largely based on the UDI group's knowledge of the commonly supported and marketed device classes in the commercial sector, and therefore may not provide all necessary interfaces to support either specialized military devices and interconnects, or newer industry standards and draft standards for devices and interconnects.

The UDI specifications are sufficiently complete to support core driver functionality for standard commercial device classes; however, there are several known deficiencies which will be resolved as the UDI Group completes their prototyping efforts and completes Rev. 1.0. However, any such standard can address only those platform, interconnect, and device capabilities known to the members of the developing group; therefore it is recommended that organizations expecting to use this standard participate in its formative stages, and ensure that any unique requirements are identified and technical solutions proposed. This process has already begun for Fibre Channel and Scalable Coherent Interface, and should be extended to address any other new I/O technologies which might not be supported by the current draft specification. This recommendation particularly extends to standard UDI Metalanguages (device class specific interfaces) for unique devices which are conceptually quite different from common commercially available devices.

The UDI Group's major participants are

Adaptec, Inc.;
Digital Equipment Corporation;
Hewlett-Packard Company;
Interphase Corporation;
Novell, Inc.;
The Santa Cruz Operation, Inc.; and
Sun Microsystems, Inc.

Two other standardization efforts are often considered device driver interface standards: Microsoft's Plug and Play and another industry group's Intelligent Input/Output (I2O) specification. Plug and Play, while it does specify device driver interfaces, is a hybrid (cooperating hardware and software) solution to an entirely different problem, that of making devices self-identifying and automatically configurable; it does not supportportability of device drivers across operating systems or platforms. I2O, on the other hand, does address the driver

portability problem, but provides a hybrid hardware/software solution which allows a portion of each device driver (the part which specifically manipulates the device hardware) to be written portably, provided that this part is executed by a standard I/O processor chip which communicates (via message passing) with the operating specific portion of the driver; introduction of this additional processor requires that the I2O specification standardize not only the device driver interfaces, but also the IOP hardware architecture, transport protocols between host and IOPs, transport driver interfaces, message protocol over the transport, and initialization and configuration of the IOP itself. The UDI group feels that both efforts will benefit from exploiting the inherent synergy between the two groups, and should work jointly toward a truly universal device driver standard. To this end, they have begun to map out several models which would support both standards working together.

The I2O specification is not available to non-members of the I2O Special Interest Group without signing of a non-disclosure agreement and payment of a fee. Because of this, the I2O specification cannot reasonably be considered a standard suitable for open systems. Perhaps when the I2O and UDI groups begin to work toward a common specification, this restriction will be lifted.

The following BSAs outline the interfaces and functionality that various kinds of device drivers will require from a portable device driver environment.

3.8.12.1 Multi-threading. Since driver-to-environment interfaces are typically invoked from the operating system kernel, it is important that such interfaces relinquish the processor whenever the associated operation cannot be completed immediately, then regain control and continue when that operation is later completed. A driver may have several logical threads of execution pending simultaneously. Each such thread may be awaiting a different resource or event and in some stage of completion, and each such thread generally needs a separate data area associated with the operation being performed. Unfortunately, a dynamic memory allocation operation itself may need to await sufficient memory resources. Multi-threading services provide, upon entry to a driver function, adequate storage for a single service request to be queued, and additional services for a driver to regain control once an operation has been initiated (but not necessarily completed), to be notified when an operation has been completed, and to obtain more storage to be used for subsequent concurrent service requests. Also, services to free storage allocated for a thread of execution, and to support cancellation of pending service requests are provided.

3.8.12.1.1 Standards. Table 3.8-79 presents standards for multi-threading.

TABLE 3.8-79 Multi-threading standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	UDI Group	Uniform Driver Interface (UDI) Specification	UDI Rev 0.75	Informational (Forming)

3.8.12.1.2 Alternative specification. Predecessors to UDI technology have been developed by several of the UDI Group's member companies, and serve to partially solve the device driver

portability problem within the domain of each vendor's operating system and hardware architecture support. Most notably, Sun Microsystems' Solaris Driver Device Interface/Driver Kernel Interface (DDI/DKI), Novell's Unixware Portable Device Interface (PDI), and DEC's OSF/1 processor abstraction interfaces served as starting points for the development of UDI technology. The API specifications for these solutions are published as part of each vendor's operating system documentation set. Although these specifications surely support multi-threaded driver code, and most of the other BSAs, none constitutes a comprehensive open-systems portability solution across the various operating systems; this is the goal of UDI.

3.8.12.1.3 Standard deficiencies. Rules for freeing a previously freed token are not yet specified.

3.8.12.1.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.1.5 Related standards. None for this service area.

3.8.12.1.6 Recommendations. UDI is recommended because it provides these services, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.2 Buffer management. Drivers typically require intermediate user data buffers to carry the line data between an application and the underlying device. Such buffers are considered logically contiguous, but may be virtually and physically segmented. Buffer management services provide for allocation and deallocation of such buffers from a pool common to all drivers, for writing to, reading from, and copying these buffers, for determining buffer constraints, and for segmentation and reassembly of buffers in support of networking protocols.

3.8.12.2.1 Standards. Table 3.8-80 presents standards for buffer management.

TABLE 3.8-80 Buffer management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.2.2 Alternative specification. Sun Microsystems' DDI/DKI, Novell's Unixware PDI, and DEC's OSF/1 processor abstraction interfaces.

3.8.12.2.3 Standard deficiencies. Buffer constraints interfaces are incomplete in UDI version 0.75. Buffer segmentation/reassembly interfaces are proposed in UDI version 0.75. Insufficient UDI usage base to rule out other deficiencies.

3.8.12.2.4 Portability caveats. Insufficient usage base to assess.

3.8.12.2.5 Related standards. None for this service area.

3.8.12.2.6 Recommendations. UDI is recommended because it provides these services, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.3 Device driver memory management. In addition to buffers, drivers often require dynamic allocation of virtually contiguous memory. Since drivers do not necessarily run in the context of an operating system process, the language specific management primitives (e.g. malloc/free or new/delete) cannot be used. Memory management services allow a driver to allocate and free memory, and to discover the memory allocation limits of the system.

3.8.12.3.1 Standards. Table 3.8-81 presents standards for device driver memory management.

TABLE 3.8-81 Device driver memory management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.3.2 Alternative specification. Sun Microsystems' DDI/DKI, Novell's Unixware PDI, and DEC's OSF/1 processor abstraction interfaces.

3.8.12.3.3 Standard deficiencies. A separate interface to allocate movable structures has not yet been defined. The maximum guaranteed size for an allocation request needs to be revisited. A memory allocation interface which accepts minimum, maximum, and granularity values still needs to be provided.

3.8.12.3.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.3.5 Related standards. The following standards are related to device driver memory management standards:

a. IEEE P1003.1j: Realtime Extension to POSIX (memory Management)
b. ISO 8652:1995: Programming Languages - Ada (allocators)
c. ISO/IEC 9899: Programming Languages - C (malloc/calloc/realloc/free)
d. ANSI X3J16 WG21/N0678: Programming Languages - C++ (new/delete)

3.8.12.3.6 Recommendations. UDI is recommended because it provides these services, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.4 Programmed I/O. A driver which actually controls a device must read and write various control and status registers, FIFOs, and dual-ported memory implemented by that device in hardware. In the Programmed I/O (PIO) model, the processor directs data between the device and memory or buffers; the device is simply commanded by the processor to accept or provide the requested data. There may be constraints on the atomicity of device data accesses, so 8-bit, 16-bit, and 32-bit (and possibly 64-bit) transfers must be supported. Programmed I/O services allow the driver to obtain a handle for a specific device, to determine the atomicity supported by the device (and intervening bus bridges), and to transfer data to and from the device, either an atom at a time or in blocks.

3.8.12.4.1 Standards. Table 3.8-82 presents standards for programmed I/O.

TABLE 3.8-82 Programmed I/O standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.4.2 Alternative specification. Sun Microsystems' DDI/DKI, Novell's Unixware PDI, and DEC's OSF/1 processor abstraction interfaces.

3.8.12.4.3 Standard deficiencies. PIO accesses may fail and need to return status, but currently do not support asynchronous return of such status; this needs to be resolved. Peer to peer PIO issues need to be resolved. PIO interfaces to access hardware that may not be responding on the bus (for initial and diagnostic probing) are still not defined.

The UDI specifications have been developed largely based on the UDI group's knowledge of the commonly supported and marketed device classes in the commercial sector, and therefore may not provide all necessary interfaces to support either specialized military devices and interconnects, or newer industry standards and draft standards for devices and interconnects.

3.8.12.4.4 Portability caveats. Insufficient UDI usage base to fully assess.

UDI achieves portability by specifying an environment which shields device drivers from the specifics of the target operating system, processor, and hardware I/O interface. Such an environment must be implemented and re-implemented for each combination of target platform, operating system, and interconnect scheme (bus architecture) intended to support UDI conforming portable device drivers. Because system and device vendors have a considerable investment in native device drivers for existing systems, implementations of such an environment must co-exist and cooperate with these existing drivers, and permit a phased transition to completely UDI-based drivers; the old driver environments may need to be supported indefinitely. To simplify this co-existence, system vendors may choose to implement the UDI environment as a shell on top of the older, system specific environment; users should be aware of the performance

degradation to be expected with such a layered implementation, and encourage system vendors to integrate the UDI environment more fully into their operating systems as soon as possible.

Even in a system where UDI has been bound as efficiently as possible to the hardware and operating system, users must be aware that portability almost always imposes some performance penalty; the UDI interfaces are portable replacements for down-and-dirty use of specific hardware capabilities such as memory mapped device registers, interrupt masking, mutual-exclusion primitives (test-and-set instructions), I/O channel commands, and DMA controllers. Just as we have grown to accept a modest performance penalty to use a High Order Language to gain portability over hand optimized assembly code, so we must understand and accept the price of device driver portability. Although UDI interfaces have been designed to allow implementation performance to be optimized to the greatest extent possible, it is still likely that UDI conforming drivers will underperform system-specific drivers. This is not a bad thing, just another engineering tradeoff which must be considered by system engineers.

3.8.12.4.5 Related standards. The following standard is related to device driver programmed I/O standards:

a. IEEE 1212:1991: IEEE Standard for CSR Architecture

3.8.12.4.6 Recommendations. UDI is recommended because it provides these services, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.5 Direct Memory Access. Some devices are capable of Direct Memory Access (DMA). Such devices are capable of independently directing the transfer of data between the device and memory without processor intervention. However, prior to such transfers, the processor must set up pathways and configure resources to make the DMA possible, and then pass information (an address and a length, or a scatter-gather structure) to the device so that the device knows the intended memory origin or destination of the data. The manner in which this is done, and the device's constraints on size, alignment, scatter-gather structure format, and other attributes of DMA transfers vary from device to device. Direct Memory Access services allow the driver to discover the DMA constraints, to bind/unbind buffers to DMA resources, and to deal efficiently with inbound data whose length and structure may not be known apriori. The actual notification to the device to begin a DMA transfer is a Programmed I/O operation, although the device may access control information (scatter-gather lists, etc.) via a DMA mechanism.

3.8.12.5.1 Standards. Table 3.8-83 presents standards for direct memory access.

TABLE 3.8-83 Direct Memory Access standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.5.2 Alternative specification. Sun Microsystems' DDI/DKI, Novell's Unixware PDI, and DEC's OSF/1 processor abstraction interfaces.

3.8.12.5.3 Standard deficiencies. Peer to peer DMA issues need to be resolved.

The UDI specifications have been developed largely based on the UDI group's knowledge of the commonly supported and marketed device classes in the commercial sector, and therefore may not provide all necessary interfaces to support either specialized military devices and interconnects, or newer industry standards and draft standards for devices and interconnects.

3.8.12.5.4 Portability caveats. Insufficient UDI usage base to assess. See Programmed I/O BSA for portability vs. performance concerns.

3.8.12.5.5 Related standards. The following standards are related to device driver Direct Memory Access standards:

a. IEEE 1212.1:1993: IEEE Std. for CSR Architecture (DMA Framework)
b. IEEE P1285: IEEE Draft Standard for Scalable Storage Interface (S2I)

3.8.12.5.6 Recommendations. UDI is recommended because it provides these services, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.6 Device driver time management. Drivers often need to perform an operation periodically (e.g. polling a device not capable of signaling I/O completion via an interrupt) or after a delay (e.g. to deal with timing characteristics of a device, or for establishing a timeout for device response). A driver thread therefore may require waiting for a time-related event rather than (or in addition to) a resource or device related event (i.e. interrupt). Since drivers do not necessarily run in the context of an operating system process, portable application level timer primitives cannot be used. Time management services provide for an abstract notion of time (including conversion to/from microseconds and discovering supported resolution), starting a one-shot or periodic timer, notification of timer expiration, and canceling a pending timer.

3.8.12.6.1 Standards. Table 3.8-84 presents standards for device driver time management.

TABLE 3.8-84 Device driver time management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.6.2 Alternative specification. Sun Microsystems' DDI/DKI, Novell's Unixware PDI, and DEC's OSF/1 processor abstraction interfaces.

3.8.12.6.3 Standard deficiencies. None currently identified for this service area.

3.8.12.6.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.6.5 Related standards. None for this service area.

3.8.12.6.6 Recommendations. UDI is recommended because it provides these services, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.7 Device node management. Before an application can use (i.e. open) a device, it must be able to locate that device by some logical name, determine if the device exists, and determine the device's status and attributes; it is the driver's responsibility to register this information in a device tree (a database), and the environment's responsibility to associate open devices with the correct driver. Device node management services allow each driver to participate in the building of a device tree, and both drivers and applications to search the tree and query attributes and status of devices.

3.8.12.7.1 Standards. Table 3.8-85 presents standards for device node management.

TABLE 3.8-85 Device node management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.7.2 Alternative specification. Sun Microsystems' DDI/DKI, Novell's Unixware PDI, and DEC's OSF/1 processor abstraction interfaces.

3.8.12.7.3 Standard deficiencies. Standard attributes have not yet been defined. Interface for searching for a device tree node is still under investigation. Bus/interconnect probe interfaces (to help build the device tree) have not yet been defined.

3.8.12.7.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.7.5 Related standards. None for this service area.

3.8.12.7.6 Recommendations. UDI is recommended because it provides these services, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.8 Mutual exclusion. In drivers which support concurrent execution of multiple threads of execution, it is essential that access to resources shared among such threads, such as buffers and flags, be synchronized to prevent race conditions. Most drivers must support at least two concurrent threads, for example a read operation and an interrupt handler. Since drivers do not necessarily run in the context of an operating system process, portable application level mutual exclusion primitives cannot be used. Mutual exclusion services ensure that two threads of driver execution can each guarantee that certain sections of code in one thread cannot be pre-empted by certain sections in the other.

3.8.12.8.1 Standards. Table 3.8-86 presents standards for mutual exclusion.

TABLE 3.8-86 Mutual exclusion standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.8.2 Alternative specification. Sun Microsystems' DDI/DKI, Novell's Unixware PDI, and DEC's OSF/1 processor abstraction interfaces.

3.8.12.8.3 Standard deficiencies. None currently identified for this service area.

3.8.12.8.4 Portability caveats. Insufficient UDI usage base to assess. See Programmed I/O BSA for portability vs. performance concerns.

3.8.12.8.5 Related standards. The following standards are related to device driver mutual exclusion standards:

a. IEEE 1003.1b:1993: Realtime extension to POSIX (semaphores)
b. IEEE 1003.1c:1995: Threads Extension to POSIX (mutexes)

3.8.12.8.6 Recommendations. UDI is recommended because it provides these services, promises to be an open-systems solution a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.9 Tracing and logging. An operating system with which device drivers co-exist typically provides tracing and logging facilities as part of an overall fault isolation strategy; drivers are expected to support this strategy. Logging simply requires that a driver record unusual occurrences which may affect functionality of the driver, device, or subsystems using the driver. Tracing requires on-demand recording of sufficient information to reconstruct a logical sequence of events within the driver, and is controlled by an external operating system unique trace facility. Tracing and logging services allow drivers to participate, in a portable fashion, in the operating system's unique tracing and logging activities. Interfaces to write trace and log data, and to respond to trace facility requests are provided.

3.8.12.9.1 Standards. Table 3.8-87 presents standards for tracing and logging.

TABLE 3.8-87 Tracing and logging standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.9.2 Alternative specification. No other consortia or de facto specifications are available.

3.8.12.9.3 Standard deficiencies. These interfaces are defined, but still under investigation.

3.8.12.9.4 Portability caveats. Insufficient UDI usage to assess.

3.8.12.9.5 Related standards. The following standard is related to device driver tracing and logging standards:

a. IEEE 1003.1b SRASS Amendment to POSIX

3.8.12.9.6 Recommendations. UDI is recommended because it provides these services, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.10 Inter-module communication. Often, the apparent functionality of a device is implemented by several cooperating drivers; since such drivers may not be able to share memory or synchronize access to shared resources, a loosely coupled form of inter- module communication is necessary. Since drivers do not necessarily run in the context of an operating system process, portable application level IPC primitives cannot be used. Inter-module communication services allow a driver to establish a connection to another driver through which that driver's services may be invoked just as if invoked directly by the environment on behalf of an application. For higher performance, cooperating drivers may also utilize shared memory when supported; therefore, inter-module communication services should also allow a driver to share memory with other drivers, and synchronize access to that shared memory.

3.8.12.10.1 Standards. Table 3.8-88 presents standards for inter-module communication.

TABLE 3.8-88 Inter-module communication standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.10.2 Alternative specification. Sun Microsystems' DDI/DKI, Novell's Unixware PDI, and DEC's OSF/1 processor abstraction interfaces.

3.8.12.10.3 Standard deficiencies. Shared memory interfaces are not currently specified.

3.8.12.10.4 Portability caveats. Insufficient UDI usage base to assess. See Programmed I/O BSA for portability vs. performance concerns.

3.8.12.10.5 Related standards. The following standard is related to device driver inter-module communication standards:

a. ISO/IEC 9945-1:1996: POSIX System API

3.8.12.10.6 Recommendations. UDI is recommended because it provides these services, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.11 Locking protocol. Drivers normally receive requests and provide responses to either a higher level driver, or the application (via the portable driver environment). The motivation for driver locking is to temporarily give control of an I/O driver to an outside subsystem (e.g. diagnostics, configuration) other than the driver's normal higher driver, for the purpose of allowing the outside subsystem to perform an undisturbed sequence of operations (requests) on the driver. While a driver is locked, its normal flow of requests from its higher driver is suspended. Normal requests are queued up, and will be processed after the driver is unlocked. Locking protocol services allow the outside subsystem to lock and unlock the driver, and if the lock will be disruptive (i.e. the outside subsystem's request cannot be transparently interleaved with normal traffic), to reset the driver to a known state and have it recover or propagate a failure/retry status to its normal user.

3.8.12.11.1 Standards. Table 3.8-89 presents standards for locking protocol.

TABLE 3.8-89 Locking protocol standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPE	UDI Group	Uniform Driver Interface (UDI) Specification	UDI Rev 0.95	Information (Permissive)

3.8.12.11.2 Alternative specification. No other consortia or de facto specifications are available.

3.8.12.11.3 Standard deficiencies. These interfaces are sketched out in concept, but still under investigation and not yet defined.

3.8.12.11.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.11.5 Related standards. None for this service area.

3.8.12.11.6 Recommendations. UDI is recommended because it plans to provide these services, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.12 Powerfail recovery. If power is lost to a peripheral and/or the main processor, but memory has been preserved, it is desirable that either I/O operations that were in progress when power failure occurred be restarted or completed; failing that, applications or higher level drivers (which may themselves have been recovered by the overall powerfail recovery strategy of the operating system) should be notified of I/O failure. Powerfail recovery services allow a driver to request notification of powerfail and poweron warning events so that it may recover if possible, or notify higher levels of a failure if not.

3.8.12.12.1 Standards. Table 3.8-90 presents standards for powerfail recovery.

TABLE 3.8-90 Powerfail recovery standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
EPC	UDI Group	Uniform Driver Interface (UDI) Specification	UDI Rev 0.75	Informational (Emerging)

3.8.12.12.2 Alternative specification. No other consortia or de facto specifications are available.

3.8.12.12.3 Standard deficiencies. These interfaces are defined, but still under investigation.

3.8.12.12.4 Portability caveats. Insufficient UDI usage to assess.

3.8.12.12.5 Related standards. None for this service area.

3.8.12.12.6 Recommendations. UDI is recommended because it provides these services, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.13 Management metalanguage. A portable driver environment, in the process of building up or tearing down a pathway from an application (or outside subsystem) through one or more drivers to a device, must pass management requests to the drivers involved. A management metalanguage defines service interfaces to drivers for initialization, binding to other drivers, unbinding, and diagnostics.

3.8.12.13.1 Standards. Table 3.8-91 presents standards for management metalanguage.

TABLE 3.8-91 Management metalanguage standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.13.2 Alternative specification. The UNIX System V (SVID) specification defines a STREAMS capability for establishing a data/control pathway through several drivers to a device.

3.8.12.13.3 Standard deficiencies. System management and diagnostic portions of this metalanguage are incomplete/proposed.

3.8.12.13.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.13.5 Related standards. None for this service area.

3.8.12.13.6 Recommendations. UDI is recommended because it defines these interfaces, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.14 Bus bridge metalanguage. A driver often must access its corresponding hardware device indirectly via a bus bridge. Requests from the device driver to the bus bridge driver and from the bus bridge driver to the device driver are required to perform initial binding of the drivers, as well as to set up and process notification (to the device driver) of device interrupts via the bus bridge driver. A bus bridge metalanguage defines service interfaces for binding and interrupt registration operations invoked on a bridge driver by a device driver, binding and interrupt registration operations invoked on a device driver by a bridge driver, interrupt notification invoked on a device driver by a bridge driver, and interrupt acknowledgment invoked on a bridge driver by a device driver. Interrupt handlers should be capable of running in either a restricted context (faster, low latency), or a general context (slower, but no restrictions on services available).

3.8.12.14.1 Standards. Table 3.8-92 presents standards for bus bridge metalanguage.

TABLE 3.8-92 Bus bridge metalanguage standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	UDI Group	Uniform Driver Interface (UDI) Specification	UDI Rev 0.75	Information (Permissive)

3.8.12.14.2 Alternative specification. No other consortia or de facto specifications are available.

3.8.12.14.3 Standard deficiencies. The binding operations of this metalanguage are not yet specified.

3.8.12.14.4 Portability caveats. Insufficient UDI usage base to assess

3.8.12.14.5 Related standards. None for this service area.

3.8.12.14.6 Recommendations. UDI is recommended because it defines these interfaces, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.15 SCSI metalanguage. For SCSI devices, a device driver is known as a SCSI peripheral driver (PD), while the bus bridge driver is known as a SCSI HBA driver (HD). Requests from the PD to HD and from the HD to PD are required to perform initial binding of the drivers, to set up and process asynchronous event notification, as well as to perform various SCSI control and I/O requests. A SCSI metalanguage defines PD to HD interfaces to request a service from the HBA driver, acknowledge an event from the HBA driver, or bind to the HBA driver; and HD to PD interfaces to return response information, notify the PD of an asynchronous event, or acknowledge a binding request.

3.8.12.15.1 Standards. Table 3.8-93 presents standards for metalanguage.

TABLE 3.8-93 SCSI metalanguage standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	UDI Group	Uniform Device Interface (UDI) Specification	UDI Rev 0.97	Information Only (Emerging)

3.8.12.15.2 Alternative specification. No other consortia or de facto specifications are available.

3.8.12.15.3 Standard deficiencies. While this metalanguage is substantially completely defined, some unresolved issues still exist.

3.8.12.15.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.15.5 Related standards. The following standard is related to device driver SCSI metalanguage standards:

a. ANSI X3T9.2 792D: Draft Common Access Method, Transport and SCSI Interface Module

3.8.12.15.6 Recommendations. UDI is recommended because it defines these interfaces, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.16 Network adapter metalanguage. The portable driver environment needs to define a framework that provides interfaces necessary to write a networking driver that works with existing and future networking protocol stacks regardless of the OS and protocol stack characteristics. The framework must support a universal set of network-related functions that provide all of the needed functionality in an OS, protocol, and transport independent manner. A network adapter metalanguage defines services to support network addressing, network control operations such as hardware MAC address registration, connection oriented operations, and connectionless operations.

3.8.12.16.1 Standards. Table 3.8-94 presents standards for network adapter metalanguage.

TABLE 3.8-94 Network adapter metalanguage standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.16.2 Alternative specification. UNIX System V (SVID) based operating systems define a STREAMS interface among network protocol layer drivers. The STREAMS Data Link Provider Interface (DLPI) forms the basis for this UDI metalanguage.

3.8.12.16.3 Standard deficiencies. None currently identified for this service area.

3.8.12.16.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.16.5 Related standards. The following standards are related to device driver network adapter metalanguage standards:

a. IEEE P1003.1g: POSIX Protocol Independent Network Interface
b. IEEE Std. 802.*: Numerous IEEE standards for network access methods
c. IEEE Std. 1596:1992: Scalable Coherent Interface

3.8.12.16.6 Recommendations. UDI is recommended because it defines these interfaces, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.17 Pointer metalanguage. Drivers for the class of pointer devices have the need to process and communicate 1, 2, or 3 dimensional position information and state changes of up to 4 buttons to the higher level driver (or the application, via the portable driver environment). Upon initial binding, the driver must disclose the number of buttons and number of dimensions. In normal operation, the driver must report position and button status asynchronously whenever one of these changes. A pointer metalanguage defines service interfaces for binding and unbinding to the pointer device driver, and for the device driver to asynchronously notify a higher level whenever the pointer device state changes.

3.8.12.17.1 Standards. Table 3.8-95 presents standards for pointer metalanguage.

TABLE 3.8-95 Pointer metalanguage standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPE	DII Comp	Unified Driver Interface (UDI) Specification	UDI Ver 0.95	Mandated (Emerging)

3.8.12.17.2 Alternative specification. No other consortia or de facto specifications are available.

3.8.12.17.3 Standard deficiencies. None currently identified for this service area.

3.8.12.17.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.17.5 Related standards. None for this service area.

3.8.12.17.6 Recommendations. UDI is recommended because it defines these interfaces, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.18 Storage metalanguage. Drivers for the class of mass storage devices need to deal with the random access, block oriented storage characteristics of such devices, and the fact that such devices often have internal buffers and smart controllers which can re-order I/O operations to optimize performance. A storage metalanguages defines service interfaces (as yet unspecified) which support the unique capabilities of this class of devices.

3.8.12.18.1 Standards. Table 3.8-96 presents standards for storage metalanguage.

TABLE 3.8-96 Storage metalanguage standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.18.2 Alternative specification. No other consortia or de facto specifications are available.

3.8.12.18.3 Standard deficiencies. A storage metalanguage is not yet included in the UDI specification.

3.8.12.18.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.18.5 Related standards. The following standard is related to device driver storage metalanguage standards:

a. IEEE P1285: Draft Standard for Scalable Storage Interface (S2I)

3.8.12.18.6 Recommendations. UDI is recommended because it will define these interfaces, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.19 Framework for custom metalanguages. Standard metalanguages address the specific capabilities of the most common device classes, and the communication among commonly stacked drivers. Device vendors and system developers will always be defining new device classes and intra-driver protocols, for which no standard metalanguage will suffice. Just as with the contentious POSIX issue of application level APIs for control of arbitrary devices, a device driver standard must provide a framework by which custom metalanguages can be integrated into the environment, even though the specific interfaces and arguments cannot be predicted when the environment is built. A framework for custom metalanguages provides the extensibility necessary so that new and unusual devices and protocols, with unique command, acknowledgment, and status requirements, can be supported; ultimately, such custom metalanguages may be transitioned to standard metalanguages based on their widespread adoption.

3.8.12.19.1 Standards. Table 3.8-97 presents standards for framework for custom metalanguages.

TABLE 3.8-97 Framework for custom metalanguages standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	UDI Group	Uniform Driver Interface (UDI) Specification	UDI Rev 0.75	Informational (Formative)

3.8.12.19.2 Alternative specification. No other consortia or de facto specifications are available.

3.8.12.19.3 Standard deficiencies. A framework for custom metalanguages is not yet included in the UDI specification.

3.8.12.19.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.19.5 Related standards. The following standard is related to device driver framework for custom metalanguage standards:

a. IEEE P1003.1d: Realtime Amendment to POSIX (device control)

3.8.12.19.6 Recommendations. UDI is recommended because it will define such a framework, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.20 Versioning. Drivers must indicate the version of a standard to which they conform, so that the environment can enforce conformance to the specific set of interfaces documented in the appropriate standard. The environment must be able to simultaneously support drivers which conform to multiple versions of the standard. Versioning services provide the necessary interfaces for the environment to query a driver for the version to which it conforms.

3.8.12.20.1 Standards. Table 3.8-98 presents standards for versioning.

TABLE 3.8-98 Versioning standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.8.12.20.2 Alternative specification. No other consortia or de facto specifications are available.

3.8.12.20.3 Standard deficiencies. Versioning capabilities are not yet included in the UDI specification.

3.8.12.20.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.20.5 Related standards. None for this service area.

3.8.12.20.6 Recommendations. UDI is recommended because it will define these interfaces, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

3.8.12.21 Packaging and distribution format. To achieve driver portability without requiring that driver vendors distribute source code, a driver binary must be built from source code conforming to the interface standards, and written onto media in some common distribution format. The environment must be able to link with these binaries. Packaging and distribution format standards should support multiple media format types to allow for systems which do not support particular media types, multiple drivers on a particular piece of media, and well-accepted common formats across all media types.

3.8.12.21.1 Standards. Table 3.8-99 presents standards for packaging and distribution format.

TABLE 3.8-99 Packaging and distribution format standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	UDI Group	Uniform Driver Interface (UDI) Specification	UDI Rev 0.75	Emerging (Emerging)

3.8.12.21.2 Alternative specification. No other consortia or de facto specifications are available.

3.8.12.21.3 Standard deficiencies. Packaging and distribution formats are not yet included in the UDI specification.

3.8.12.21.4 Portability caveats. Insufficient UDI usage base to assess.

3.8.12.21.5 Related standards. None for this service area.

3.8.12.21.6 Recommendations. UDI is recommended because it will define these formats, promises to be an open-systems solution to a major software portability problem, and is being developed by, and backed by, a substantial portion of the computer industry.

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 9 of 14 parts)

SYSTEM MANAGEMENT SERVICES

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

TABLE OF CONTENTS

LIST OF TABLES

3.9 System management services. Centralized system management services refer to services that allow systems and/or enterprises to be managed from a single, centralized point. Distributed system management services refer to services that allow systems and/or enterprises to be managed from any node in the enterprise, in a variety of ways. In some cases an enterprise may be managed as a single unit, but management tasks can be performed at any node. In other cases, the enterprise may be split into multiple domains, each having its own management system, but the different management systems can cooperate with each other and exchange and use each others' management information.

3.9.1 State management. This requirement states the need for a mechanism that initializes the system or components of the system, to a pre-determined state where it can operate in the distributed environment. Also required is the ability to shutdown all or part of the system gracefully for maintenance, security, or component upgrade reasons. Complementing startup, the ability to suspend, synchronize, or shutdown is also required. A less invasive mechanism of enroll/disenroll is needed to allow a component to be recognized or excluded from the distributed system while not directly affecting its operation.

3.9.1.1 Independent window management services. (This BSA appears both in part 3 and part 9.) Window management services are a necessary part of any windows system to perform functions such as resizing or moving windows. These services are not to be confused with services managing individual windows as though they were separate terminals.

3.9.1.1.1 Standards. Table 3.9-1 presents standards for independent window management services.

TABLE 3.9-1 Independent window management services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	Modular Toolkit Environment (MTE)	1295:1993	Informational (Approved)
CPC	OSF	Motif	Motif 1.2	Informational (Approved)
CPC	MIT X Consortium	X Window System (Tab Window Manager)	X11R5	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)

Motif 1.2 is the current version of the OSF specification for GUI behavior and appearance and programming and data interfaces. X11R5 is the current release of Version 11 of the X Windows GUI standard. The IBM Presentation Manager is included to support legacy systems.

3.9.1.1.2 Alternative specifications. The following specifications are also available for legacy support:

a. APIW

b. USL/Sun Open Look Windows Manager (olwm)
c. IBM SAA Presentation Manager Window Manager.

3.9.1.1.3 Standards deficiencies. Although all window managers perform functions such as window resizing and moving (window manipulation), some do not manage their windows independently, as if each window were a separate system. Failure to manage windows independently may create situations in which an application seizing in one window may propagate the errors to other windows causing them to seize (lock up). In addition, without an independent window manager, usually it is not possible to invoke programs that run in graphical mode at the same time (but in different windows on the same screen) as programs running in character mode. Certain windows systems running under single-tasking DOS also do not support independent window managers.

Motif 2.0 is somewhat incompatible with the multi-threading implementation in X11R6.

As no significant products are as yet available for Motif 2.0, the previous version, Motif 1.2, remains as the reference standard. Adoption of Motif 2.0 will be delayed until an appropriate threshold of Motif 2.0 products are available and until resolution of potential conflicts between Motif 2.0 and X11R6.

3.9.1.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.9.1.1.5 Related standards. No standards are related to independent window management standards.

3.9.1.1.6 Recommendations. A procurement should specify a Windows Manager that accommodates window manipulation and application seizure protection. Windows systems using X Windows operating on protected operating systems like UNIX are more robust (i.e., the failure of one application will not cause other applications to fail automatically) than some running on the unprotected DOS operating system.

3.9.1.2 System startup and shutdown. System startup and shutdown refers to a standardized method for starting up and gracefully shutting down a system without losing or corrupting data or code, and in the case of a multiuser system, giving users advance notification of the shutdown so that they can save their files and log off the system in time.

3.9.1.2.1 Standards. Table 3.9-2 presents standards for system startup and shutdown.

TABLE 3.9-2 System startup and shutdown standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.9.1.2.2 Alternative specifications. The following specifications are also available:

a. Berkeley BSD 4.3 UNIX.
b. System V Release 4.

3.9.1.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.9.1.2.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.9.1.2.5 Related standards. No standards are related to system startup and shutdown standards.

3.9.1.2.6 Recommendations. No specific standards are recommended at this time.

3.9.1.3 Batch scheduling. (This BSA appears both in part 8 and part 9.) Batch scheduling refers to the ability to submit jobs to be executed when the system load permits. The "at" command allows jobs to be executed at a predefined time. Batch queuing refers to the ability to place multiple jobs in a queue for processing, and to access and manage the queue.

3.9.1.3.1 Standards. Table 3.9-3 presents standards for batch scheduling.

TABLE 3.9-3 Batch scheduling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 2:Shell and Utilities - Amendment 1: Batch Environment	1003.2d:1994	Mandated (Approved)
CPC	X/Open	Single UNIX Specification (Spec. 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C436 (9/94)	Emerging (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 15: Scheduling Function	10164-15:1995	Informational (Approved)
CPC	OSF	OSF/1 Operating System	OSF/1 O.S.	Informational (Approved)

3.9.1.3.2 Alternative specifications. The Berkeley BSD 4.3 Unix "at" and "batch" commands are also available.

3.9.1.3.3 Standards deficiencies. The POSIX.2 and Unix "at" and "batch" commands are designed for a single machine, centralized environment. Traditional POSIX and Unix batch capabilities, such as "at" and "batch," are inadequate and inefficient for managing resources and scheduling jobs in many environments, particularly environments that manage expensive resources, because they are very limited. For example, "at" allows users only to schedule machines to run jobs at particular times. No Ada bindings exist for the POSIX.2d Batch Queuing Extensions.

3.9.1.3.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.9.1.3.5 Related standards. No standards are related to batch scheduling.

3.9.1.3.6 Recommendations. The mandated standards are recommended, but both provide only limited batch functionality. For international work, use the POSIX.2 standard's new "-t time" option for the "at" command to express a time for execution of the submitted job in a way to support other time conventions more easily.

3.9.1.4 Process management and core operating system services. (This BSA appears in both part 8 and part 9.) Core operating system services are basic operating system services and interfaces, including traditional process management, memory management, time services, scheduling, terminal handling, error and exception management services, file-oriented services, and generalized input and output.

3.9.1.4.1 Standards. Table 3.9-4 presents standards for process management and core operating system services.

TABLE 3.9-4 Process management and core operating system services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Emerging (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) Amendment 2: Threads Extension [C Language]	1003.1c:1995	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
NPC	IEEE	Test Methods for Measuring Conformance to POSIX - System Interfaces	2003.1:1992	Informational (Approved)
NPC	IEEE	POSIX-Based Supercomputing Application Environment Profile	1003.10:1995	Informational (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	IEEE	POSIX - Part 1: Protocol Independent Interfaces	P1003.1g	Emerging (Draft)
NPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1a	Emerging (Draft)
NPC	IEEE	POSIX Multiprocessor Application Environment Profile	P1003.14	Emerging (Draft)
NPC	IEEE	POSIX Interactive System Application Environment Profile	P1003.18	Emerging (Draft)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C language]. (to profiled by FIPS PUB 151-2:1993)	9945-1:1990	International (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.9.1.4.2 Alternative specifications. Other consortia or de facto alternative specifications (such as ECMA APIW) for the Portable Operating System Interface for Computer Environments (POSIX) standard P1003.1 are available.

3.9.1.4.3 Standards deficiencies. ISO 9945-1:1996 incorporated IEEE 1003.1b Realtime and IEEE 1003.1c Threads. This resolves some of the deficiencies in the original POSIX.1, but the following deficiencies remain in the available standards:

a. Lacks batch scheduling for distributed computing.

b. Has weak event, error, and exception management services.

c. Has weak or no generalized I/O device driver services.

d. Has reentry problems when used for multiprocessing.

e. Reliability and maintainability not reflected in the standard.

f. The tasking model on which Ada is based does not map well to the process model on which POSIX.1 is based.

g. Has tape handling facilities requiring long backup times.

3.9.1.4.4 Portability caveats. Different specifications and implementations conforming with POSIX (e.g., OSF/1, SVID, SVR4, X/Open, and vendor products) often support the same function, but support them slightly differently. For example, the names of system calls may be identical, but unanticipated incompatibilities will arise because of differences in the data types of the function, the data types of the arguments, the return values, the required header files, and the symbolic error values.

Implementations conforming with POSIX may require extra header files for function calls that are ported from a system not requiring header files to another requiring header files. Although the impact of requiring extra header files is not always clear, differences in header file requirements can reduce portability. For example, if a program is ported from a system not requiring a header file for a particular function call, to a system requiring it, the call to that function may be undefined and generate an error message about the nonexistent header file.

Differences within header files can reduce portability when moving from a system that does not require a header file to one that does. For example, a header file may define attributes like data types or symbols conflicting with locally defined symbols.

Implementations of systems conforming with POSIX may refer to devices by logical names, numeric indicators, data structures, or pointers. Superset functions in implementations conforming with POSIX are important to have and convenient to use, but they reduce portability.

The meaning of ownership of "symbolic links" is not clear or consistent across different systems. Only the meaning of owning a file is consistent.

Many system attributes, such as system limits and configuration values limits, are defined by implementation.

3.9.1.4.5 Related standards. The following standards are related to process management and core operating system services or their standards:

a. IEEE 1003.2:1992: POSIX - Shell and Utilities.
b. IEEE 1003.2a:1992 POSIX - User Portability Extension.
c. IEEE P1003.1e: POSIX - Security Interface Extensions.
d. IEEE P1003.21: POSIX - Real Time Distributed Systems Communications.
e. X/Open Common Desktop Environment (XCDE) - Definitions and Infrastructure.

3.9.1.4.6 Recommendations. The mandated standards are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. IEEE 1003.1b (section 3) standardized additional functions not in 9945-1:1990 such as memory management and clocks and timers. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. It specifies many of the implementation-defined system limits related to files and directories and input/output.

To ensure maximum portability and smooth running information processing functions, it is important to determine, at a detailed level (e.g., arguments, order of the arguments, data types of the function and arguments, return values, symbolic error numbers), the specific areas of incompatibility between POSIX and the systems bid by vendors.

To ensure that no harm will result if an application is ported from a system that requires and supports a header file to a system that does not require the "include" statement in the system call, remove the header file from the application.

Avoid the use of extensions to POSIX. However, if extensions to POSIX must be used (they may be convenient), the applications in which they are used must be designed carefully for portability (e.g., separate the portable from the nonportable code, carefully document all nonportable code).

Including those header files required by POSIX.1 will ensure that properly written programs will build successfully on all FIPS-certified POSIX.1, regardless of which header files may be optional on a given vendor's platform.

Specifying that systems must conform to the X/Open's Single Unix Specification as demonstrated by a current X/Open Branding Certificate will eliminate the portability problems identified in the first paragraph of the portability caveats section.

3.9.1.5 System administration and management APIs. (This BSA appears in part 8 and part 9.) Operating system-based system administration standards provide interfaces to traditional, centralized operating system administration services and utilities. System management APIs refer to standardized Application Programming Interfaces that can be used by system and network managers and application developers to manage a system or network. They also are used to develop a system or network management application, without having to resort to writing third-generation language code or UNIX/POSIX shell scripts to perform the same functions on different machines. In this sense, system and network management APIs are considered productivity tools for system managers and system management application developers.

3.9.1.5.1 Standards. Table 3.9-5 presents standards for system administration and management APIs.

TABLE 3.9-5 System administration and management APIs standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Management Protocol Profiles (XMPP)	C206 (11/93)	Adopted (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
NPC	IEEE	Open Systems Interconnection (OSI) Abstract Data Manipulation - Application Program Interface (API) (Language Independent)	1224:1993	Adopted (Approved)
NPC	IEEE	POSIX System Administration - Part 2: Software Administration (former P1003.7.2)	1387.2:1995	Informational (Approved)
NPC	IEEE	POSIX: System Administration - Part 3: User and Group Administration	1387.3:1996	Informational (Approved)
NPC	IEEE	POSIX System Administration - Part 1: Overview (formerly 1003.7)	P1387.1	Informational (Draft)
NPC	IEEE	POSIX System Administration - Part 4: Print Administration (former P1003.7.1)	P1387.4	Informational (Draft)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.9.1.5.2 Alternative specifications. The following specifications are also available:

a. Groupe Bull: Consolidated Management Architecture (CMA), on which X/Open's XMP and OSF's CM-API are based.

b. Tivoli Systems: Objcall API, which is incorporated in MRB which is based on Tivoli. NOTE: A high-level API, such as the Tivoli Systems' "objcall" API is more suited for application development and integration than for management tasks such as long-term monitoring of system devices.

c. Tivoli Systems: Application Programming Interface (API) to objects.

d. Berkeley Unix.

e. OSF: OSF/1.

3.9.1.5.3 Standards deficiencies. All traditional Unix system administration is difficult. Neither System V system administration facilities nor Berkeley Unix system administration facilities were designed for a distributed networked environment. Traditional Unix system administration is not object-based and is not easily extendable.

3.9.1.5.4 Portability caveats. The traditional AT&T/USL system administration facilities are largely different from and incompatible with the traditional Berkeley Unix system administration facilities.

UI specifies the AT&T/USL system administration for the SVID. OSF provides the Berkeley Unix system administration facilities for OSF/1, except for the System V accounting facilities. The SVID and OSF/1 system administration interfaces, configuration files, and procedures are incompatible. Most of the shell scripts written for SVID-based Unix will not be portable to OSF/1 systems. The many system administration configuration files required by POSIX and Unix are not portable across different machines.

3.9.1.5.5 Related standards. The following standards are related to traditional operating system administration:

a. ISO IS 9595/9596/CCITT X.710/711: CMIS/CMIP (Common Management Information Service/Protocol).

b. ISO IS 7498:1986/CCITT X.700: Management Framework.

c. ISO IS 10040:1991: Systems Management Overview.

d. ISO IS 10164-1:1993/CCITT X.730: Object Management Function.

e. ISO IS 10164-2:1993/CCITT X.731: State Management Function.

f. ISO IS 10164-3:1993/CCITT X.732: Attributes for Representing Relationships.

g. ISO IS 10164-4:1992/CCITT X.733: Alarm Reporting Function.

h. ISO IS 10164-5:1993/CCITT X.734: Event Report Management Function.

i. ISO IS 10164-6:1993:Log Control Function.

j. ISO IS 10164-7:1992/CCITT X.736: Security Alarm Reporting Function.

k. ISO IS 10164-8:1993 Security Audit Trail Function.

l. ISO IS 10164-12:1994 Test Management Function.

m. ISO IS 10165-1:1993/CCITT X.720: Structure of Management Information.

n. ISO IS 10165-2:1992/CCITT X.721: Definition of Management Information.

o. ISO IS 10165-4:1992/CCITT X.722: Guidelines for the Definition of Managed Objects

p. ISO DIS 10181-2.2:1993: Authentication Framework.

q. ISO 8824:1990: (Edition 2) Specification of Abstract Syntax Notation 1 (ASN.1).

r. ISO 8825:1990: Specification of Basic Encoding Rules for ASN.1 (BER).

s. NIST FIPS 146-2: POSIT (for ASN.1 and BER (related to ISO 8824 and 8825)).

t. NIST FIPS 158-1: X Window System (X11 Version 5).

u. NIST FIPS 179-1: Government Network Management Profile (GNMP).

v. IEEE P1003.1e: Security Interface Standards for POSIX.

w. X/Open: G207:9/93: Systems Management Reference Model

x. X/Open: G303:9/93: Systems Management: Managed Object Guide (XMOG).

3.9.1.5.6 Recommendations. The PM should plan to use X/Open's XMPP as a common API to CMIP and SNMP. X/Open, Unix International, and OSF specify the same API, although they call them by different names (XMP and CM-API). The XMP and CM-API hide some of the differences between CMIP and SNMP and eliminate the need to learn two different syntaxes to access both protocols.

The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications. It replaces FIPS 179 (GNMP) in Version 3.0 of the NIST Application Portability Profile.

3.9.1.6 Scheduling. (This BSA appears both in part 8 and part 9.) Scheduling services and interfaces provide different scheduling policies, such as time-sharing, priority-based, and user-defined. Scheduling services initiate and terminate jobs (programs) in the computer, maintain a list of jobs to be run, and allocate computer resources depending on priority. Each process is controlled by an associated scheduling policy and priority.

Priority and preemptive scheduling standards provide interfaces to scheduling services allowing the highest-priority process to run first and to completion. Preemptive multitasking shares processing time with all running programs. For example, background programs can be given recurrent CPU time no matter how heavy the foreground load. Priority bumping is the process during a link, trunk, or facility failure where lower priority user access to network services is interrupted to offer those services or bandwidth to a predesignated higher priority user.

3.9.1.6.1 Standards. Table 3.9-6 presents standards for scheduling.

TABLE 3.9-6 Scheduling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1a	Emerging (Draft)
GPC	NIST	POSIX Real Time Extensions	FIPS PUB (Future)	Informational (Formative)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C language], (as profiled by FIPS PUB 151-2:1993)	9945-1:1990	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.9.1.6.2 Alternative specifications. There are no alternative specifications available.

3.9.1.6.3 Standards deficiencies. The POSIX.1 standard is not suitable for real time applications, because it supports only time-sliced time-sharing scheduling and does not allow scheduling based on the priority of a process.

The POSIX "nice" command for adjusting process priorities is not suitable for real time applications, because the "nice" function is merely a request to the operating system to favor a particular process for scheduling. However, in traditional Unix and POSIX.1, the effect of the "nice" command is tempered by degrading priorities based on CPU usage. In addition, the "nice" interface specifies an adjustment to a "nice" value, rather than setting it to an explicit value. Real time applications usually want to set priority to an explicit value. Finally, "nice()" does not allow for changing the priority of another process.

POSIX.1 scheduling is not based on absolute priorities. A process's scheduling priority degrades as it runs. POSIX.1 does not allow a system operator or real time application developer to tailor process scheduling.

POSIX.1b does not address the priorities of "system" processes. If system processes are not running in low priority ranges, conflicts with real time processes could result.

POSIX.1b does not address the interaction between priority and swapping because swapping and virtual memory paging-related issues are extremely dependent on the implementation and nearly impossible to standardize. However, the POSIX.1b scheduling paradigm fully describes the scheduling behavior of runnable processes, including the requirement for the working set to be resident in memory.

POSIX.1b does not address the temporary lending of priority from one process to another by the system (e.g., for the purposes of affecting the freeing of resources).

POSIX.1b does not define the effect of I/O interruptions and other system processing activities because the effect of I/O interruptions and system loading is intrinsically nondeterministic.

Influence levels (restrictions on a process's ability to affect other processes beyond a certain level) are defined by the implementation.

POSIX.1b does not address the mechanisms used to control access to scheduling facilities.

POSIX.1b does not address whether a process' handling of an event with a higher priority should have its priority boosted. This may be addressed later.

POSIX.1b provides a minimum of 32 priority levels. While this number conforms to the currently accepted scheduling theory requiring at least 32 priority levels for predictable responses with acceptable processor utilization, it is less than the 256 priority levels that many real time systems need.

3.9.1.6.4 Portability caveats. POSIX.1b supports a time-sharing scheduling policy, a real time scheduling policy, and a user-defined scheduling policy, but does not define the default scheduling policy. This could cause problems in porting the scheduling, and as a result, could cause problems in the response time behavior of real time applications.

POSIX.1b does not address resource preemption. The lack of resource preemption standardization could affect the ability to port real time applications so that they maintain the same behavior between systems. However, this does not affect source code portability, because resource preemption functions lie underneath the POSIX.1b interface.

The POSIX.1b priority-based scheduling functions are incompatible with the System V.4 SVID and SVR4 real time extensions' priority scheduling. The System V.4 "priocntl()" interface for priority scheduling violates POSIX.1b guidelines since it uses an argument to define the system call function. This increases the complexity of the "priocntl()" system call because it consolidates a large collection of related but logically separate functions into a single interface. Also, the "priocntl()" interface is less flexible than the POSIX.1b interface, because "priocntl()" does not permit separate disjointed or overlapping priority ranges between policies.

The specification of only 32 priority levels could reduce the behavior of some applications that depend on multiple priority levels to have reduced portability across conforming implementations.

In a conforming implementation, the priority ranges for the FIFO and Round Robin scheduling policies (SCHED_FIFO and SCHED_RR) defined in the header <sched.h> must be allowed to overlap, because these scheduling policies are identical except for the time interval. Because the third scheduling policy permitted by POSIX.1b (SCHED_OTHER) is defined by the user or implementation, any interactions among SCHED_OTHER and SCHED_FIFO or SCHED_RR also is defined by the implementation. Therefore, any application that depends on this interaction is not a strictly conforming application, and may not be portable across all systems.

3.9.1.6.5 Related standards. The following standard is related to priority and preemptive scheduling standards:

a. IEEE P1003.1e: Security Interface Standards for POSIX.

3.9.1.6.6 Recommendations. The mandated standards are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. IEEE 1003.1b standardized additional functions not in the original POSIX.1. FIPS 151-2 specifies many of the implementation-defined system limits and chooses among incompatible POSIX options.

Each real time functionality in the POSIX.1b standard is an option. If procurements do not call out the POSIX.1b Execution Scheduling option explicitly, vendors may provide a system conforming with POSIX.1b but not including this option.

Procurements should require implementations to document the priority ranges in which system processes run to check that conflicts will not exist between system processes and real time processes.

If a particular default scheduling policy is desired, a procurement should either specify the default explicitly or specify the ability for system operators to define one.

System processes always should execute in low priority ranges to avoid conflict with real time processes.

A portable, standardized interface for locking portions of a process in memory is necessary to ensure that paging behavior does not affect the scheduling of real time processes.

An organization-wide standard default scheduling policy should be established. Also, applications should make no assumptions about the default scheduling policy.

Although the POSIX.1b real time standard allows source code portable applications to be written, it does not guarantee that two such applications can coexist in a single system. To minimize conflicts, developers should adhere to certain programming guidelines to document the intent, rather than the syntax, of the standardization issues.

3.9.1.7 Subsystem management. (This BSA appears both in part 8 and part 9.) Subsystem Management Service (SMS) is a product that controls the execution of system processes (usually daemons). It ensures that related processes are started (or stopped) in the proper sequence. It also provides a standard systems administration command syntax to start/stop these processes, and the specification for an RPC interface that could be embedded into daemons to allow administrator interaction. Without SMS, the commands to start these processes are embedded in the system startup file. There is no mechanism to ensure that one daemon is ready before starting a related one. To stop a daemon, the administrator needs to know the syntax of the appropriate command, and needs to know which other related daemons also need to be stopped. If a daemon dies, the administrator needs to know which related processes to stop, and the proper sequence to restart them.

3.9.1.7.1 Standards. Table 3.9-7 presents standards for subsystem management.

TABLE 3.9-7 Subsystem management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Management Environment (DME): Subsystem Management Service	DME SMS	Mandated (Not Recommended (No commercial product))

3.9.1.7.2 Alternative specifications. There are no alternative specifications available.

3.9.1.7.3 Standards deficiencies. There are no products currently using the OSF DME SMS specifications. The software available from the OSF could be used as-is, although it is intended to be used by third-party vendors as the basis for products.

There are also no daemons that implement the SMS RPC interface, except for the ones that come with OSF DME. Therefore the SMS is required to use Signals to stop daemons, which may have unpredictable results if the daemon does not catch the signal correctly.

3.9.1.7.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.9.1.7.5 Related standards. The following standard is related to subsystem management.

a. OSF DCE Remote Procedure Call (RPC)

3.9.1.7.6 Recommendations. There are no recommendations.

3.9.2 User and group management. This requirement states the need to establish identity by appropriate authentication means for a user prior to interaction with application software, establishing a session on an application platform, accessing information storage, or establishing communication. Coupled with this identification is the association of privilege, by individual or group and requisite resource authorization, potentially across multiple components of the system.

3.9.2.1 User/group identification. (This BSA appears both in part 8 and part 9.) User/group identification services provide traditional system administration interfaces for administering users and groups. These services are mechanisms for system and network administrators to use when implementing a management policy across a system. Administrators can use the services to establish domains and policies for management throughout the system. They can provide the ability for applications to access group and user databases. Users can set up their own areas of management and policies or use system defaults that are included in management services.

3.9.2.1.1 Standards. Table 3.9-8 presents standards for user/group identification.

TABLE 3.9-8 User/group identification standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
NPC	IEEE	POSIX: System Administration - Part 3: User and Group Administration	1387.3:1996	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
GPC	NIST	Computer Security Guidelines for Implementing the Privacy Act of 1974	FIPS PUB 41:1975	Informational (Approved)
GPC	NIST	Guidelines on Evaluation of Techniques for Automated Personal Identification	FIPS PUB 48:1977	Informational (Approved)

3.9.2.1.2 Alternative specifications. The following specifications are also available:

a. Berkeley Unix: Centralized User and Group Management.
b. OSF/1 O.S.: Centralized User and Group Management.

3.9.2.1.3 Standards deficiencies. User and group management in the SVID, OSF/1, and Berkeley Unix is designed for a centralized, single machine environment. No Ada bindings exist for user and group management standards.

3.9.2.1.4 Portability caveats. System V Unix and the SVID use the commands "useradd" and "groupadd" to add a new user or group to the system. The OSF and Berkeley Unix use the commands "adduser" and "addgroup" to do the same thing.

Although the functionality defined by P1387.3 is based on historical user and group administration practice, no commercial products which conform to the (draft) standard are available as yet.

3.9.2.1.5 Related standards. The following standards are related to user and group management or user and group management standards:

a. ISO/IEC 9595:1991: CMIS.

b. ISO/IEC 9596:1991: CMIP.

c. ISO/IEC DIS 11578.2: RPC.

d. Network Management Forum: OMNIPoint 1.

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

f. Internet RFC 1157: Simple Network Management Protocol.

g. Internet RFC 1213: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

3.9.2.1.6 Recommendations. The mandated standards are recommended.

3.9.3 Configuration control. This requirement states the need to be able to manage the configuration of the system. This entails the ability to view the current configuration statically and dynamically modify the configuration, and the ability to tune the system.

3.9.3.1 Software distribution. (This BSA appears both in part 2 and part 9.) Software distribution and installation services comprise utilities for packaging, installing, and distributing software for use on heterogeneous and potentially incompatible systems. These services will enable network managers to transmit software to any stand-alone or networked system, regardless of the media used for distribution. Standards for software distribution in a system provide a standardized layout for distributing and installing software in a single system or network. They explicitly define each phase of software distribution, installation, and configuration--covering such distribution media as disks, tapes, and CD-ROM.

3.9.3.1.1 Standards. Table 3.9-9 presents standards for software distribution.

TABLE 3.9-9 Software distribution standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	POSIX System Administration - Part 2: Software Administration (former P1003.7.2)	1387.2:1995	Adopted (Approved)
CPC	X/Open	Single UNIX Specification (Spec. 1170)	T908: 1995	Emerging (Approved)
CPC	X/Open	Systems Management: Distributed Software Administration (XDSA)	P429:1997	Informational (Approved)

3.9.3.1.2 Alternative specifications. The following specifications are also available:

a. Hewlett-Packard: "swinstall" and "swpackage" systems.
b. USG: SVR4-based "pkgadd" system.
c. Santa Cruz Operation (SCO): "custom+" system.

3.9.3.1.3 Standards deficiencies. The IEEE 1387.2 standard does not provide for acting upon log files in remote file systems. No Ada bindings are available for software distribution standards.

3.9.3.1.4 Portability caveats. Although the IEEE 1387.2 standard is based on Hewlett-Packard's "swinstall" and "swpackage" systems, the standard has modified the specifications so that they are not exactly like the HP systems.

3.9.3.1.5 Related standards. The following standards are related to software distribution or software distribution standards:

a. ISO/IEC JTC1 IS 9595:1991: Common Management Information Service (CMIS).

b. ISO/IEC JTC1 IS 9596:1991: Common Management Information Protocol (CMIP).

c. ISO/IEC IS 11578: 1996, Information Technology - Open Systems Interconnection - Remote Procedure Call (RPC).

d. Internet RFC 1155 (STD 17): Structure and Identification of Management Information for TCP/IP-based Internets.

e. Internet RFC 1157 (STD 15): A Simple Network Management Protocol.

f. Internet RFC 1213 (STD 17): Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

g. Network Management Forum: OMNIPoint 1.

3.9.3.1.6 Recommendations. IEEE 1387.2 is recommended.

A new version of the X/Open Single UNIX Specification (Spec. 1170) is expected to be issued in 1997.

3.9.3.2 Software configuration management. (This BSA appears both in part 2 and part 9.) Configuration management is the process of applying administrative and technical procedures throughout the software life cycle to identity, define, and baseline configuration items for software in a system; control modifications and releases of the items; record and report the status of the items and modification requests; ensure the completeness and correctness of the items; and control storage, handling, and delivery of the items. This includes activities employed by the developer to identify entities (such as computer files, documents, Computer Software Configuration Items) whose version and status are to be tracked and controlled, to apply such controls, to keep records of these controls, and to audit that these controls are being applied.

3.9.3.2.1 Standards. Table 3.9-10 presents standards for software configuration management.

TABLE 3.9-10 Software configuration management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
NPC	EIA	National Consensus Standard for Configuration Management	IS-649	Adopted (Approved)
NPC	ANSI/IEEE	Software Configuration Management	1042:1987	Informational (Approved)
NPC	ANSI/IEEE	Software Configuration Management Plans	828:1990	Informational (Approved)
GPC	NIST	Guideline for Software Documentation Management	FIPS PUB 105:1984	Informational (Approved)
GPC	DOD	Configuration Management	MIL-STD-973(13): 1995	Informational (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207.0S-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Process - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

MIL-STD-498, Software Development and Documentation has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service.

3.9.3.2.2 Alternative specifications. The following additional guidance document is also available: Guidelines for Configuration Management (MIL-HDBK-761), although it is used with MIL-STD-973(13): 1995, which will most likely be canceled.

3.9.3.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.9.3.2.4 Portability caveats. Portability problems with the existing standards are unknown.

3.9.3.2.5 Related standards. None.

3.9.3.2.6 Recommendations. The adopted standards are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

3.9.3.3 Data dictionary. (This BSA appears in part 4 and part 9.) A data dictionary is a part of a database management system that transparently provides a centralized meaning, relationship to other data, origin, usage, and format. It also indicates which application programs use that data, so that when a change in a data structure is contemplated, a list of affected programs can be generated. The data dictionary a stand-alone system or may be an integral part of the DBMS and used to control it. Data integrity and accuracy is better ensured in the latter case.

3.9.3.3.1 Standards. Table 3.9-11 presents standards for data dictionary.

TABLE 3.9-11 Data dictionary standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Information Resource Dictionary System (IRDS) (adopts ANSI X3.138-1988 and X3.138A-1991)	FIPS PUB 156:1989	Adopted (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Framework	10027:1990	Informational (Approved)
GPC	NIST	Guide for the Development, Implementation, and Maintenance of Standards for the Representation of Computer Processed Data Elements	FIPS PUB 45:1976	Informational (Approved)
GPC	NIST	Guidelines for Planning and Using a Data Dictionary System	FIPS PUB 76:1980	Informational (Approved)
NPC	ANSI	Information Resource Dictionary System (IRDS)	X3.138-1988	Informational (Approved)
NPC	ANSI	Information Resource Dictionary System (IRDS) Services Interface	X3.185-1992	Informational (Approved)
NPC	ANSI	Information Resource Dictionary System (IRDS) Export/Import File Format	X3.195-1991	Informational (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Services Interface	10728:1993	Informational (Approved)
CPC	Metadata Coalition	Metadata Interchange Specification (MDIS)	MDIS 1.0:1996	Informational (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Services Interface Amendment 1: C Language Binding	10728 AMD 1:1994	Informational (Draft)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Export/Import Support for SQL:1992 with Integrity Enhancement	JTC1/SC21/WG03 Nxxx	Informational (Formative)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Design Support for SQL Applications	JTC1/SC21/WG03 Nxxx	Informational (Draft)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Services Interface Amendment 2: Ada bindings (binding for Ada 83)	10728 WDAM 2:1993(E)	Informational (Draft)

3.9.3.3.2 Alternative specifications. No applicable consortia or de facto specifications for the data dictionary are available.

3.9.3.3.3 Standards deficiencies. The following deficiencies have been identified in the available standards:

a. APIs with the IRDS are not currently defined.

b. There are no IRDS bindings to Ada.

c. IRDS does not support the development of active functionality.

d. IRDS does not support object-oriented data structures. An upcoming major IRDS revision is expected to add support for object-oriented data structures and communications between data management tools. Computer Aided Software Engineering (CASE) tool proponents are lobbying for this revision.

e. IRDS does not support information communications among data management tools.

f. IRDS conformance tests do not exist, although they are being developed.

g. While DOD 8320.1-M-1 Data Element Standardization Procedures, January 1993, provides procedures for the approval and maintenance of data elements. The standard governing the design, definition, and naming rules for data elements comes from Integration Definition for Information Modeling (IDEF1X), Corporate Information Management Process Improvement Methodology for DOD Functional Managers (1992). This has been adopted as FIPS 184.

h. There are no implementations.

3.9.3.3.4 Portability caveats. The ANSI and ISO services interface standards have diverged and are not compatible. All attempts to converge these standards have failed because the ANSI and ISO IRDS specifiers have different data dictionary interests. As a result, the ISO model is geared toward developing an underlying interface between the dictionary and the DBMS. U.S. Federal agencies, the NIST, and ANSI focus on user interfaces.

One example of how ANSI and ISO IRDS diverge is concerned with whether or not relationships are permitted to have attributes. ISO says no, on the grounds that its simpler model, without attributes, is more easily integrated with SQL tables. ANSI says yes, claiming that even though a model permitting attributes is more complex and difficult to use, it provides greater flexibility for more IRDS users. People using IRDS for system planning processes, for example, might need to store certain items in the dictionary that would not necessarily be applicable for interfacing with DBMSs.

3.9.3.3.5 Related standards. The following standards are related to data dictionaries or data dictionary standards:

a. International Telecommunications Union - Telecommunications Standards Sector (ITU-T) (formerly International Telegraph and Telephone Consultative Committee (CCITT))/ISO X.500: Directory Services

b. Standard Textual Language (STL): IEEE 1175 (particularly for use with CASE tools)

c. Many CASE tools, because the IRDS acts as a focus for sharing data and metadata and can be applied to them.

d. NIST FIPS 183: IDEF0

e. NIST FIPS 184: IDEF1X

f. Data element standards in the data dictionary BSA, above.

3.9.3.3.6 Recommendations. IRDS, FIPS 156, is recommended. Most computer vendors claim that they are committed to IRDS, but few have it now. If specific IRDS documents are not specified explicitly in a procurement, vendors most likely will propose products that are not compatible with IRDS.

If a procurement is targeted at a traditional database environment and a simpler-to-use IRDS is desirable, consider the ISO specification. If other environments are at stake and attributes on relationships, or many-to-many relationships are needed to represent the relationships between hardware and programs, as well as between programs and data, then choose FIPS 156 IRDS and use ANSI IRDS wherever FIPS 156 has not specified certain capabilities. Whether the choice is for ISO, ANSI, or FIPS IRDS, be prepared to lock yourself in for other procurement, rather than mixing ISO and ANSI IRDS because of the incompatibilities.

3.9.3.4 Distributed directory services. (This BSA appears in part 4, part 9, and part 11.) A directory or naming service provides a standardized naming scheme, a standardized interface with the naming facilities, and the ability for the interface to provide transparent access to a variety of naming schemes and mechanisms (e.g., DCE).

Directory service applications convert a name into a physical address on a network, providing logical to physical conversion. Names can be user names, computers, printers, servers, or files. This enables users to find these resources without knowing their locations. The transmitting station sends a name to the server containing the naming service software, which sends back the actual address of the user or resource.

3.9.3.4.1 Standards. Table 3.9-12 presents standards for distributed directory services.

TABLE 3.9-12 Distributed directory services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Directory (Global and Cell) Service	DCE 1.1 Directory:1994	Mandated (Approved)
IPC	ISO	Open Systems Interconnection-Session Service Definition	8326:1987	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Connection-Oriented Session Protocol	8327:1987	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Basic Connection Oriented Presentation Service Definition	8822:1988	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Connection-Oriented Presentation Protocol	8823:1988	Informational (Approved)
IPC	ITU-T	The Directory: Models (X-ref: ISO 9594-2)	X.501 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Authentication Framework (X-ref: ISO 9594-8)	X.509, Version 3: 1993	Informational (Approved)
IPC	ITU-T	The Directory: Abstract Service Definition (X-ref: ISO 9594-3)	X.511 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Procedures for Distributed Operation (X-ref: ISO 9594-4)	X.518: 1993	Informational (Approved)
IPC	ITU-T	The Directory: Protocol Specification (X-ref: ISO 9594-5)	X.519 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Selected Attributes Types (X-ref: ISO 9594-6)	X.520 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Selected Object Classes (X-ref: ISO 9594-7)	X.521 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Replication (X-ref: ISO 9594-9)	X.525 (1993)	Informational (Approved)
CPC	X/Open	Federated Naming: The XFN Specification	C403 (7/95)	Informational (Approved)
NPC	IEEE	Directory services/Name space API	1224.2:1993	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Domain Name Service Profile (References IAB STD 13 (RFC 1034, 1035))	MIL-STD-2045-17505:1994	Informational (Approved)

3.9.3.4.2 Alternative specification. There are no alternative specifications available.

3.9.3.4.3 Standard deficiencies. Deficiencies in the existing specifications are unknown.

3.9.3.4.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.9.3.4.5 Related standards. There are no related standards.

3.9.3.4.6 Recommendations. OSF DCE directory services are recommended for DCE applications. For more information on non-DCE directory services, see the Host Application Support BSA in part 7, Communication Services.

3.9.3.5 System configuration. (This BSA appears both in part 8 and part 9.) System configuration services is a representation of the components and component parameters of a computer system (e.g., memory boards, amounts of memory, memory addresses, particular interrupts, networks, network addresses, and specific peripherals such as keyboards, disk drives, terminals, mice or other input devices, and specialized instruments). Clearly, every computer must have a way to do this. System configuration also refers to the automation of this procedure (i.e., automated system configuration) and the ability to configure the system on-line. On-line configuration refers to the ability for system administrators to make dynamic configuration changes, while users are working on-line, rather than having to take the system down.

3.9.3.5.1 Standards. Table 3.9-13 presents standards for system configuration.

TABLE 3.9-13 System configuration standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 1: Object Management Function	10164-1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 2: State Management Function	10164-2:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 3: Attributes for Representing Relationships	10164-3:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 12: Test Management Function	10164-12:1994	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)

3.9.3.5.2 Alternative specifications. No other consortia or de facto specifications are available.

3.9.3.5.3 Standards deficiencies. The present ISO 10164-3, "Attributes for Representing Relationships," and 10164-12, "Test Management Function," standards were designed with network configuration in mind. Theoretically, these standards should be able to be used for configuration management of any computer system. Until now, very little work has been done in this area, either in standards groups or in products. Exactly how these standards should be used in host management is undetermined.

Versions 1.0 and 2.0 of the GNMP specify only network management capabilities. Not until Version 3.0 is available will the GNMP specify the management information required for general system management, such as host computer configuration and management, operating systems management, and database management systems.

The present ISO standards and GNMP specifications require ISO CMIS/CMIP for the communication of management information and ISO OSI networking protocols. Plans are for the

GNMP to provide a capability to integrate the present GNMP with SNMP also. One reason for this goal is the widespread use of SNMP.

No Ada bindings exist for the configuration management standards or consortia specifications.

3.9.3.5.4 Portability caveats. Unknown

3.9.3.5.5 Related standards. The following standards are related to system configuration or system configuration standards:

a. ISO/IEC 7498-4:1989: Management Framework.

b. ISO/IEC 8571:1988: File Transfer, Access, and Management (FTAM), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if FTAM functionality are required.

c. ISO/IEC 8650:1988: ACSE, as specified in GOSIP Version 2, Section 4.2.7.1, as modified by the Network Management SIG (NMSIG) agreements in Part 18 of the OSI Implementors' Workshop (OIW) Implementors Agreements.

d. ISO/IEC 8824:1990: Specification of Abstract Syntax Notation 1 (ASN.1).

e. ISO/IEC 8825:1990: Specification of Basic Encoding Rules for ASN.1.

f. ISO/IEC 9041:1990: (OSI Virtual Terminal), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if virtual terminal functionality is required.

g. ISO/IEC 9072:1989: Remote Operations Service Element (ROSE), as specified in the Remote Operations Part 1: Model Notation and Service Definition (ROSES), and the Remote Operations Part 2: Protocol Specification (ROSEP), and as modified by the NMSIG agreements clause 6.5.

h. ISO/IEC 9595:1991: CMIS.

i. ISO/IEC 9596:1991: CMIP.

j. ISO/IEC 10165-1:1993: Structure of Management Information (SMI).

k. ISO/IEC 10165-2:1992: Definition of Management Information (DMI).

l. ISO/IEC 10165-4:1992: Guidelines for the Definition of Managed Objects (GDMO).

m. ISO/IEC DIS 11578.2: Remote Procedure Call.

n. IEEE 1224:1993: OSI Abstract Data Manipulation (Object Management) API - Language Independent Specification.

o. IEEE 1327:1993: OSI Abstract Data Manipulation (Object Management) API - C Language Binding.

p. Comite Consultatif International de Telegraphique et Telephonique (CCITT) X.400 Message Handling System (MHS), as specified in GOSIP Version 2 Sections 4.2.7.3 and 5.3.2, if message handling functionality is required.

q. NIST OSI Implementors Workshop (OIW) Implementor Agreements relating to the Presentation and Session layers, as specified in Part 5 (Upper Layer Agreements), clause 13.7 of the OIW Stable Implementation Agreements for OSI Protocols Version 3 (NIST Special Publication 500-224).

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

s. Internet RFC 1157: Simple Network Management Protocol.

t. Internet RFC 1213: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

u. X/Open: C315:5/94: OSI-Abstract-Data Manipulation API (XOM) (Object Management).

3.9.3.5.6 Recommendations. OMNIPoint 1 is recommended. The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications.

To build or procure configuration management applications, users must identify the system management functions that are applicable to their requirements. Then they must identify the various ISO 10164 and 10165 standards whose specifications are related to these requirements. Finally, they must include their explicit requirements and the related standards in the RFP.

3.9.3.6 Network configuration management. Network configuration management defines the procedures for initializing, operating, and closing down the managed objects, and the procedures for reconfiguring the managed objects.

3.9.3.6.1 Standards. Table 3.9-14 presents standards for network configuration management.

TABLE 3.9-14 Network configuration management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)

3.9.3.6.2 Functionalities supported. This network service supports the Network Management functionality.

3.9.3.6.3 Related network services. Addressing is related to this network service.

3.9.3.6.4 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.9.3.6.5 Recommendations. The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications. It replaces FIPS 179 (GNMP) in Version 3.0 of the NIST Application Portability Profile.

3.9.3.6.6 Portability caveats. Portability problems related to the existing specifications are unknown.

3.9.4 Usage monitoring and cost allocation. Services that allow monitoring of system usage, allocation of resources, and assessment of charges to users.

3.9.4.1 Software license management. (This BSA appears in both part 2 and part 9.) License management addresses the problem of tracking software licenses in a distributed systems environment. The DME licensing technology includes models that assist users in keeping track of how many software copies are needed and who is using it once it is purchased. Software license management for a system provides license administration, monitoring, and enforcement services that allow more detailed, firm and equitable licensing terms for users, and better protection against illegal software usage for vendors.

3.9.4.1.1 Standard. Table 3.9-15 presents standards for software license management.

TABLE 3.9-15 Software license management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	POSIX System Administration - Part 2: Software Administration (former P1003.7.2)	1387.2:1995	Adopted (Approved)
CPC	X/Open	Systems Management: Distributed Software Administration (XDSA)	P429:1997	Informational (Approved)
CPC	OSF	Distributed Management Environment (DME) License Management (LM) Service	DME LM	Informational (Emerging (Not recommended))

3.9.4.1.2 Alternative specification. The following specifications are also available:

a. Hewlett-Packard: Network License System (NetLS) Version 2.0 on which OSF's DME License Management System (LS) is based.

b. Gradient Technologies: PC Client libraries for license management and PC Ally server, on which DME's License Management PC component is based.

3.9.4.1.3 Standard deficiencies. No Ada bindings exist for any of the configuration management standards or consortia specifications.

3.9.4.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.9.4.1.5 Related standards. The following standards are related to license management or license management standards:

a. ISO/IEC JTC1 IS 9595:1991: Common Management Information Service (CMIS).

b. ISO/IEC JTC1 IS 9596:1991: Common Management Information Protocol (CMIP).

c. ISO/IEC IS 11578: 1996, Information Technology - Open Systems Interconnection - Remote Procedure Call (RPC).

d. Internet RFC 1155 (STD 17): Structure and Identification of Management Information for TCP/IP-based Internets.

e. Internet RFC 1157 (STD 15): A Simple Network Management Protocol.

f. Internet RFC 1213 (STD 17): Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

g. Network Management Forum: OMNIPoint 1.

3.9.4.1.6 Recommendations. IEEE 1387.2 is recommended.

3.9.4.2 Accounting management. (This BSA appears in part 8 and part 9.) Accounting management services provide the ability to cost services for charging and reimbursement. An effective cost management system should contribute to the development of a sound investment strategy that recognizes and evaluates cost and alternatives. The services should also provide for the ability to measure and prioritize resource usage and to monitor assets and maintain costing records for chargeback purposes. Costs of information technology services should be capable of being apportioned to users, and reports of those costs should be capable of being provided to management and customers.

3.9.4.2.1 Standards. Table 3.9-16 presents standards for accounting management.

TABLE 3.9-16 Accounting management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	OSI Systems Management, Part 10: Usage Metering Function for Accounting Purposes	10164-10:1995	Adopted (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 13: Summarization Function	10164-13:1995	Adopted (Approved)
GPC	NIST	Guideline for Developing and Implementing a Charging System for Data Processing Services	FIPS PUB 96:1982	Adopted (Approved)

3.9.4.2.2 Alternative specifications. The following specifications are also available:

a. OSF/1 O.S.: Centralized Accounting Mgmt.
b. Berkeley BSD 4.3 Unix.

3.9.4.2.3 Standards deficiencies. A variety of different chargeback systems are using different metrics and methods that are causing compatibility problems within agencies and services. The Unix accounting functions are designed for a single machine environment.

The present ISO 10164-10, "Accounting Metering Function," and 10164-13, "Summarization Function," standards were designed with a networked system configuration in mind. Little work has been done in standards groups or products to determine how to use these standards for host configuration management.

Although several standard libraries of object classes that allow a common view of network resources are planned, few are currently available or sufficiently complete. For example, these library specifications have incomplete object definitions for modems, OSI routers, and transport connections.

The ISO standards require ISO CMIS/CMIP for the communication of management information and ISO OSI networking protocols, and do not interoperate with TCP/IP.

No Ada bindings exist for any of the ISO or consortia system management specifications.

3.9.4.2.4 Portability caveats. OSF/1 uses the System V Unix accounting facilities. Although the OSF/1 and System V accounting systems differ, and each operating system has extra accounting functions, the use of the same accounting facilities eliminates one source of incompatibility.

3.9.4.2.5 Related standards. The following standards are related to accounting management or accounting management standards:

a. ISO/IEC 7498:1986: Management Framework.

b. ISO/IEC 8571:1988: FTAM, as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if FTAM functionality are required.

c. ISO/IEC 8650:1988: ACSE, as specified in GOSIP Version 2, Section 4.2.7.1, as modified by the NMSIG agreements in Part 18 of the OIW Implementors Agreements.

d. ISO/IEC 8824:1990: Specification of Abstract Syntax Notation 1 (ASN.1).

e. ISO/IEC 8825:1990: Specification of Basic Encoding Rules for ASN.1.

f. ISO/IEC 9041:1990 (OSI Virtual Terminal), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if virtual terminal functionality is required.

g. ISO/IEC 9072:1989: ROSE, as specified in the Remote Operations Part 1: Model Notation and Service Definition (ROSES), and the Remote Operations Part 2: Protocol Specification (ROSEP), and as modified by the NMSIG agreements clause 6.5.

h. ISO/IEC 9595:1991 CMIS.

i. ISO/IEC 9596:1991 CMIP.

j. ISO/IEC 10165-1:1993: SMI.

k. ISO/IEC 10165-2:1992: DMI.

l. ISO/IEC 10165-4:1992: Guidelines for the Definition of Managed Objects (GDMO).

m. ISO/IEC DIS 11578.2: RPC.

n. CCITT X.400 Message Handling System (MHS), as specified in GOSIP Version 2 Sections 4.2.7.3 and 5.3.2, if message handling functionality is required.

o. IEEE 1224:1993: OSI Abstract Data Manipulation (Object Management) API - Language Independent Specification.

p. IEEE 1327:1993: OSI Abstract Data Manipulation (Object Management) API - C anguage Binding.

q. NIST OSI Implementors Workshop (OIW) Implementor Agreements relating to the Presentation and Session layers, as specified in Part 5 (Upper Layer Agreements), clause 13.7 of the OIW Stable Implementation Agreements for OSI Protocols Version 3 (NIST Special Publication 500-224).

r. Internet RFC 1155: Structure and Identification of Management Information for Internets based on TCP/IP.

s. Internet RFC 1157: Simple Network Management Protocol.

t. Internet RFC 1213: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

u. Network Management Forum: OMNIPoint 1.

v. X/Open: OSI-Abstract-Data Manipulation API (XOM) (Object Management).

3.9.4.2.6 Recommendations. To build or procure account management applications, users must identify the system management functions that are applicable to their requirements. Then they must identify the various specifications within the ISO 10164 and 10165 standards that are related to these requirements. Finally, they must explicitly include the requirements and the related standards in the RFP.

In the future, the NIST plans to provide a capability in the GNMP to integrate the present GNMP with SNMP.

3.9.4.3 System resource limits. (This BSA appears both in part 8 and part 9.) Resource limits functionality allows system administrators to control the amount of system resources available to users.

3.9.4.3.1 Standards. Table 3.9-17 presents standards for system resource limits.

TABLE 3.9-17 System resource limits standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Adopted (Approved)
NPC	IEEE	POSIX-Based Supercomputing Application Environment Profile	1003.10:1995	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.9.4.3.2 Alternative specifications. The following specifications are also available:

a. Berkeley 4.3 Unix.
b. Cray Research, Inc.: "limits" interfaces.
c. OSF: OSF/1 Operating System: "getrlimit/setrlimit."

3.9.4.3.3 Standards deficiencies. The Berkeley Unix and System V "setrlimit" and "ulimit" interfaces have the limitation that users may act only to make their limits more restrictive.

3.9.4.3.4 Portability caveats. The actual numeric limit values for different resource limits are not portable across various platforms. Applications need to provide some sort of configuration parameters to specify the actual numeric values for each site.

3.9.4.3.5 Related standards. The following standards are related to resource limits or resource limit standards:

a. ISO/IEC 9945-1:1996: POSIX.1 System Application Programming Interfaces.
b. IEEE P1003.1e: Security Interface Standards for POSIX.
c. IEEE P1387.1: POSIX System Administration - Part 1: Overview.
d. IEEE 1003.2d:1994: POSIX Batch Environment Amendments.

3.9.4.3.6 Recommendations. X/Open Single Unix Specification (SUS) provides "setrlimit/getrlimit" functionality.

3.9.5 Performance monitoring. Performance monitoring services allow information technology resources to be managed efficiently. Performance aspects of hardware, software, and network components must be monitored and subsequently made available to the system manager. The manager must then have access to services and parameters with which to tune the system to meet performance targets.

3.9.5.1 Software management indicators. (This BSA appears both in part 2 and part 9.) Software management indicators aid in managing the software development process. Various measurements of both software products and software processes are available. Product measures(such as lines of code, function points, etc.) are often associated with the product specification and should be used as management indicators throughout the product life cycle. Process measures(such as software trouble reports) should be tracked to determine whether the software development process is within statistical control limits. Key indicators should be identified in the software development plan, and the developer should then collect, analyze, interpret, take corrective actions, and report on the selected key management indicators.

3.9.5.1.1 Standards. Table 3.9-18 presents standards for software management indicators.

TABLE 3.9-18 Software management indicators standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Adopted (Approved)
IPC	ISO/IEC	Quality Characteristics and Guidelines for Their Use	9126:1991	Adopted (Approved)
NPC	IEEE	Use of Standard Measures to Produce Reliable Software	982.2:1988	Informational (Approved)
NPC	IEEE	Standard Dictionary of Measures to Produce Reliable Software	982.1:1988	Informational (Approved)
NPC	IEEE	Software Productivity Metrics	1045:1992	Informational (Approved)
NPC	IEEE	Software Quality Metrics Methodology	1061:1992	Informational (Approved)
IPC	ISO/IEC	Software Life Cycle Processes	12207:1995	Informational (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207/IS-data	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1/IS-data	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2/IS-data	Informational (Draft)

MIL-STD-498, Software Development and Documentation has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service.

3.9.5.1.2 Alternative specifications. For additional metrics information, consult the following documents:

a. Metrics for I-CASE Pilot Project (MIPP) Program, Metrics Reporting Guidebook, (prepared by Mitre Corporation, 27 May 1994, for DISA/JIEO/CIM/TXEM).

b. Practical Software Measurement: A Guide to Objective Program Insight, Draft 12 April 1995.

c. Streamlined Integrated Software Metrics Approach (SISMA) Guidebook; Application of STEP Metrics, (prepared by Software Productivity Solutions, Indialantic, FL 32903, 12 July 1993, for the U.S. Army).

d. Software Measurement Guidebook, (prepared by the Software Productivity Consortium Services Corporation, December 1992, Herndon VA, for DARPA).

3.9.5.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.9.5.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.9.5.1.5 Related standards. Related software management guidance can be found in the Software Engineering Institute's Capability Maturity Model (CMM). The Software Engineering Institute's CMM provides guidance on how to gain control of the software development and maintenance processes. The CMM has defined an evaluation procedure, the CMM Based Appraisal (CBA), as a means of identifying the risks associated with potential contractor performance. Diagnostic tools based on the CMM have been deployed. One of those tools, the Software Capability Evaluation(SCE), is designed to be used by an acquiring organization to either identify process risks associated with a particular proposal during the source selection or to monitor the risk-reducing process improvements during the contract execution.

3.9.5.1.6 Recommendations. The adopted standards are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. MIL-STD-498 contains requirements for security and privacy for software development and documentation. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA

12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service policy, until organizational processes for IEEE/EIA 12207US are in place.

For other related information, consult ISO/IEC 9126. Appropriate standards should be selected based on software metrics requirements.

3.9.5.2 Performance management. (This BSA appears in part 8 and part 9.) Performance management provides services and interfaces for tuning systems and subnetworks to meet individual performance requirements. Performance management enables the behavior of resources and the effectiveness of communication activities to be evaluated. It includes functions to: gather statistical information; maintain and examine logs of system state histories; determine system performance under natural and artificial conditions; and alter system modes of operation for the purpose of conducting performance management activities. Performance management may make use of event management facilities.

3.9.5.2.1 Standards. Table 3.9-19 presents standards for performance management.

TABLE 3.9-19 Performance management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Data Communications Systems and Services -User Oriented Performance Parameters (adopts ANSI X3.102-1983/R1990)	FIPS PUB 144:1985	Adopted (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 11: Metric Objects and Attributes	10164-11:1994	Informational (Approved)
GPC	NIST	Guideline on Computer Performance Management: An Introduction	FIPS PUB 49:1977	Informational (Approved)
GPC	NIST	Guidelines for the Measurement of Interactive Computer Service Response Time and Turnaround Time	FIPS PUB 57:1978	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
GPC	NIST	Guidelines for Measurement of Remote Batch Computer Service	FIPS PUB 72:1980	Informational (Approved)

3.9.5.2.2 Alternative specifications. No other consortia or de facto specifications are available.

3.9.5.2.3 Standards deficiencies. The present 10164-11 ("Workload Monitoring Function) and generic 10165-xx standards were designed with network configuration in mind. Theoretically, they should be able to be used for configuration management of any computer system. Little work has been done in this area, either in standards groups or in products. Exactly how these standards should be used in host management is undetermined. Standards for system performance measurement are needed.

Although several standard libraries of object classes that allow a common view of network resources and support performance management of network resources are planned, few are currently available or sufficiently complete. For example, these library specifications have incomplete object definitions for modems, OSI routers, and transport connections. Based on needs of the U.S. Federal Government (as shown by NIST surveys), the GNMP added more object class specifications and definitions. These include the following objects: LANs, X.25 WANs, ISDN, FDDI, modems, bridges, links, and a rudimentary capability to manage OSI

routers and transport connections. Phase 2 GNMP objects also will include protocol software (layers 3-7), routers, terminal servers, MTAs, PBXs, and circuit switches.

Versions 1.0 and 2.0 of the GNMP currently specify only network management capabilities. Not until Version 3.0 will the GNMP specify the management information required for general system management, such as host computer configuration and management, operating systems, and database management systems.

The present ISO standards and GNMP specifications require ISO CMIS/CMIP for the communication of management information and ISO OSI networking protocols. Plans are for the GNMP eventually to provide a capability to integrate the present GNMP with SNMP. One reason for this goal is the widespread use of SNMP.

No Ada binding is available for the ISO system management standards.

Performance management could make use of generalized event management facilities, but most products currently implement their own event management.

3.9.5.2.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.9.5.2.5 Related standards. The following standards are related to performance management or performance management standards:

a. ISO/IEC 7498-4:1989: Management Framework.

b. ISO/IEC 8571:1988: FTAM, as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if FTAM functionality are required.

c. ISO/IEC 8650:1988: Association Control Service Element (ACSE), as specified in GOSIP Version 2, Section 4.2.7.1, as modified by the NMSIG agreements in Part 18 of the OIW Implementors Agreements.

d. ISO/IEC 8824:1990: Specification of Abstract Syntax Notation 1 (ASN.1).

e. ISO/IEC 8825:1990: Specification of Basic Encoding Rules for ASN.1.

f. ISO/IEC 9041:1990: (OSI Virtual Terminal), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if virtual terminal functionality is required.

g. ISO/IEC 9072:1989: ROSE, as specified in the Remote Operations Part 1: Model Notation and Service Definition (ROSES), and the Remote Operations Part 2: Protocol Specification (ROSEP), and as modified by the NMSIG agreements clause 6.5.

h. ISO/IEC 9595:1991: CMIS.

i. ISO/IEC 9596:1991: CMIP.

j. ISO/IEC 10165-1:1993: SMI.

k. ISO/IEC 10165-2:1992: DMI.

l. ISO/IEC 10165-4:1992: GDMO.

m. ISO/IEC DIS 11578.2: RPC.

n. CCITT X.400 Message Handling System (MHS), as specified in GOSIP Version 2 Sections 4.2.7.3 and 5.3.2, if message handling functionality is required.

o. IEEE 1224:1993: OSI Abstract Data Manipulation (Object Management) API - Language Independent Specification.

p. IEEE 1327:1993: OSI Abstract Data Manipulation (Object Management) API - C Language Binding.

q. NIST OSI Implementors Workshop (OIW) Implementor Agreements relating to the Presentation and Session layers, as specified in Part 5 (Upper Layer Agreements), clause 13.7, of the OIW Stable Implementation Agreements for OSI Protocols Version 3 (NIST Special Publication 500-224).

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

s. Internet RFC 1157: Simple Network Management Protocol.

t. Internet RFC 1158: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

u. X/Open: C315:5/94: OSI-Abstract-Data Manipulation API (XOM) (Object Management).

3.9.5.2.6 Recommendations. To procure performance management applications, users must identify the system management functions that are applicable to their requirements. Then they must identify the various specifications in the ISO 10164 and 10165 standards related to these requirements. Finally, they must include their requirements and the related standards in the RFP.

The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications. It replaces FIPS 179 (GNMP) in

Version 3.0 of the NIST Application Portability Profile. OMNIPoint adopts the ISO 10164 and 10165 series of standards.

FIPS 144 is a mandatory standard according to the Federal ADP and Telecommunications Standards Index and shall be used if it satisfies the user's requirements.

3.9.5.3 Network flow control. Flow control refers to the regulation of the movement of datagrams through the transfer process. It includes the ability to manage the size of the information at various stages in the process.

3.9.5.3.1 Standards. Table 3.9-20 presents standards for network flow control.

TABLE 3.9-20 Network flow control standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	Transmission Control Protocol	Standard 7/RFC-793	Mandated (Approved)
IPC	IAB	Host Requirements	Standard 3/RFC-1122/RFC-1123	Mandated (Approved)
IPC	IAB	The Point-to-Point Protocol (PPP)	Standard 51/RFC 1661	Mandated (Approved)
GPC	DOD	Transport Profile: Reliable End System Transport for DOD Communications	MIL-STD-2045-14500 Part 1:March 1994	Informational (Approved)
GPC	DOD	Internet Transport Profile for DOD Communications Wide Area Network Access (References ISO 8208 Information Processing Systems - Data communications - X.25 Packet Level Protocol for Data Terminal Equipment)	MIL-STD-2045-14502 Part 3:July 1994	Informational (Approved)
GPC	DOD	Transport Profile: Balanced Point-to-Point Digital Data Circuit	MIL-STD-2045-14500 Part 2:March 1994	Informational (Approved)
GPC	DOD	Transport Profile: Subnetwork for an Unbalanced Data Link	MIL-STD-2045-14500 Part 3:March 1994	Informational (Approved)
GPC	DOD	Internet Transport Profile for DOD Communications: Point-to-Point Links	MIL-STD-2045-14502 Part 2:July 1994	Informational (Approved)
GPC	DOD	Transport Protocol for High Bit Error Rate Operational Environment	MIL-STD-2045-44000	Informational (Emerging)

3.9.5.3.2 Alternative specifications. There are no alternative specifications.

3.9.5.3.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.9.5.3.4 Portability caveats. Connection-oriented transport classes do not interoperate. Applications using different classes of transport service will have portability problems. Class Zero connection-oriented transport must be provided along with X.25 if public messaging systems are to be connected to the procured systems.

The X.25 equipment that conforms to different X.25 specification dates (e.g., 1980, 1984, 1988, 1992) can have interoperability problems.

3.9.5.3.5 Related standards. There are no related standards.

3.9.5.3.6 Recommendations. Flow control is one of the functions supported by the Transmission Control Protocol (TCP). The TCP should be used as specified in the IAB STD 7. The IAB STD 3 identifies and corrects errors in the TCP.

MIL-STD-2045-14500-01 should be used for legacy systems interoperability. It uses Class Four connection-oriented transport protocol is one of the base standards. It provides the most reliable transport service and, in turn, assumes the least about the network layer services supporting transport. Implementations requiring use of TP4 for flow control services should comply with MIL-STD-2045-14500-01. A connection-oriented transport class must be chosen based on the reliability of the other OSI layers in the system. MIL-STD-2045-14500 parts 2 and 3 should be used for legacy systems. For legacy systems, LAPB should be used as specified in MIL-STD-2045-14500 Parts 2 and 3.

If recommended standards do not meet system requirements, or are cost prohibitive, standards for the legacy systems may be used as long as interoperability is not impacted. The use of legacy systems standards may require a waiver from the appropriate authority. MIL-STD-2045-44000 is an emerging standard. It uses TCP and UDP with enhancements to meet specific requirements for high-stress resource constrained environments.

3.9.5.4 Network sequencing. Sequencing is a function performed by the N-layer to preserve the order of N-service data units that were submitted to the N-layer (ISO 7498).

3.9.5.4.1 Standards. Table 3.9-21 presents standards for network sequencing.

TABLE 3.9-21 Network sequencing standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	Transmission Control Protocol	Standard 7/RFC-793	Mandated (Approved)
IPC	IAB	Host Requirements	Standard 3/RFC-1122/RFC-1123	Mandated (Approved)
IPC	IAB	The Point-to-Point Protocol (PPP)	Standard 51/RFC 1661	Mandated (Approved)
GPC	DOD	Internet Transport Profile for DOD Communications Wide Area Network Access (References ISO 8208 Information Processing Systems - Data communications - X.25 Packet Level Protocol for Data Terminal Equipment)	MIL-STD-2045-14502 Part 3:July 1994	Informational (Approved)
GPC	DOD	Internet Transport Profile for DOD Communications: Point-to-Point Links	MIL-STD-2045-14502 Part 2:July 1994	Informational (Approved)
GPC	DOD	Transport Profile: Reliable End System Transport for DOD Communications	MIL-STD-2045-14500 Part 1:March 1994	Informational (Approved)
GPC	DOD	Transport Profile: Balanced Point-to-Point Digital Data Circuit	MIL-STD-2045-14500 Part 2:March 1994	Informational (Approved)
GPC	DOD	Transport Profile: Subnetwork for an Unbalanced Data Link	MIL-STD-2045-14500 Part 3:March 1994	Informational (Approved)
GPC	DOD	Transport Protocol for High Stress Electronic Constrained Environments	MIL-STD-2045-44000	Informational (Formative)

3.9.5.4.2 Alternative specifications. There are no alternative specifications.

3.9.5.4.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.9.5.4.4 Portability caveats. Connection-oriented transport has five levels of service that deal with reliability. These classes do not interoperate. Applications using different classes of transport service will have portability problems. Class Zero connection-oriented transport must be provided along with X.25 if public messaging systems are to be connected to the procured systems.

The X.25 equipment conforming to different specification dates (e.g., 1980, 1984, 1988, 1992) can have interoperabilty problems.

3.9.5.4.5 Related standards. There are no related standards.

3.9.5.4.6 Recommendations. Sequencing is one of the functions supported by Transmission Control Protocol (TCP). The TCP should be used as specified in the IAB STD 7. The IAB STD 3 identifies and corrects errors in the TCP.

MIL-STD-2045-14500-01 is recommended for legacy systems interoperability. It uses TP4 as one of its base standards. The Class Four transport provides the most reliable transport service. It assumes that the underlying network service is unreliable. A connection-oriented transport class must be chosen based on the reliability of the other OSI layers in the system. MIL-STD-2045-14500 parts 2 and 3 are recommended for legacy systems use. LAPB should be used as specified in MIL-STD-2045-14500 Parts 2 and 3.

If recommended standards do not meet system requirements, or are cost prohibitive, standards from the legacy column may be used as long as interoperability is not impacted. The use of legacy systems standards may require a waiver from the appropriate authority. MIL-STD-2045-44000 is an emerging standard. It uses TCP and UDP with enhancements to meet specific requirements for high-stress resource constrained environments.

3.9.5.5 Communication of management information. (This BSA appears in part 8 and part 9.) Communication of management information refers to a mechanism and protocol with extensions specifically geared to the communication of data and information used by system management and network management applications for monitoring and controlling resources. This management information may be shared between management processes and structured according to the requirements of those processes.

3.9.5.5.1 Standards. Table 3.9-22 presents standards for communication of management information.

TABLE 3.9-22 Communication of management information standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	Simple Network Management Protocol (SNMP)	Standard 15/RFC-1157	Mandated (Approved)
GPC	DOD	DoD Standardized Profiles - Internet Network Management Profile for DoD Communications	MIL-STD-2045-17507:7/94	Informational (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) - Part 1: Specification (Includes amendment 1 and 2 of ISO/IEC 9596-1:1990)	9596-1:1991	Informational (Approved)
IPC	ISO/IEC	Elements of Management Information Relating to OSI Network Layer Standards	10733:1993	Informational (Approved)
IPC	ISO/IEC	Elements of Management Information Related to OSI Data Link Layer Standards	10742:1994	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
CPC	X/Open	Management Protocol Profiles (XMPP)	C206 (11/93)	Informational (Approved)
CPC	IETF	Protocol Operations for Simple Network Management Protocol, version 2 (SNMPv2)	RFC 1448:1993	Informational (Approved)
IPC	ISO	OSI Remote Procedure Call (RPC) (Replaces DIS 11578 PT 1 Thru PT 4)	11578.2	Informational (Draft)
IPC	IAB	Simple Management Protocol (SMP)(Developed in response to an IETF request for an improved SNMP)	SMP	Informational (Draft)

3.9.5.5.2 Alternative specifications. Hewlett-Packard's Postmaster, on which the OSF DME's CMIP and Simple Network Management Protocol (SNMP) implementations are based, is also available.

3.9.5.5.3 Standards deficiencies. With its object-oriented approach, CMIS/CMIP has a relatively expensive initial application implementation cost. This flaw is offset by a low maintenance cost, because CMIS/CMIP allows objects to be added, and an associated level of management to be

provided, at a small incremental cost. There is no standard API to CMIS/CMIP. Only a limited number of narrowly focused applications are implemented with it. It lacks a complete set of associated object definitions needed for network management and sufficient associated security standards.

The SNMP is a simple request-and-reply protocol. It performs all its operations using a fetch-and-store paradigm, rather than defining a large set of commands. Effectively, the SNMP network manager is restricted to only two commands that are performed on Management Information Base (MIB) data items: "set" and "get." Variables are retrieved (get) or modified (set). All other operations are defined as side-effects of the "set" operation.

The SNMP's chief disadvantage is the fact that its simplicity severely limits the protocol's ability to satisfy users' requirements for event reporting, sufficient control, and extensibility. Because SNMP is so simplistic and limited, it provides more of a monitoring and data gathering capability than a management function.

The SNMP accommodates only limited event reporting by means of the "trap" mechanism. Other events must be discovered by the managing node by means of periodic polling. Its simplicity compromises its ability to support consistent or extensive addressing. It has limited security capabilities, and does not support threshold-driven performance notification except indirectly through side effects or "set" operations on MIB items. SNMP cannot be extended easily.

The SNMP has a high maintenance cost. Although the first implementation of SNMP is relatively inexpensive, SNMP's simplicity so severely limits its extensibility that future SNMP developments are more likely to occur in the form of new proprietary and standard Management Information Bases (MIBs) rather than as SNMP enhancements. Each additional MIB will require changes and additions to its existing specific applications to support new functions. New MIBs also will require a unique application code to be developed, modified, documented, and supported. MIB development and maintenance can result in a high cost to users and vendors and present a major SNMP concern.

The SNMP lacks an object-oriented approach to network management. The lack of object orientation is a major factor limiting the SNMP's extensibility and its ability to support legacy systems, support system and network management, and make complex distributed system management more intuitive.

It lacks the ability to manage a network of networks in which different managers must interact on a peer-to-peer basis.

Because the SNMP cannot be extended easily, and extensions require changes to SNMP applications, developing new SMP products rather than retooling existing ones probably will be less costly.

The future of SMP is uncertain because it is unclear whether vendors will want to develop new products for a protocol that is incompatible with the major systems management standards today (e.g., from ISO, NMF, X/Open, and OSF). SMP is still less functional than CMIS/CMIP.

The SMP is not an Internet standard. Although developed in response to a request issued by the Internet Engineering Task Force (IETF) for an improved SNMP, SMP was developed outside the IETF. Furthermore, the SMP developers do not plan to submit it as a proposed Internet standard. They feel that submitting SMP to a committee would subject it to alteration and a lengthy review, and would slow down development of a coherent technology.

SMP is not accepted by groups such as the Network Management Forum (NMF), X/Open, OSF, and the National Institute of Standards and Technology (NIST). These groups are resistant to SMP because it lacks an object-oriented approach to network management. Despite the improvements, without object orientation, SMP is still incompatible with the ISO and NMF network management model, as well as with the OSF's Distributed Management Environment (DME) and X/Open's systems management specifications. Vendors moving from SNMP to SMP may find it more cost effective to develop new SMP products.

SMP is not easily extensible, and like SNMP, is expensive to extend. This is largely due to SMP's lack of an object-oriented approach to network management.

3.9.5.5.4 Portability caveats. Nonstandard SNMP MIB definitions have proliferated.

The SNMP MIB is tailored to accommodate only Internet equipment. Despite the X/Open, OSF, and former UI (now X/Open) consolidated interface to CMIP and SNMP (X/Open Management Protocol (XMP) and CM-API), without object-orientation SNMP is still incompatible with the ISO and NMF network management model, as well as with the OSF's Distributed Management Environment (DME) and X/Open's systems management specifications.

SNMP's design does not lend itself to migration from and coexistence with legacy systems. For example, SNMP does not support the ability to send the same operation to different classes of objects (an important concept known in this context as "polymorphism," which CMIS/CMIP supports).

3.9.5.5.5 Related standards. The following standards are related to management information communication standards:

a. ISO/IEC 7498:1986: Management Framework.

b. ISO/IEC 8326:1987 and 8327:1987: Connection-Oriented Session Service and Connection-Oriented Session Protocol, respectively.

c. ISO/IEC 8326 AD 2: Connection-Oriented Session Service - Incorporation of Unlimited User Data.

d. ISO/IEC 8327 AD 2: Connection-Oriented Session Protocol - Incorporation of Unlimited User Data.

e. ISO/IEC 8571:1988: FTAM, as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if File transfer, Access, and Management functionality are required.

f. ISO/IEC 8649:1988 and 8650:1988: Association Control Service Element (ACSE) and Association Control Protocol (ACP), as specified in GOSIP Version 2, Section 4.2.7.1, as modified by the NMSIG agreements in Part 18 of the OIW Implementors Agreements.

g. ISO/IEC 8822:1988 and 8823:1988: Connection-Oriented Presentation Service and Connection-Oriented Presentation Protocol, respectively.

h. ISO/IEC 8824:1990: Abstract Syntax Notation 1 (ASN.1).

i. ISO/IEC 8825:1990: Basic Encoding Rules (BER) for ASN.1 .

j. ISO/IEC 9041:1990: (OSI Virtual Terminal), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if virtual terminal functionality is required.

k. ISO/IEC 9072-1:1989 and 9072-2:1989: ROSE and Remote Operations Protocol (ROP), as specified in the Remote Operations Part 1: Model Notation and Service Definition (ROSES) and the Remote Operations Part 2: Protocol Specification (ROSEP), and as modified by the NMSIG agreements clause 6.5.

l. ISO/IEC 10165-1:1993: SMI.

m. ISO/IEC 10165-2:1992: DMI.

n. ISO/IEC 10165-4:1992: Guidelines for the Definition of Managed Objects (GDMO).

o. CCITT X.400 Message Handling System (MHS), as specified in GOSIP Version 2 Sections 4.2.7.3 and 5.3.2, if message handling functionality is required.

p. NIST OSI Implementors Workshop (OIW) Implementor Agreements relating to the Presentation and Session layers, as specified in Part 5 (Upper Layer Agreements), clause 13.7, of the OIW Stable Implementation Agreements for OSI Protocols Version 3 (NIST Special Publication 500-224).

q. Open Software Foundation Distributed Computer Environment (DCE): Remote Procedure Call (RPC) Service Definition.

r. Plan to use IEEE 1327 Object Management API, or X/Open's XOM (on which 1327 is based) to simplify the management of networked managed resources in a CMIP environment. (See system management APIs BSA in part 8 for more information.)

s. RFC 1006:1987: ISO transport services on top of the TCP: version 3 (IAB Std 35).

3.9.5.5.6 Recommendations. All new systems and systems undergoing major upgrades should use the Internet Architecture Board (IAB) STD 15, SNMP (RFC 1157). Those persons conducting procurements that involve IAB standards should review the latest version of the IAB official protocol standards list to ensure that the appropriate RFCs are specified.

The PM should plan to use CMIS/CMIP for OSI/GOSIP networks and existing TCP/IP networks, because SNMP does not have the required functionality to manage distributed networks and is very expensive to maintain.

Until environments become distributed, SNMP is a suitable solution for stand-alone local area networks.

The PM also should plan to use either X/Open's XMP or OSF's CM-API (they are the same) as a common API to CMIP and SNMP. (See the system administration and management APIs BSA in part 8 for more information).

The CMOT users, vendors, and applications should be aware of some of the functional differences between OSI managed systems and Internet agents because CMIS/CMIP's more sophisticated and additional features may be difficult to map reliably to TCP/IP and SNMP.

A common protocol API should be used to access CMIP and SNMP. X/Open, Unix International, and OSF specify the same API. X/Open and Unix International call the API "XMP" (X/Open Management Protocol); OSF calls the same protocol CM-API (Consolidated Management API). Although XMP and CM-API provide an extra call specific to SNMP, because the SNMP "GetNext" function call does not work in an OSI environment, the consolidated management protocol API provides the union of the CMIP and SNMP protocols and service primitives consistently. It hides some of the differences between CMIP and SNMP. For most work, programmers and system managers need to learn only a single syntax to access both protocols.

3.9.5.6 Managed information base. Defined objects are network and system objects that can be managed by a network or system management application and are stored in a management information database.

3.9.5.6.1 Standards. Table 3.9-23 presents standards for managed information base.

TABLE 3.9-23 Managed information base standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	Structure of Management Information (SMI)	Standard 16/RFC-1155/RFC-1212	Mandated (Approved)
IPC	IAB	Management Information Base	Standard 17/RFC-1213	Mandated (Approved)
NPC	IEEE	POSIX System Administration - Part 2: Software Administration (former P1003.7.2)	1387.2:1995	Informational (Approved)
IPC	ISO/IEC	OSI Structure of Management Information (SMI), Part 1: Management Information Model	10165-1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Structure of Management Information (SMI), Part 2: Definition of Management Information (DMI)	10165-2:1992	Informational (Approved)
IPC	ISO/IEC	OSI Structure of Management Information (SMI), Part 4: Guidelines for the Definition of Managed Objects (GDMO)	10165-4:1992	Informational (Approved)
IPC	ISO/IEC	OSI Structure of Management Information (SMI), Part 5: Generic Management Information (GMI)	10165-5:1993	Informational (Approved)
NPC	IEEE	POSIX: System Administration - Part 3: User and Group Administration	1387.3:1996	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
CPC	NMF	Object Class Library Supplement: DIS GDMO Translation	Forum Library - Volume 1:Release 1.0 Definitions - Issue 1.3	Informational (Approved)
CPC	NMF	OSI/NM Forum Modeling Principles for Managed Objects Technical Report	NMF Technical Report	Informational (Approved)
CPC	IETF	Management Information Base for SNMP v2	RFC 1450:1993	Informational (Approved)
NPC	IEEE	POSIX: System Administration - Part 4: Print Administration (former P1003.7.1)	P1387.4	Informational (Draft)
NPC	OSI's Special Interest Group	Catalog of OSF Managed Object Definitions (Generic objects, and objects to represent hardware, the operating system (particularly OSF/1), application, users, distributed environments (particularly the DCE), and metadata.)	Catalog of OSF Managed Object Definitions	Informational (Formative (Working documents))
CPC	IETF	OSI Integrated Management (OIM): Management Information Base for TCP/IP Networks (MIB)	RFC XXXX	Informational (Formative)
GPC	NIST	Registry for managed objects	TBD Registry for managed objects	Informational (TBD)
CPC	IETF	OSI Internet Management: Management Information Base (CMIP over TCP/IP)(CMOT)(SNMP MIB II mapped into CMIP)	RFC 1214:1991	Informational (Historic (Not recommended))
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179:1992	Informational (Superseded)

3.9.5.6.2 Alternative specifications. There are no alternative specifications available.

3.9.5.6.3 Standards deficiencies. ISO's object model is targeted at networking and communications, rather than general system management. It is built around CMIP and is specific to CMIS services. Among other things, the ISO object model contains concepts such as the registration of objects and a class hierarchy. This registration is patterned around the way CMIS/CMIP objects are registered. This is of great concern to network management. A more generic extensible object model that can be specialized for many kinds of system and software objects and used with multiple types of communication systems (e.g., remote procedure calls) is needed for system management.

The ISO Guidelines for the Definition of Managed Objects (GDMO) formal object definition language syntax is highly specific to CMIP and uses the complex ISO CSI ASN.1 notation. This syntax lends itself to the definition of objects such as modems and other network devices. It is not necessarily suitable for defining more abstract objects, such as applications and operating systems, which are needed for general system management.

The OMG's objects lack the ability to have more than one interface. This ability, called "allomorphism," is taken from the ISO OSI management model's allomorphism requirement. This multiple interface ability makes it possible to identify different classes of objects (e.g., classes A, B, and C), then have an application operate on an instance of class A as if it were an instance of class B or C. Allomorphism is important because it allows the definition of enhanced versions of a managed object class that are backward compatible with previous versions. Migration costs are thereby reduced.

3.9.5.6.4 Portability caveats. Multiple object models are being defined by various organizations (e.g., ISO, the Object Management Group). These different models conflict with each other. Among other things, they differ in the way they represent objects, the object interfaces, the targeted application domain, and the targeted types of objects.

The OMG object model, on which the OSF object model is based, is a generic one, to which extensions can be added to specialize objects for different domains. In contrast, the ISO object model is targeted at networking and communications. It is built around CMIP and is specific to CMIS services. Although CMIS/CMIP is supposed to accommodate any management data, until now, the focus has been on network management.

The ISO, NMF, and IEEE P1387 distributed system administration groups define their managed objects using the ISO GDMO definition language. OSF is using its Interface, Inheritance, Implementation, and Installation (I4DL) definition language, which is based on the OMG's Interface Definition Language (IDL), to define its managed objects. Unfortunately, the GDMO, I4DL, and IDL interfaces defined by each of the object models affect the basic object model (which are different for ISO, OSF, and OMG) and make it difficult to use one object model's set of interfaces for another.

3.9.5.6.5 Related standards. The Object Management Group's Interface Definition Language (IDL) for defining generic objects is related to object definition standards.

3.9.5.6.6 Recommendations. All new systems and systems undergoing major upgrades should use the Internet Architecture Board (IAB) STD 16 and IAB STD 17. Those persons conducting procurements that involve IAB standards should review the latest version of the IAB official protocol standards list to ensure that the appropriate RFCs are specified. If recommended standards do not meet system requirements or are cost prohibitive, standards for the legacy systems may be used, as long as interoperability is not impacted. The use of legacy system standards may require a waiver from the appropriate authority.

3.9.5.7 Event management. Event management and notification services allow system managers and system administrators to be informed that a predefined system or network event of interest (e.g., additional resources needed) has occurred, so that the event may be managed in a predefined way that prevents network or system problems. Event management is related closely to fault and performance management, in that each of these services could make use of event management to log, track, and provide alerts based on relevant events.

3.9.5.7.1 Standards. Table 3.9-24 presents standards for event management.

TABLE 3.9-24 Event management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
GPC	NIST	Stable Implementation Agreements for Open System Environments, Ver. 8, Ed. 1	Special Pub. 500-224:12/94	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 5: Event Report Management Function	10164-5:1993	Informational (Approved)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Informational (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amend: Services For Reliable, Available, and Serviceable Systems (SRASS) (C Language)	P1003.1b	Informational (Emerging)

3.9.5.7.2 Alternative specifications. The following specifications are also available:

a. Banyon Systems' Network Event Logger (from Wang Laboratories) on which OSF's Event Notification Component is based.

b. Banyon Systems' PC library for the Network Event Logger, which filters and logs PC events locally and sends them to a Network Event Logger server on a host system for further processing. The OSF DME's PC Error Logging Component is based on this Banyon Systems' PC library.

3.9.5.7.3 Standards deficiencies. None of the event notification components in any of the consortia management systems are compatible with the IEEE P1003.1b specifications for event notification. OSF DME event management is intended to be used as the basis for commercial management systems, but is not currently supported by any products.

3.9.5.7.4 Portability caveats. Portability problems with the existing specifications are unknown.

3.9.5.7.5 Related standards. The following standards are related to event management and notification standards:

a. ISO/IEC DIS 11578.2: RPC (Replaces DIS 11578 PT 1 Thru PT 4.)

b. NIST APP - Special Pub. 500-230: 1995.

c. OSF: Distributed Computing Environment (DCE) Remote Procedure Call Component.

d. USL/Sun Microsystems: Open Network Computing (ONC) Remote Procedure Call (RPC) Component.

e. NIST FIPS 179-1:1995: Government Network Management Profile (GNMP).

f. ISO/IEC 9596-1:1991: OSI CMIP, Part 1: Specification.

g. IAB: RFC 1157: SNMP.

3.9.5.7.6 Recommendations. OMNIPoint 1 is recommended. The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications.

3.9.5.8 Input/Output control. (This BSA appears in both part 8 and part 9.) Input/Output (I/O) control standards include services such as device initialization, device attachment, asynchronous operation, error notification, raw I/O, and other services needed to implement logical device drivers in a system.

Input/output control enables control of different media devices over the network through software. The media devices include videocassette recorders, laser disc players, video cameras, CD players, and so on. Control capabilities may be available on the workstation through a graphical user interface (GUI). They are similar to the controls on the device, such as play, record, reverse, eject, and fast forward. Input/output control is important because it enables the operator to control video and audio remotely without requiring physical access.

3.9.5.8.1 Standards. Table 3.9-25 presents standards for input/output control.

TABLE 3.9-25 Input/Output control standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Emerging (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Emerging (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
NPC	IEEE	POSIX Part 1: Real Time System API Extensions	P1003.1d	Emerging (Draft)
NPC	IEEE	POSIX Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1a	Emerging (Draft)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C language], (as profiled by FIPS PUB 151-2:1993)	9945-1:1990	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.9.5.8.2 Alternative specifications. The following specifications are also available:

a. Berkeley 4.2/4.3 Unix.
b. OSF: OSF/1 (product implementation).

3.9.5.8.3 Standards deficiencies. POSIX.1 provides basic input/output primitives, but lacks the generalized services needed to implement device drivers for many types of devices. POSIX.1b provides support for asynchronous and synchronized I/O, but also lacks generalized services needed to implement device drivers for many types of devices.

3.9.5.8.4 Portability caveats. The "ioctl" function, which is associated with the control of an asynchronous device (including terminal characteristics) has been identified repeatedly as a source of portability problems. It is an old system call, and during the many years it has been in Unix, several variants have evolved. The differences appear at low levels. However, it is not always easy to spot these differences, because each "ioctl" is defined loosely and makes its own assumptions. As networking becomes more common, the device drivers executing some code may be located across a network, remote from the source of the system call. The many variants and interpretations of "ioctl," complicate networking because the same "ioctl" system call possibly cannot be used across a network to control a remote peripheral. For example, the SVID version of "ioctl" looks like a completely different call. Because of the difficulty in reaching agreement on a standardized version of the "ioctl," the POSIX standards groups eliminated "ioctl" from the standard early. Because the POSIX.1b real time group believes that most devices communicate using "ioctl," there was a move to reinstate and standardize "ioctl" in the P1003.1b standard. The final result, however, was the incorporation of specific "tc" (terminal control) functions to replace each "ioctl" function.

The use of "ioctl" calls to set certain terminal modes causes problems because a single, standard terminal interface or portable mechanism to set the modes of an asynchronous terminal does not exist. Such a standard has not been defined, because it would require the "raw" (unprocessed) and "cooked" (processed) modes to be defined. Defining these would create other problems. However, not defining them could cause application codes to be written in a nonportable way.

The SVID and XPG support the "ioctl" call as part of their device service interfaces. In practice, this support is different on every different implementation of these specifications. The "ioctl" function, while deprecated for asynchronous terminal control in favor of the POSIX.1 "tc" functions, is still required to control other, less common device types. Unfortunately there is no standard for programmatic control of video cameras, etc., even though every system which supports such a device will provide the basic control functionality needed in some way.

3.9.5.8.5 Related standards. The following standards are related to input/output control or input/output control standards:

a. ISO 10164-7: Security Management.

b. IEEE P1003.1e: Security Interface Standards for POSIX.

c. IEEE 1003.2d:1994: POSIX Batch Environment Amendments.

d. IEEE P1201.1: Uniform API-GUI.

e. NIST FIPS 179-1:1995: GNMP (Government Network Management Protocol): Authentication.

f. MIT Consortium: X Window System.

3.9.5.8.6 Recommendations. The mandated standards are recommended for input/output control. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. It specifies read/write functionality. The "tc-functions" were introduced into POSIX.1 to solve portability issues arising from "ioctl" calls. X/Open SUS covers all the core POSIX functions.

3.9.6 Fault monitoring. Fault monitoring services allow a system to react to the loss or incorrect operation of system components at various levels.

3.9.6.1 Software safety. (This BSA appears in both Part 2: Software Engineering and Part 9: System Management.) These standards provide procedures for identifying as safety-critical those CSCIs or portions thereof whose failure could lead to a hazardous system state (one that could result in death, injury, loss of property, or environmental harm). The developer shall develop a safety assurance strategy, including both tests and analyses, to assure that the requirements, design, implementation, and operating procedures for the identified software minimize or eliminate the potential for hazardous conditions. The objective is to eliminate hazards, and reduce the associated risk to a level of acceptability to the managing activity.

3.9.6.1.1 Standards. Table 3.9-26 presents standards for software safety.

TABLE 3.9-26 Software safety standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	System Safety Program Requirements	MIL-STD-882C: 1996	Adopted (Approved)
NPC	IEEE	Software Safety Plans	1228:1994	Informational (Approved)

3.9.6.1.2 Alternative specifications. No other specifications are known.

3.9.6.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.9.6.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.9.6.1.5 Related standards. None.

3.9.6.1.6 Recommendations. MIL-STD-882C is recommended.

3.9.6.2 Database recovery. (This BSA appears in both part 4 and part 9.) Database recovery refers to the ability to detect a failure in a system, recover from failure, and permit a slave copy to become a master copy, assuring data integrity and consistency.

3.9.6.2.1 Standards. Table 3.9-27 presents standards for database recovery.

TABLE 3.9-27 Database recovery standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	OSI Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element	9804:1990	Informational (Approved)
IPC	ISO/IEC	OSI Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Service Element	9805:1990	Informational (Approved)

3.9.6.2.2 Alternative specifications. No other consortia or de facto specifications are available.

3.9.6.2.3 Standards deficiencies. Deficiencies in database recovery standards are unknown.

3.9.6.2.4 Portability caveats. At present, CCR is not widely implemented, although most vendors intend to implement it. Therefore, one should make no assumptions about the degree of portability and interoperability existing for any database recovery utilities.

3.9.6.2.5 Related standards. The following standards are related to database recovery or database recovery standards:

a. ISO/IEC 10026 Parts 1, 2, and 3: Distributed Transaction Processing (DTP) protocol

b. X/Open XA Interface specification, which includes CCR's two-phase commitment

3.9.6.2.6 Recommendations. If CCR is desired (and it is necessary for multivendor, distributed database and distributed transaction processing), it must be referenced specifically in procurement specifications. Otherwise, vendors probably will propose products that do not meet this specification.

For the greatest portability, design applications as if CCR were not present.

3.9.6.3 Recovery and restart services for long running transactions. (This BSA appears in both part 4 and part 9.) Checkpoint and restart is provided for interactive transactions on centralized systems via the SQL "commit" and "rollback" commands, and for short-running transactions on distributed systems via the 2-Phase Commit specified in the ISO CCR standard. However, long running transactions require standardized checkpointing, restarting, and migration services and interfaces to prevent the loss of the transaction if a system fails or shuts down. Two APIs must be standardized for this purpose. One will allow application control of the checkpoint. The other will allow the transaction manager to control the checkpointing and restart activity over a range of heterogeneous resource managers.

3.9.6.3.1 Standards. Table 3.9-28 presents standards for recovery and restart services for long running transactions.

TABLE 3.9-28 Recovery and restart services for long running transactions standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 2:Shell and Utilities - Amendment 1: Batch Environment	1003.2d:1994	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API [illegible] (C language)	P1003.1a	Informational (Draft)
NPC	IEEE	POSIX, Part 1: System API - Amendment 2: Checkpoint/Restart Interface (C Language)	P1003.1m	Informational (Formative)

3.9.6.3.2 Alternative specifications. The following specifications are also available:

a. USL: Tuxedo
b. Transarc: Encina
c. NCR: Top End

3.9.6.3.3 Standards deficiencies. Based on a requirement from the P1003.15 Batch Queuing Extensions Standards Group, the POSIX.1 revision will specify application control of checkpointing. But this specification is geared to batch environments, and does not address the transaction manager's control of checkpoint, restart, or migration of services needed for a transaction processing environment. This need is not being addressed other than by de facto solutions.

1003.2d specifies some capabilities needed for checkpointing and restart in batch environments, but as a standard geared to batch environments, it does not address the transaction manager's control of checkpoint, restart, or migration of services.

3.9.6.3.4 Portability caveats. Without standardized interfaces to allow application control of checkpointing and transaction manager's control of checkpointing and restart activity, portability and interoperability across heterogeneous resource managers are nonexistent, except for short-

running transactions (which are controlled via SQL's "commit" and "rollback" commands and via ISO's CCR standard).

3.9.6.3.5 Related standards. The following standards are related to recovery and restart services or standards:

a. ISO 9041-1: Basic Class Virtual Terminal Protocol Specification
b. ISO 9075:1992: SQL 3rd edition
c. IEEE 1003.1b:1993: Real-Time Extension to POSIX
d. IEEE 1003.1c:1995: Threads Extension to POSIX

3.9.6.3.6 Recommendations. There is no recommendation for recovery and restart services.

3.9.6.4 Network error recovery. These are procedures for the detection and reconstitution of corrupted data, packet data units, and/or datagrams.

3.9.6.4.1 Standards. Table 3.9-29 presents standards for network error recovery.

TABLE 3.9-29 Network error recovery standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	Transmission Control Protocol	Standard 7/RFC-793	Mandated (Approved)
IPC	IAB	Host Requirements	Standard 3/RFC-1122/RFC-1123	Mandated (Approved)
IPC	IAB	The Point-to-Point Protocol (PPP)	Standard 51/RFC 1661	Mandated (Approved)
GPC	DOD	Transport Profile: Reliable End System Transport for DOD Communications	MIL-STD-2045-14500 Part 1:March 1994	Informational (Approved)
GPC	DOD	Internet Transport Profile for DOD Communications Wide Area Network Access (References ISO 8208 Information Processing Systems - Data communications - X.25 Packet Level Protocol for Data Terminal Equipment)	MIL-STD-2045-14502 Part 3:July 1994	Informational (Approved)
GPC	DOD	Transport Profile: Balanced Point-to-Point Digital Data Circuit	MIL-STD-2045-14500 Part 2:March 1994	Informational (Approved)
GPC	DOD	Transport Profile: Subnetwork for an Unbalanced Data Link	MIL-STD-2045-14500 Part 3:March 1994	Informational (Approved)
GPC	DOD	Internet Transport Profile for DOD Communications: Point-to-Point Links	MIL-STD-2045-14502 Part 2:July 1994	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.9.6.4.2 Alternative specifications. There are no alternative specifications.

3.9.6.4.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.9.6.4.4 Portability caveats. Connection-oriented transport has five levels of service that deal with reliability. These classes do not interoperate. Applications using different classes of transport service will have portability problems.

The X.25 equipment conforming to different specification dates (e.g., 1980, 1984, 1988, 1992) can have interoperability problems.

3.9.6.4.5 Related standards. There are no related standards.

3.9.6.4.6 Recommendations. Error recovery is one of the functions supported by the Transmission Control Protocol (TCP). The TCP should be used as specified in the IAB STD 7. The IAB STD 3 identifies and corrects errors in the TCP.

MIL-STD-2045-14500-01 is recommended for legacy systems interoperability. It specifies the details necessary to meet DoD requirements for connection-oriented transport service over a connectionless network service. It uses class four transport protocol as one of its base standards. It is an error detection and recovery class that assumes the underlying network service is unreliable. MIL-STD-2045-14500 parts 2 and 3 are recommended for legacy systems interoperability. Use of LAPB for Balanced Point to Point Digital Data Circuit should comply with MIL-STD-2045-14500-02. For an Unbalanced link, LAPB should be used as specified in MIL-STD-2045-14500-03.

If recommended standards do not meet system requirements, or are cost prohibitive, standards for the legacy systems may be used as long as interoperability is not impacted. The use of legacy systems standards may require a waiver from the appropriate authority. MIL-STD-2045-44000 is an emerging standard. It uses TCP and UDP with enhancements to meet specific requirements for high-stress resource constrained environments.

3.9.6.5 Fault management. (This BSA appears in part 8 and part 9.) Fault management services allow a system to react to the loss or incorrect operation of system components. Fault management services encompass services for fault detection, isolation, diagnosis, recovery, and avoidance. Fault management may make use of event management facilities. In practice, fault management and performance management products often incorporate event management functions.

3.9.6.5.1 Standards. Table 3.9-30 presents standards for fault management.

TABLE 3.9-30 Fault management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 4: Alarm Reporting Function	10164-4:1992	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 5: Event Report Management Function	10164-5:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 6: Log Control Function	10164-6:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 12: Test Management Function	10164-12:1994	Informational (Approved)
NPC	SAE	General Open Architecture (GOA) Framework	AS 4893 (Committee AS-5)	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 14: Confidence and Diagnostic Test Categories	10164-14	Informational (Draft)
NPC	IEEE	POSIX, Part 1: System API - Amendment: Services for Reliable, Available, and Serviceable Systems (CRASS) (C Language)	P1003.1h	Emerging (Formative)
NPC	IEEE	POSIX, Part 1: System API - Amendment 2: Checkpoint/Restart Interface (C Language)	P1003.1m	Emerging (Formative)
NPC	IEEE	POSIX, Part 1: System API, Amendment 2: Recovery Limit Interface (C Language)	P1003.1p	Emerging (Formative)

3.9.6.5.2 Alternative specifications. The following specifications for network fault reporting are available:

a. Banyon Systems's Network Event Logger (originally developed by Wang Laboratories), on which OSF's DME event services and logging services are based.

b. Gradient Technologies: PC Event system integrated with a Banyon Systems-based Network Event Logger PC library and a PC Ally server on which OSF has based its PC event and logging component.

3.9.6.5.3 Standards deficiencies. The present ISO 10164-4, "Alarm Reporting Function," 10164-6, "Log Control Function," 10164-5, "Event Report Management Function," 10164-12, "Test Management Function," and 10164-14, "Confidence and Diagnostic Testing Service" standards were designed with network configuration in mind. Theoretically, these standards should be able to be used for configuration management of any computer system. Little work has been done in this area, either in standards groups or in products. Therefore, exactly how these standards should be used in host management is undetermined.

Although several standard libraries of object classes that allow a common view of network resources and fault management of network resources are planned, few are available or sufficiently complete. For example, these library specifications have incomplete object definitions for modems, OSI routers, and transport connections. Based on U.S. Federal Government needs (as shown by NIST surveys), the GNMP added more object class specifications and definitions. These include the following objects: LANs, X.25 Wide-Area-Networks (WANs), Integrated Services Digital Network (ISDN), Fiber Distributed Data Interface (FDDI), modems, bridges, links, and a rudimentary capability to manage OSI routers and transport connections.

Phase 2 GNMP objects also will include protocol software (layers 3-7), routers, terminal servers, Message Transfer Agents (MTAs), Private Branch Exchange (PBXs), and circuit switches.

Versions 1.0 and 2.0 of the GNMP currently specify only network management capabilities. Not until Version 3.0 will the GNMP specify the management information required for general system management, such as host computer configuration and management, operating systems, and database management systems.

The present ISO standards and GNMP specifications require ISO CMIS/CMIP for the communications of management information and ISO OSI networking protocols. Plans are for the GNMP eventually to provide a capability to integrate the present GNMP with SNMP also. One reason for this goal is the widespread use of SNMP.

No Ada bindings exist for any of the ISO or consortia system management specifications.

Fault management should make use of general event management such as OSF DME event services, but most products currently implement their own event management facilities.

Finally, standards are needed for problem reporting and tracking, diagnostic standards for hardware and software, and fault isolation.

3.9.6.5.4 Portability caveats. Portability problems with existing standards are unknown.

3.9.6.5.5 Related standards. The following standards are related to fault management or fault management standards:

a. ISO/IEC 7498-4:1989: Management Framework.

b. ISO/IEC 8571:1988: File Transfer, Access, and Management (FTAM), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if File transfer, Access, and Management functionality are required.

c. ISO/IEC 8650:1988: Association Control Service Element (ACSE), as specified in GOSIP Version 2, Section 4.2.7.1, as modified by the NMSIG agreements in Part 18 of the OIW Implementors Agreements.

d. ISO/IEC 8824:1990: Specification of Abstract Syntax Notation 1 (ASN.1).

e. ISO/IEC 8825:1990: Specification of Basic Encoding Rules for ASN.1.

f. ISO/IEC 9041:1990: (OSI Virtual Terminal), as specified in GOSIP Version 2 Sections 4.2.7.2 and 5.3.1, if virtual terminal functionality is required.

g. ISO/IEC 9072:1989: Remote Operations Service Element (ROSE), as specified in the Remote Operations Part 1: Model Notation and Service Definition (ROSES), and the Remote Operations Part 2: Protocol Specification (ROSEP), and as modified by the NMSIG agreements clause 6.5.

h. ISO/IEC 9595:1991: Common Management Information Service (CMIS).

i. ISO/IEC 9596:1991: Common Management Information Protocol (CMIP).

j. ISO/IEC 10165-1:1993: Structure of Management Information (SMI).

k. ISO/IEC 10165-2:1992: Definition of Management Information (DMI).

l. ISO/IEC 10165-4:1992: Guidelines for the Definition of Managed Objects (GDMO).

m. ISO/IEC DIS 11578.2: Remote Procedure Call.

n. CCITT X.400 Message Handling System (MHS), as specified in GOSIP Version 2 Sections 4.2.7.3 and 5.3.2, if message handling functionality is required.

o. IEEE 1224:1993: OSI Abstract Data Manipulation (Object Management) API - Language Independent Specification.

p. IEEE 1327:1993: OSI Abstract Data Manipulation (Object Management) API - C Language Binding.

q. NIST OSI Implementors Workshop (OIW) Implementor Agreements relating to the Presentation and Session layers, as specified in Part 5 (Upper Layer

Agreements), clause 13.7 of the OIW Stable Implementation Agreements for OSI Protocols Version 3 (NIST Special Publication 500-224).

r. Internet RFC 1155: Structure and Identification of Management Information for Internets based on TCP/IP.

s. Internet RFC 1157: Simple Network Management Protocol.

t. Internet RFC 1158: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

u. X/Open: OSI-Abstract-Data Manipulation API (XOM) (Object Management).

3.9.6.5.6 Recommendations. To build or procure fault management applications, users must identify the system management functions that are applicable to their requirements. Then they must identify the various specifications within the ISO 10164 and 10165 standards related to these requirements. Finally, they must specify the requirements and the related standards in the RFP.

The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications. It replaces FIPS 179 (GNMP) in Version 3.0 of the NIST Application Portability Profile.

3.9.6.6 Storage device management. (This BSA appears both in part 8 and part 9.) Storage device management is familiar to most people as "Logical Volume Management." With logical volume management, a logical volume manager provides disk partition flexibility by allowing the disk partitions to grow automatically as the system runs, and by allowing files to span physical volumes. This allows a given file to be larger than any one disk. This flexibility is possible because the logical volume manager manages the disk space by creating what it calls "logical volumes." The logical volume manager determines the correspondences between the logical volumes and the actual physical volumes. A logical drive is an allocated part of a physical drive designated and managed as an independent unit. Hierarchical storage management and archiving addresses the ability to handle different levels of storage transparently, such as disks, tapes, and juke boxes.

3.9.6.6.1 Standards. Table 3.9-31 presents standards for storage device management.

TABLE 3.9-31 Storage device management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Distributed File Service (DFS)	DCE 1.1 DFS:1994	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE): Network File Service (NFS)	DCE 1.1 NFS:1994	Informational (Approved)
CPC	OSF	OSF/1 Operating System	OSF/1 O.S.	Informational (Approved)
CPC	UDI Group	Uniform Driver Interface (UDI) Specification	UDI Rev 0.91	Informational (Formative)

3.9.6.6.2 Alternative specifications. Future releases of SVR4 will support the Logical Volume Manager, but no other alternative specifications are available.

3.9.6.6.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.9.6.6.4 Portability caveats. Portability caveats are unknown at this time.

3.9.6.6.5 Related standards. No standards are related to storage device management.

3.9.6.6.6 Recommendations. Open Software Foundation's Distributed File Service is recommended. Logical volume managers are extremely valuable, as many system managers know who have had to back up a system, take it down, repartiation it to accommodate the growth of applications and data in certain partitions, and restore the system, only to do the same thing months later. The logical volume manager eliminates this problem by allowing partitions to grow dynamically.

3.9.6.7 Backup and restore. (This BSA appears both in part 8 and part 9.) Backup and restore standards provide facilities and interfaces to save data as a precaution to system failure and restore the system to a previous data state after failure.

3.9.6.7.1 Standards. Table 3.9-32 presents standards for backup and restore.

TABLE 3.9-32 Backup and restore standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Single UNIX Specification (Spec. 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C436 (9/94)	Emerging (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	ANSI	Recorded Magnetic Tape for Information Interchange (1600 cpi, Phase Encoded)	X3. 39-1986 (R1992)	Informational (Approved)
NPC	ANSI	Recorded Magnetic Tape for Information Interchange (6250 cpi, Group-Coded Recording)	X3. 54-1986 (R1992)	Informational (Approved)
CPC	OSF	OSF/1 Operating System	OSF/1 O.S.	Informational (Approved)
NPC	IEEE	POSIX - Part 1: System API Supplement - Removable Media Support	P1003.1k	Emerging (Formative)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C language] (as profiled by FIPS PUB 151-2:1993)	9945-1:1990	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.9.6.7.2 Alternative specifications. The "dd" utility is useful for data copy with optional conversion that promotes portability, (e.g., ASCII to EBCDIC) or for record conversion with discrete record sizes, or multiple sector reads/writes to disk. The Berkeley Unix "dump" command is also available. The OSF's OSF/1 "tar" and "cpio" utilities and USG's System V Release 4 (SVR4) are also av. lable.

3.9.6.7.3 Standards deficiencies. Although the "tar" and "cpio" commands can be used to back up disks, they are very limited in capability. "tar" and "cpio" are copy commands. These commands do not perform incremental backups. Furthermore, "tar" does not span multiple disks. No Ada bindings exist for distributed backup and restore standards.

3.9.6.7.4 Portability caveats. The "ustar" format is an extension of the historical "tar" archive format and, as such, may be read by historical implementation of the "tar" command. The POSIX.2 "pax" command has been developed as a replacement for both "tar" and "cpio"

commands. It can read and write "ustar" and "cpio" archives, and most implementations have been extended to read historical "tar" format archives as well.

The "cpio" command can produce two different types of archives: "character"and "binary." The binary archives are non-portable, and cannot be read except on the same platform on which they were produced. POSIX documents only the character "cpio" format, and the "pax" command is only guaranteed to be able to read the character format.

The Berkeley Unix-based set of "backup" commands (e.g., "dump" and "rdump") are not the same as the backup commands based on System V (SVID) (e.g., "backup," "bkexcept,"). The two backup systems have different interfaces and do not work in a compatible manner.

3.9.6.7.5 Related standards. The following standards are related to backup and restore or backup and restore standards.

a. ISO/IEC 9595: CMIS.

b. ISO/IEC 9596: CMIP.

c. ISO/IEC DIS 11578.2: RPC.

d. Network Management Forum: OMNIPoint 1.

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

f. Internet RFC 1157: Simple Network Management Protocol.

g. Internet RFC 1158: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

3.9.6.7.6 Recommendations. ISO/IEC 9945-1 and ISO/IEC 9945-2 archiving services are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. "Pax" was commissioned for POSIX.2 because "tar" and "cpio" were considered inadequate. "Pax" is similar to "tar" and "cpio." The "tar" and "cpio" formats are expected to be retired from a future version of POSIX.1 in favor of the newer "ustar" format.

3.9.6.8 Hardware error and event conditions. (This BSA appears in both part 8 and part 9.) An event is an unsolicited communication from a hardware device to a computer operating system, application, or driver. Events are generally attention-getting messages, allowing a process to know when a task is complete or when an external event occurs. Error conditions (e.g., system failures, unauthorized access attempts, or strange glitches) must be detected and reported so corrective action can be taken to minimize system or network problems. (See the BSA on error and event logging for more information on tracking errors.)

Offline diagnosis of events which have been written in encoded form to the system log is termed event classification. Encoded events which are written to the system log for later analysis form the raw material for algorithms designed to diagnose and passivate faults, that is to prevent them from being reactivated. Offline classification of errors or events which are indicative of the potential failure of a component can be conducted only when the required information has been saved. Algorithms designed to improve system maintenance and to shorten the duration of outages generally scan the system event log for patterns of event types. Such algorithms can be used to predict imminent failure of software or hardware components. This analysis of logged events could also be processed in parallel while the main system continues to perform.

Services for the detection of events come in two basic forms: active and passive. Events come in two types, those which are anomalous and those which are not. Anomalous events may be classified into two categories: errors, and events which are indicative of a fault which is not yet producing errors, but is the cause of some degradation in system performance. P1003.1h is already addressing passive errors in their draft standard.

3.9.6.8.1 Standards. Table 3.9-33 presents standards for hardware error and event conditions.

TABLE 3.9-33 Hardware error and event conditions standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990) and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Emerging (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Emerging (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) - Amend: Technical Corrigenda to Real Time Extension [C Language]	1003.1i:1995	Informational (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API Extensions (C language)	P1003.1a	Emerging (Draft)
NPC	IEEE	POSIX, Part 1: System API - Amend: Services for Reliable, Available, and Serviceable Systems (SRASS) IC	P1003.1h	Emerging (Formative)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
		[illegible]		
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.9.6.8.2 Alternative specifications. The OSF's OSF/1 (product implementation) is also available.

3.9.6.8.3 Standards deficiencies. POSIX.1 has limited event management capabilities.

3.9.6.8.4 Portability caveats. Symbolic error numbers are a set of names defined for error numbers set by the "exec" functions to indicate the nature of an error condition that has occurred. Symbolic error numbers have been around for a long time and are reasonably stable. However, many implementations, especially the newer ones, use symbolic error numbers that are different from one another. Applications using such new, different symbolic error numbers are not portable except to implementations using the same error number set.

POSIX, X/Open, and SVID support many of the same symbolic error numbers, with some exceptions. For example, POSIX does not support the error symbols "EIDRM" (indicating an identifier has been removed from the system), "ENOMSG" (required message not in the message queue), and "ETXTBSY" (attempt to overwrite active procedure), even though X/Open, and SVID support them. Other differences in symbolic error numbers occur in the following error symbols: "EBADMSG," "ENOSR," "ENOSTR," "EPROTO," "ERESTART," and "ETIME."

Symbolic error numbers provide portability only if programmers and vendors implement programs using them. Implementations using numeric numbers instead of symbolic error names and numbers are not portable.

POSIX, X/Open, and SVID allow additional implementation-defined symbolic error names to be created. Such implementation-defined symbolic error numbers may be a necessity for a particular application. These values are usually returned by extended functionality, not defined by POSIX.1. The SVID, for example, defines the symbolic errors "EBADMSG", "ENOSR", and "ENOSTR" which are returned by the kernal "STREAMS" subsystem. These new symbolic error numbers should be portable among all systems which provide the underlying functionality. The longest of the symbolic error number names is "ENAMETOOLONG."

X/Open's Single Unix Specification (Spec 1170) has aligned XPG4 with POSIX in the areas where they overlap. Thus any XPG4 or Single Unix conforming system is guaranteed to respond with the same symbolic error value although, as discussed above, the actual error number may vary.

3.9.6.8.5 Related standards. The following standards are related to hardware error conditions:

a. IEEE 1003.2:1992: POSIX - Shell and Utility Application Interface.

b. IEEE R1003.5:1992: Ada Language Binding for POSIX (under revision).

c. IEEE P1003.1e: Security Interface Standards for POSIX.

d. IEEE P1387.1: POSIX System Administration - Part 1: Overview.

e. IEEE 1387.2:1995: POSIX System Administration - Part 2: Software.

f. IEEE P1387.3: POSIX System Administration - Part 3: User and Group Administration.

g. IEEE P1003.1g: Protocol Independent Interfaces.

h. IEEE 1224.2:1993: Directory Services API - Language Independent.

i. IEEE 1224.1:1993: X.400 Based Electronic Messaging API.

j. IEEE P1238.1: OSI Applications Program Interface - FTAM.

k. IEEE P1351: OSI Application Interfaces - ACSE.

3.9.6.8.6 Recommendations. The mandated standards are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. Federal Information Processing Standard (FIPS) 151-2 should also be consulted. It adopted ISO 9945-1:1990 and is still applicable to the 1996 version. IEEE 1003.1b added asynchronous event notification to the original IEEE 1003.1. FIPS 151-2 specifies the read/write return options. SUS supports additional error symbols.

To get the better event management capabilities needed for networking, communications, transaction processing, and real time applications, explicitly specify the IEEE 1003.1b standard's real time signals option for asynchronous event notification. For U.S. Federal Government procurements, the NIST Application Portability Profile (APP) and FIPS 151-2 have some special file and directory requirements:

a. The APP and FIPS 151-2 require support for the error message "ENAMETOOLONG" for the open command.

b. The APP and FIPS 151-2 require read() calls and write() calls that are interrupted by a signal after they have successfully read or written data shall return the number of bytes the system has read. POSIX allows the return of either the number of

bytes read or written or a return of -1 with "errno" set to [EINTR] after a successful read or write.

To get greater functionality than POSIX provides, establish the error management interfaces provided by X/Open as an internal standard. The problem is that in implementations compliant with POSIX, many specific system calls have differences in their error messages and exception management handling. These system call commands must be analyzed to see which error messages to specify for certain critical commands, as the NIST did in developing FIPS 151-1. A second problem occurs because X/Open, the SVID, and OSF specify more functionalities than POSIX. Even when these functionalities are the same, X/Open's, the SVID's, and OSF/1's error messages are often different. In general, X/Open's error messages for specific system calls tend to be the same, but they differ from OSF/1's, which is the same as Berkeley UNIX's.

3.9.6.9 Event management. Event management and notification services allow system managers and system administrators to be informed that a predefined system or network event of interest (e.g., additional resources needed) has occurred, so that the event may be managed in a predefined way that prevents network or system problems. Event management is related closely to fault and performance management, in that each of these services could make use of event management to log, track, and provide alerts based on relevant events.

3.9.6.9.1 Standards. Table 3.9-34 presents standards for event management.

TABLE 3.9-34 Event management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
GPC	NIST	Stable Implementation Agreements for Open System Environments, Ver. 8, Ed. 1	Special Pub. 500-224:12/94	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 5: Event Report Management Function	10164-5:1993	Informational (Approved)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Informational (Approved)
NPC	IEEE	Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension (C language)	1003.1b:1993	Informational (Approved)
NPC	IEEE	POSIX Part 1: System API - Amend: Services for Reliable, Available, and Serviceable Systems (SRASS) (C Language)	P1003.1b	Informational (Formative)

3.9.6.9.2 Alternative specifications. The following specifications are also available:

a. Banyon Systems' Network Event Logger (from Wang Laboratories) on which OSF's Event Notification Component is based.

b. Banyon Systems' PC library for the Network Event Logger, which filters and logs PC events locally and sends them to a Network Event Logger server on a host system for further processing. The OSF DME's PC Error Logging Component is based on this Banyon Systems' PC library.

3.9.6.9.3 Standards deficiencies. None of the event notification components in any of the consortia management systems are compatible with the IEEE P1003.1b specifications for event notification. OSF DME event management is intended to be used as the basis for commercial management systems, but is not currently supported by any products.

3.9.6.9.4 Portability caveats. Portability problems with the existing specifications are unknown.

3.9.6.9.5 Related standards. The following standards are related to event management and notification standards:

a. ISO/IEC DIS 11578.2: RPC (Replaces DIS 11578 PT 1 Thru PT 4.)

b. NIST' APP - Special Pub. 500-230: 1995.

c. OSF: Distributed Computing Environment (DCE) Remote Procedure Call Component.

d. USL/Sun Microsystems: Open Network Computing (ONC) Remote Procedure Call (RPC) Component.

e. NIST FIPS 179-1:1995: Government Network Management Profile (GNMP).

f. ISO/IEC 9596-1:1991: OSI CMIP, Part 1: Specification.

g. IAB: RFC 1157: SNMF.

3.9.6.9.6 Recommendations. OMNIPoint 1 is recommended. The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications.

3.9.6.10 Process checkpoint and restart. (This BSA appears both in part 8 and part 9.) Checkpoint and restart is a method of recovering from a system failure. A checkpoint is a copy of the computer's memory saved periodically on disk along with the current register settings (e.g., the last instruction executed). In the event of any failure, the last checkpoint serves as a recovery point. When the problem has been fixed, the restart program copies the last checkpoint into memory, resets all the hardware registers, and starts the computer from that point. Any transactions in memory after the last checkpoint was taken until the failure occurred will be lost. Checkpoint restart is helpful in any system running long jobs and requiring more time than can be expected between system down-times, and in any job that would be inconvenient to start over in the event of a system failure.

3.9.6.10.1 Standards. Table 3.9-35 presents standards for process checkpoint and restart.

TABLE 3.9-35 Process checkpoint and restart standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	POSIX, Part 1: System API - Amendment x: Checkpoint/Restart Interface (C Language)	P1003.1m	Emerging (Formative)

3.9.6.10.2 Alternative specifications. The only other specifications available are proprietary.

3.9.6.10.3 Standards deficiencies. P1003.1a does not specify how files and directories are identified in the checkpoint file.

3.9.6.10.4 Portability caveats. One checkpoint restart implementation provides a value of "RESTART_FORCE" to restart a checkpoint file or directory, whether or not it could be restarted rationally. This behavior cannot be used in a portable way, since no predictable meaning exists for restarting a process that was in a condition that could not be checkpointed.

3.9.6.10.5 Related standards. ISO IS 9804/9805: CCR is related to process checkpoint and restart.

3.9.6.10.6 Recommendations. Too many unresolved issues are in the checkpoint restart specification in the P1003.1m draft standard to specify the emerging checkpoint restart specification. Issues range from the error codes to how much of the process state to specify explicitly.

Checkpoint/restart, originally in P1003.1a system services as a separate API is now a separate IEEE project work item under P1003.1m. This work was started by the Super Computer and Batch processing systems working groups in conjunction with the P1003.1a working groups to provide mechanisms to suspend a long executing job and/or provide checkpoints along the way so it could be restarted if something happened during execution.

3.9.6.11 Error and event logging. (This BSA appears both in part 8 and part 9.) Error logging is the automatic logging of errors and events to a log (special file) to avoid system or network faults (by detecting that the operation of a component is approaching the edge of its operational range) and to provide a historical record that can be studied to diagnose faults after their occurrence and perhaps prevent their happening in the future.

On the detection of events of interest, the operating system may automatically write the encoded event to the system log and/or may notify a process of the occurrence. This is certainly the case when an error with a high severity level is detected. Logging or notification may occur at any time in the operation of a system. They may occur when an application or the operating system has detected an error, when an event has been generated during event classification (especially if the event is indicative of imminent failure of a component), or when an event is severe and requires the immediate attention of a process and when a corrective action is taken, such as when a processor(hardware) or process(software) is being registered for service.

3.9.6.11.1 Standard. Table 3.9-36 presents standards for error and event logging.

TABLE 3.9-36 Error and event logging standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Adopted (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 4: Alarm Reporting Function	10164-4:1992	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 5: Event Report Management Function	10164-5:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 6: Log Control Function	10164-6:1993	Informational (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Emerging (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Emerging (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amend: Services for Reliable, Available, and Serviceable Systems (SRASS) [C Language]	P1003.1h	Emerging (Formative)

3.9.6.11.2 Alternative specification. The following specifications are also available:

a. Banyon Systems' Network Event Logger (NeL) (from Wang Laboratories) on which OSF's Event Notification Component is based.

b. Banyon Systems' PC library for the Network Event Logger (NeL), which filters and logs PC events locally and sends them to a Network Event Logger server on a host system for further processing.

3.9.6.11.3 Standard deficiencies. No Ada bindings are available for any of the consortium's system management Error Logging Components.

3.9.6.11.4 Portability caveats. Portability problems related to the existing standards are unknown

3.9.6.11.5 Related standards. The following standards are related to error logging standards:

a. ISO/IEC DIS 11578.2: OSI - RPC (Replaces DIS 11578 PT 1 Thru PT 4).
b. NIST APP - Special Pub. 550-230:1995.
c. OSF: DCE RPC Component.
d. USL/Sun Microsystems: Open Network Computing (ONC) RPC Component.

3.9.6.11.6 Recommendations. OMNIPoint 1 is recommended. The OMNIPoint program defines a collection of specifications for the management of network and distributed systems using open standards and specifications.

3.9.7 Security monitoring. Security monitoring provides management services which contribute to the protection of open systems information resources in accordance with applicable security policies.

3.9.7.1 System development. (This BSA appears in part 2, part 9, and part 10.) Development of secure systems requires that security engineering be a key discipline in conjunction with other system, software, and hardware engineering activities.

3.9.7.1.1 Standard. Table 3.9-37 presents standards for system development.

TABLE 3.9-37 System development standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Network Interpretation	NCSC-TG-005, Version 1: 1987	Mandated (Approved)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
GPC	DOD	FORTEZZA Cryptologic Programmers' Guide	MD40000501-1.52: 1996	Mandated (Approved)
GPC	DOD	FORTEZZA Application Implementors' Guide	MD4002101-1.52: 1996	Mandated (Approved)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Informational (Approved)
IPC	ISO/IEC	Software Life Cycle Processes	12207:1995	Informational (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Guidelines for Security of Computer Applications	FIPS PUB 83:1980	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Abstract Service Definition: (same as ITU-T X.511 (1993))	9594-3:1993 (or 1994)	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Procedures for Distributed Operations:(same as ITU-T X.519(1993))	9594-4:1993 (or 1994)	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Authentication Framework (same as ITU-T X.509 (1993))	9594-8:1993 (or 1994)	Informational (Approved)
CPC	X/Open	Generic Security Service API (GSS-API) Base	C441 (12/95)	Informational (Approved)
NPC	IEEE	POSIX Part 1: System API - Amendment 8: Protection, Audit, and Control Interfaces (C Language). Draft 15	P1003.1e: 1995	Legacy (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.9.7.1.2 Alternative specification. There are no alternative specifications.

3.9.7.1.3 Standard deficiencies. Deficiencies in the existing standards are unknown.

3.9.7.1.4 Portability caveats. If FORTEZZA services are used, the following guidelines should be consulted:

a. MD4002101-1.52, 3/5/96, FORTEZZA Application Implementors' Guide

b. MD400501-1.52, 1/30/96, FORTEZZA Cryptologic Programmers' Guide, Revision 1.52

3.9.7.1.5 Related standards. DOD Directive 5200.28 "Security Requirements for Automated Information Systems (AISs)," provides the DOD-wide program for AIS security. It provides mandatory, minimum AIS security requirements for systems processing classified, sensitive but unclassified, and unclassified information. For intelligence systems, Director, Central Intelligence Directive (DCID) 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks," and "Security Manual for Uniform Protection of Intelligence Information Processed in Automated Information Systems and Networks," should be used in conjunction with DOD 5200.28-STD. The following guidelines also are for use with DOD 5200.28-STD:

a. NCSC-TG-006, Version 1, 28 March 1988, A Guide to Understanding Configuration Management in Trusted Systems

b. NCSC-TG-007, Version 1, 2 October 1988, A Guide to Understanding Design Documentation in Trusted Systems

c. NCSC-TG-008, Version 1, 15 December 1988, A Guide to Understanding Trusted Distribution in Trusted Systems

d. NCSC-TG-018, Version 1, July 1992, A Guide to Understanding Object Reuse in Trusted Systems

e. NCSC-TG-023, Version 1, July 1993, A Guide to Understanding Security Testing and Test Documentation in Trusted Systems

3.9.7.1.6 Recommendations. The standards listed as mandated are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. MIL-STD-498 contains requirements for security and privacy for software development and documentation. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management, and acquirer-supplier interaction. The two guides are expected to be final by September 1997. The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 can be used for transition from MIL-STD-498, subject to Agency/Service approval, until organizational processes for IEEE/EIA 12207US are in place.

If FORTEZZA services are used, the following two guidelines should be consulted:

a. MD4002101-1.52, 3/5/96, FORTEZZA Application Implementors' Guide

b. MD4000502-1.52, 1/30/96, FORTEZZA Cryptologic Programmers' Guide, Revision 1.52

3.9.7.2 Security management. (This BSA appears in part 7, part 8, part 9, and part 10.) Security management is a particular instance of information system management. Security management provides supporting services that contribute to the protection of information and resources in open systems in accordance with information domain and information security policies. The basic elements that must be managed are users, security policies, information, information processing systems that support one or more security policies, and the security functions that support the security mechanisms (automated, physical, personnel, or procedural) used to implement security services. For each of these elements, the managed objects that constitute them must be identified and maintained. For example, users must be known and registered, security policies must be represented and maintained and information objects must be identified and maintained. Security policies, security services and security mechanisms are the first classes of managed objects.

3.9.7.2.1 Standards. Table 3.9-38 presents standards for security management.

TABLE 3.9-38 Security management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Network Interpretation	NCSC-TG-005, Version 1: 1987	Mandated (Approved)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
IPC	ITU-T	The Directory: Procedures for Distributed Operation (X-ref: ISO 9594-4)	X.518: 1993	Informational (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) - Part 1: Specification (Includes amendment 1 and 2 of ISO/IEC 9596-1:1990)	9596-1:1991	Informational (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 7: Security Alarm Reporting Function (same as ITU-T X.736)	10164-7:1992	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 8: Security Audit Trail Function (same as ITU-T X.740)	10164-8:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 9: Objects and Attributes for Access Control	10164-9:1995	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.9.7.2.2 Alternate specifications. There are no alternative specifications.

3.9.7.2.3 Standards deficiencies. Deficiencies exist in standardization of security policy rule representation; key management, including generation, distribution, and accounting; audit information formats; exchange of security management information; and remote security management.

The DGSA principle of decision and enforcement separation requires that the functions determining how to enforce a security policy and the actual enforcement of the policy be implemented independently. That is, the enforcement mechanisms do not need any knowledge of security policy. Standards are needed for object class definitions for classes of managed objects and for methods of representing security policy.

The DGSA calls for a separation mechanism, such as separation kernel, to mediate all calls to security critical functions to ensure that strict isolation is maintained. Standardization of object class definitions for management of critical functions used within the separation kernel is needed.

The present ISO/IEC 10164-7 "Security Alarm Reporting Function," and 10164-8, "Security Audit Trail Function," standards were designed with network security in mind. Little work has been done, either in standards groups or in products, on how to use these standards for general system management (e.g., computer systems and software).

FIPS PUB 179-1 supersedes FIPS PUB 179. The present GNMP specifications require ISO CMIS/CMIP to communicate management information and ISO OSI networking protocols. Plans are for the GNMP eventually to provide a capability to integrate the present GNMP with SNMP. One reason for this goal is the widespread use of SNMP.

No Ada bindings exist for any of the ISO or consortia system management specifications.

The IEEE POSIX Security Working Group (formerly P1003.5) is defining security extensions to the base POSIX interface standard (ISO 9945-1), to include support for audit, privilege, discretionary and mandatory access control, and information labels. These have been redesignated IEEE P1003.1e and IEEE P1003.2c. The draft standards are still incomplete, and the specifications may change.

The POSIX/UNIX permission bits are inadequate for fine-grained control over exactly which users can perform specified actions to particular files.

In the IETF, efforts to develop an acceptable security standard for SNMPv2 have been on hold since September 1995 when the IETF SNMP Working Group failed to agree on the proposals submitted. Since then, two sets of proposals for providing SNMPv2 security have emerged. The first set of proposed specifications, the User-based Security Model (USEC), also referred to as SNMPv2u, consists of two documents: RFC 1909, "An Administrative Infrastructure for SNMPv2" and RFC 1910, "The User-based Security Model for SNMPv2." Both RFCs were issued 28 February 1996 and are classified by the IETF as experimental RFCs. The other proposal is known as SNMPv2*, which its proponents claim is heavily based on USEC. Neither USEC nor SNMPv2* has been approved for a standards track by IETF.

3.9.7.2.4 Portability caveats. The structure of certain traditional UNIX directories, such as the familiar "/tmp," "/usr/spool," and "/usr/spool/mail" directories will have to change to accommodate the P1003.1e and P1003.2c security standards. This is because these are directories to which all users have access and to which many programs write. A change in the way programs write to directories has the potential for causing software portability and systems administrator portability problems.

The traditional UNIX permission bits that have been carried into POSIX are inadequate for defining exactly which user can perform specific actions on specific files. Eliminating the permission bits in favor of Access Control Lists could make the secure POSIX systems incompatible with non-POSIX compliant systems and many applications.

OSF DCE version 1.1's authentication service is based on Kerberos Version 5 (RFC 1510), but is not tatally compatible with RFC 1510. DCE 1.2.2 adds testing and official support for Kerberos Version 5.

3.9.7.2.5 Related standards. ISO/IEC 9945-1 as profiled by FIPS PUB 151-2 is related to IEEE P1003.1e and IEEE P1003.2c.

3.9.7.2.6 Recommendations. The mandated standards are recommended.

All IEEE P1003.1e and IEEE P1003.2c security systems should incorporate Access Control Lists as an optional feature in addition to permission bits (not "in place of" permission bits). The incompatibilities between the two access control methods (permission bits and access control

lists) are not resolvable. The best method for resolving the overall problems seem to be incorporation Access Control Lists as an optional feature on top of permission bits. The permission bits would represent the lowest common denominator of security, showing the maximum amount of openness possible in a system. Organizations needing only the lowest level of security could continue to use the familiar permission bits and associated "chmod" command. Use of access control lists will require a change in security policy such that access is granted if and only if permission is granted and access control permits it.

3.9.7.3 Security risk management. (This BSA appears in part 2, part 7, part 9, and part 10.) Security risk management supports accreditation through a risk analysis of an information system and its operational environment, and the steps taken to manage the risk requirements.

3.9.7.3.1 Standards. Table 3.9-39 presents standards for security risk management.

TABLE 3.9-39 Security risk management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	NIST	Guideline for the Analysis of Local Area Network Security	FIPS PUB 191:1994	Informational (Approved)
GPC	NIST	Guideline for Automated Data Processing Risk Analysis	FIPS PUB 65:1979	Informational (Approved)
GPC	NIST	Guidelines for Automatic Data Processing Physical Security and Rick Management	FIPS PUB 31:1974	Informational (Approved)

3.9.7.3.2 Alternate specifications. There are no alternative specifications.

3.9.7.3.3 Standards deficiencies. Because of its age, FIPS PUB 31 does not include information of all modern security concepts.

3.9.7.3.4 Portability caveats. Portability problems with the existing standards are unknown.

3.9.7.3.5 Related standards. The following standards are related to the TCSEC standard:

a. CSC-STD-003-85 25 June 1985, Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer Security Evaluation Criteria in Specific Environments

b. CSC-STD-004-85, 25 June 1985, Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer Security Evaluation Criteria in Specific Environments

3.9.7.3.6 Recommendations. The mandated standard is recommended. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," provides guidance on effective security risk management of federal information systems. NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook" provides additional guidance on risk management. DOD Directive 5200.28 requires a risk analysis of an information system be conducted in its operational environment to support accreditation of the information system. System implementors should perform the risk analysis in accordance with CSC-STD-003-85 and CSC-STD-004-85 to determine the appropriate DOD-5200.28-STD class.

3.9.7.4 Security audit. (This BSA appears in part 7, part 9, part 10, and part 11.) Security auditing is a review or examination of records and activities to test controls, ensure compliance with policies and procedures, detect breaches in security, and indicate changes in operation (paraphrased from ISO 7498-2).

3.9.7.4.1 Standards. Table 3.9-40 presents standards for security audit.

TABLE 3.9-40 Security audit standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 8: Security Audit Trail Function (same as ITU-T X.740)	10164-8:1993	Informational (Approved)
CPC	X/Open	Security Interface Specification: Auditing and Authentication	S020: 1990	Informational (Approved)
IPC	OCSB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems, Part 7: Security Audit Framework	10181-7	Informational (Draft)
IPC	ISO/IEC	OSI Distributed Transaction Processing (DTP) - Draft Amendments to Parts 1-3: Transaction Processing Security	WDAMs (SC21 N6232) to ISO 10026-1,2,3: 1994	Informational (Draft)

3.9.7.4.2 Alternate specifications. There are no alternative specifications.

3.9.7.4.3 Standards deficiencies. ISO Transaction Processing Security work (WDAMs to ISO 10026-1,2,3) is in the early stages. Its content is not defined, and it cannot be used for procurement. ISO 10164-8 does not define a security audit, or explain how to perform one. It does not define implementation aspects, occasions where the use of the security audit trail function is appropriate, or the services necessary for the establishment and normal or abnormal release of a management association.

There is a need for a standard for programming interfaces to support development of portable tools for audit trail analysis and configuration.

3.9.7.4.4 Portability caveats. Proposed amendments to ISO 10026 have ceased. This is a high portability risk area.

3.9.7.4.5 Related standards. The following guidelines support the TCSEC standard:

a. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation

b. NCSC-TG-011, Version 1, 1 August 1990, Trusted Network Interpretation Environments Guideline - Guidance for Applying the Trusted Network Interpretation

c. NCSC-TG-001, Version 2, June 1988, A Guide to Understanding Audit in Trusted Systems

3.9.7.4.6 Recommendations. The mandated standard is recommended.

3.9.7.5 Security alarm reporting. (This BSA appears in part 7, part 9, part 10, and part 11.) Security alarm reporting is the capability to receive notifications of security-related events, alerts of any misoperations in security services and mechanisms, alerts of attacks on system security, and information as to the perceived severity of any misoperation, attack, or breach of security.

3.9.7.5.1 Standards. Table 3.9-41 presents standards for security alarm reporting.

TABLE 3.9-41 Security alarm reporting standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 7: Security Alarm Reporting Function (same as ITU-T X.736)	10164-7:1992	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179:1992	Informational (Superseded)

3.9.7.5.2 Alternate specifications. There are no alternative specifications.

3.9.7.5.3 Standards deficiencies. FIPS PUB 179-1 supersedes FIPS PUB 179. ISO 10164-7 does not define implementation aspects, specify the manner in which management is accomplished by the user of the Security Alarm Reporting Function (SARF), define interactions that result in the use of the SARF, or specify the services necessary for the establishment and normal and abnormal release of a management association.

3.9.7.5.4 Portability caveats. Portability problems with the existing standards are unknown.

3.9.7.5.5 Related standards. There are no related standards.

3.9.7.5.6 Recommendations. There are no recommended standards for security alarm reporting.

3.9.7.6 Personal authentication. (This BSA appears in part 2, part 3, part 9, and part 10.) Personal authentication supports the accountability objective of being able to trace all security relevant events to individual users. In addition to supporting unique identification, standards are provided to authenticate the claimed identity.

3.9.7.6.1 Standards. Table 3.9-42 presents standards for personal authentication.

TABLE 3.9-42 Personal authentication standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
GPC	NIST	Password Usage	FIPS PUB 112: 1985	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
GPC	NIST	Guidelines on Evaluation of Techniques for Automated Personal Identification	FIPS PUB 48:1977	Informational (Approved)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - The Directory: Authentication Framework edition 2 (Same as ITU-T X.509:1993)	9594-8.2:1993	Informational (Approved)
GPC	NIST	Guideline for Use of Advanced Authentication Technology Alternatives	FIPS PUB 190:1994	Informational (Approved)
CPC	IETF	A One-Time Password System	RFC 1938: 1996	Emerging (Draft)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
CPC	IETF	The Kerberos Network Authentication Service (V5)	RFC 1510:1993	Informational (Draft)

3.9.7.6.2 Alternate specifications. There are no alternative specifications.

3.9.7.6.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.9.7.6.4 Portability caveats. OSF DCE Version 1.1's authentication service is based on Kerberos Version 5 (RFC 1510), but is not totally compatible with RFC 1510. DCE 1.2.2 adds testing and official support for Kerberos Version 5.

3.9.7.6.5 Related standards. The following standards are related to personal authentication standards (particularly TCSEC):

a. DOD 5200.28-STD, DOD Trusted Computer Systems Evaluation Criteria

b. NCSC-TG-017, Version 1, "A Guide to Understanding Identification and Authentication in Trusted Systems

c. CSC-STD-002-85, "Password Management Guideline"

d. NCSC-WA-002-85, "Personal Computer Security Considerations"

e. ITU-T X.509 (1993) (same as ISO 9594-8), The Directory: Authentication Framework

3.9.7.6.6 Recommendations. The mandated standards are recommended.

3.9.7.7 Entity authentication. (This BSA appears in part 8, part 9, part 10, and part 11.) Entity authentication standards address data, processes, systems, and enterprises.

3.9.7.7.1 Standards. Table 3.9-43 presents standards for entity authentication.

TABLE 3.9-43 Entity authentication standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
GPC	NIST	Computer Data Authentication	FIPS PUB 113:1985	Informational (Approved)
GPC	NIST	Entity Authentication Using Public Key Cryptography	FIPS PUB 196:1996	Emerging (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO	Financial Transactions - Retail Banking Security Requirements for Message Authentication	9807	Informational (Approved)
IPC	ISO	Entity Authentication Mechanisms - Part 1: General Model	9798-1:1991	Informational (Approved)
IPC	ISO	Entity Authentication Mechanisms - Part 3: Entity Authentication Using a Public Key Algorithm	9798-3:1993	Informational (Approved)
GPC	NIST	Guideline for Use of Advanced Authentication Technology Alternatives	FIPS PUB 190:1994	Informational (Approved)
IPC	ISO	Entity Authentication - Part 2: Mechanisms Using Symmetric Encipherment Algorithms	9798-2:1994	Informational (Approved)
IPC	ISO	Entity Authentication - Part 4: Mechanisms Using a Cryptographic Check Function	9798-4:1995	Informational (Approved)
CPC	X/Open	Security Interface Specification: Auditing and Authentication	S020: 1990	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
CPC	IETF	The Kerberos Network Authentication Service (V5)	RFC 1510:1993	Informational (Draft)
IPC	ISO	Entity Authentication Mechanisms, Part 5: Entity Authentication Using Zero Knowledge Techniques	9798-5:1995	Informational (Draft)

3.9.7.7.2 Alternate specifications. There are no alternative specifications.

3.9.7.7.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.9.7.7.4 Portability caveats. OSF DCE Version 1.1's authentication service is based on Kerberos Version 5 (RFC 1510), but is not totally compatible with RFC 1510. DCE 1.2.2 adds testing and official support for Kerberos Version 5.

3.9.7.7.5 Related standards. The following standards are related to entity authentication:

a. DOD NCSC-TG-017, Version 1, September 1991, Guide to Understanding Identification and Authentication in Trusted Systems.

b. FIPS PUB 196, 11 October 1996.

FIPS PUB 196 becomes effective 6 April 1996. It is based on ISO/IEC 9798-3:1993 and specifies two challenge-response protocols by which entities in a computer system may authenticate their identities to one another. FIPS PUB 196 is for use in public key based challenge-response and authentication systems at the application layer within computer and digital telecommunications systems.

3.9.7.7.6 Recommendations. The mandated standards are recommended.

3.9.7.8 System access control. (This BSA appears in part 4, part 9, part 10, and part 11.) System access control standards provide high-level guidance on access control frameworks and implementation.

3.9.7.8.1 Standards. Table 3.9-44 presents standards for system access control.

TABLE 3.9-44 System access control standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 9: Objects and Attributes for Access Control	10164-9:1995	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 3: Access Control	10181-3	Informational (Draft)

3.9.7.8.2 Alternate specifications. There are no alternative specifications.

3.9.7.8.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.9.7.8.4 Portability caveats. Portability problems with the existing standards are unknown.

3.9.7.8.5 Related standards. The following guidelines support the TCSEC standard:

a. NCSC-TG-003, Version 1, September 1987, A Guide to Understanding Discretionary Access Control in Trusted Systems

b. NCSC-TG-028, Version 1, May 1992, Assessing Controlled Access Protection

c. NCSC-TG-020-A, August 1989, Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX System

3.9.7.8.6 Recommendations. The mandated standards are recommended.

3.9.7.9 Network access control. (This BSA appears in part 7, part 9, and part 10.) Access control is the prevention of unauthorized use of a resource, including its use in an unauthorized manner.

3.9.7.9.1 Standards. Table 3.9-45 presents standards for network access control.

TABLE 3.9-45 Network access control standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Information Technology - Defense Standardized Profiles AMHXn(D)- Message Handling Systems - Message Security Protocol (MSP) Parts 1-5	MIL-STD-2045-18500: 1993	Mandated (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 3 (SP3)	SDN.301, Revision 1.5: 1989	Mandated (Approved)
NPC	IEEE	Standard for Interoperable LAN Security - Part B: Secure Data Exchange (SDE)	802.10b:1992	Legacy (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO	Transport Layer Security Protocol (TLSP) (Includes Amendment 1)	10736:1994	Informational (Approved)
IPC	ISO	Network Layer Security Protocol (NLSP)	11577:1994	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
GPC	NIST	Guidelines for Security of Computer Applications	FIPS PUB 83:1980	Informational (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 4 (SP4)	SDN.401, Rev. 1.3:1989	Informational (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, v. 4.0, Rev. A: 1997	Emerging (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, Rev. 3.0: 1994	Legacy (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179:1992	Informational (Superseded)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - The Directory - Parts 1-4 DAM1: Access Control	9594-1,2,3,4:1990/ DAM1	Informational (Draft)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - The Directory - Part 8: Authentication Framework, DAM1: Access Control	9594-8:1990/ DAM1	Informational (Draft)
IPC	ISO	OSI File Transfer, Access and Management (FTAM) - Parts 1-4: Amendment 4: Enhancement to FTAM Security Services	8571: 1,2,3,4:1988/ WDAM4:1993	Informational (Draft)

3.9.7.9.2 Alternate specifications. There are no alternative specifications.

3.9.7.9.3 Standards deficiencies. Deficiencies in the existing standards are unknown. FIPS PUB 179-1 supersedes FIPS PUB 179.

3.9.7.9.4 Portability caveats. Proposed security enhancements to FTAM (WDAM4 to ISO 8571) has ceased. This is a high portability risk area because no standards exist.

3.9.7.9.5 Related standards. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation, and NCSC-TG-011, Version 1, August 1990, Trusted Networks Interpretation Environments Guideline - Guideline for Applying the Trusted Network Interpretation, supports the DOD 5200.28-STD.

3.9.7.9.6 Recommendations. The mandated standards are recommended.

MIL-STD-2045-18500 describes the security provided by MSP. It should be used for DOD message systems that are required to exchange classified and sensitive but unclassified information. It is based on Version 3.0 of the MSP documented in SDN.701, "Secure Data Network System (SDNS) Message Security Protocol," Revision 1.5, 1 August 1989. MSP is under revision to Version 4.0 to accommodate, in part, Allied requirements. This DOD Standardized Profile (DSP) standard will be replaced by a portion of the U.S. Supplement to ACP 123 or ACP 120, Common Security Protocol, when the revision to MSP is complete.

SDN.701, Rev.3.0, is used with DMS, Phase 1. It is for use with legacy systems only.

SP3 provides connectionless security services and is the basis for ISO 11577. SP3 is designed to be used at the top of layer 3.

The work on File Transfer, Access, and Management (FTAM) security (WDAM4 to ISO 8571) security enhancements has been suspended. Procurements requiring access control for FTAM and transaction processing should not use these standards.

IEEE 802.10b is for use with legacy LANs only.

3.9.7.10 Certification and accreditation. (This BSA appears in part 2, part 9, and part 10.) Certification and accreditation constitute a set of procedures and judgments leading to a determination of the suitability of the system to operate in the targeted operational environment.

Accreditation is the official management authorization to operate a system. The accreditation normally grants approval for the system to operate (a) in a particular security mode, (b) with a prescribed set of countermeasures (administrative, physical, personnel, communications security, emissions, and computer security controls), (c) against a defined threat and with stated vulnerabilities and countermeasures, (d) within a given operational concept and environment, (e) with stated interconnections to other systems, (f) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility, and (g) for a specified period of time. The Designated Approving Authority(s) (DAA) formally accepts security responsibility for the operation of the system and officially declares that the specified system will adequately protect against compromise, destruction, or unauthorized modification under stated parameters of the accreditation. The accreditation decision affixes security responsibility with the DAA and shows that due care has been taken for security in accordance with the applicable policies.

An accreditation decision is in effect after the issuance of a formal, dated statement of accreditation signed by the DAA, and remains in effect for the specified period of time (varies according to applicable policies). A system processing classified or sensitive unclassified information should be accredited prior to operation or testing with live data unless a written waiver is granted by the DAA. In some cases (e.g., when dealing with new technology, during a transition phase, or when additional time is needed for more rigorous testing), the DAA may grant an interim approval to operate for a specified period of time. At the end of the specified time period, the DAA must make the final accreditation decision.

Certification is conducted in support of the accreditation process. It is the comprehensive analysis of both the technical and nontechnical security features and other safeguards of a system to establish the extent to which a particular system meets the security requirements for its mission and operational environment. A complete system certification must consider factors dealing with the system in its unique environment, such as its proposed security mode of operation, specific users, applications, data sensitivity, system configuration, site/facility location, and interconnections with other systems. Certification should be done by personnel who are technically competent to assess the systems ability to meet the security requirements according to an acceptable methodology. The resulting documentation of the certification activities is provided to the DAA to support the accreditation decision. Many security activities support certification, such as risk analysis, security test and evaluation, and various types of evaluations.

Ideally, certification and accreditation procedures encompass the entire life cycle of the system. Ideally, the DAA is involved from the inception of the system to ensure that the accreditation goals are clearly defined. A successful certification effort implies that system security attributes were measured and tested against the threats of the intended operational scenarios. Additionally, certification and accreditation are seen as continuing and dynamic processes; the security state of the system needs to be tracked and assessed through changes to the system and its operational

environment. Likewise, the management decision to accept the changing system for continued operation is an ongoing decision process.

Standards for certification and accreditation services provide definitions and procedures for the testing and accreditation of computer systems in so far as their conformance with security standards is concerned.

3.9.7.10.1 Standards. Table 3.9-46 presents standards for certification and accreditation.

TABLE 3.9-46 Certification and accreditation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	NIST	Guideline for Computer Security Certification and Accreditation	FIPS PUB 102:1983	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.9.7.10.2 Alternate specifications. No other consortia or de facto specifications are available.

3.9.7.10.3 Standards deficiencies. Because of its age, FIPS PUB 102 does not include services for the certification and accreditation of all modern security concepts.

Certification and accreditation evaluation criteria that address cuttent information technology, such as distributed computing and networking, are needed. As new criteria such as the Common Criteria emerge, revision of existing certification and accreditation guidelines may be required.

3.9.7.10.4 Portability caveats. There are no portability problems related to the existing specifications.

3.9.7.10.5 Related standards. NCSC-TG-029, "Introduction to Certification and Accreditation," January 1994, discusses basic concepts related to certification and accreditation and is the first of a series of guidelines in the "Rainbow Series" supporting the Trusted Computer System Evaluation Criteria (TCSEC) standard.

3.9.7.10.6 Recommendations. The mandated standard is recommended.

Procurements that require that an AIS be certified and/or accredited must reference DOD Directive 5200.28 and applicable designated approving authority guidance. DOD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," requires certification and accreditation of AIS. FIPS PUB 102, Guidelines for Computer Security and

Accreditation provides Federal guidelines for certification and accreditation. Because of its age, this FIPS PUB does not include services for the certification and accreditation of all modern security concepts. DOD 5200.28-STD provides criteria to assess security assurances of trusted systems to specific classes. DCID 1/16 provides security requirements fo systems processing intelligence information.

The DISA CISS and NSA are each developing documents that will standardize the certification and accreditation process within DOD. Each document is in draft form; final documents are expected to be issued in 1997. The NSA document, "Certificati n and Accreditation Process Handbook for Certifiers," wil' be published as a "Rainbow" series document supporting the TCSEC standard. This NSA handbook focuses on certification and accreditation of standalone systems. The DISA CISS document, "DOD Information Technology Certification and Accreditation Process" (DITSCAP), will be published as a DOD publication. The DITSCAP focuses on certification and accreditation in conjunction with the programmatic aspects of the DII.

3.9.7.11 Detection and notification. (This BSA appears in part 2, part 9, and part 10.) Detection and notification objectives ensure that a secure system has the capability to recognize that it is: under attack; may potentially enter a non-available state; has been compromised; or has failed in a potentially compromising manner. Guidance in this area focuses on reporting detected security critical conditions to proper authorities, and implementing predetermined corrective actions.

3.9.7.11.1 Standards. Table 3.9-47 presents standards for detection and notification.

TABLE 3.9-47 Detection and notification standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

3.9.7.11.2 Alternate specifications. There are no alternative specifications.

3.9.7.11.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.9.7.11.4 Portability caveats. Portability problems in the existing standards are unknown.

3.9.7.11.5 Related standards. NSA's C-Technical Report-001, Computer Viruses: Prevention, Detection, and Treatment, and NIST SP 800-5, A Guide to the Selection of Anti-Virus Tools and Techniques, provide guidance on computer viruses. The following specifications support the TCSEC standard:

a. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation

b. NCSC-TG-015, Version 1, October 1989, A Guide to Understanding Trusted Facility Management

c. NCSC-TG-016, Version 1, October 1992, Guidelines for Writing Trusted Facility Manuals

3.9.7.11.6 Recommendations. The mandated standard is recommended.

3.9.7.12 Security recovery. (This BSA appears in part 2, part 9, and part 10.) Recovery guidance defines provisions to allow system personnel or processes with the proper authorizations to repair or eliminate the cause of security relevant failures, isolate compromised portions of the system, and revalidate proper operations prior to returning the system to a fully operational secure state.

3.9.7.12.1 Standards. Table 3.9-48 presents standards for security recovery.

TABLE 3.9-48 Security recovery standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	CSSB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0, 1996	Emerging (Draft)

3.9.7.12.2 Alternate specifications. There are no alternative specifications.

3.9.7.12.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.9.7.12.4 Portability caveats. Portability problems with the existing standards are unknown.

3.9.7.12.5 Related standards. The following specifications are related to the TCSEC standard:

a. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation

b. NCSC-TG-022, Version 1, December 1991, A Guide to Understanding Trusted Recovery in Trusted Systems

c. NCSC-TG-015, Version 1, October 1989, A Guide to Understanding Trusted Facility Management

d. NCSC-TG-016, Version 1, October 1992, Guidelines for Writing Trusted Facility Manuals

3.9.7.12.6 Recommendations. The mandated standard is recommended.

3.9.7.13 Database security. (This BSA appears in part 4, part 9, and part 10.) Database security standards provide protection for stored data from unauthorized access, modification, and denial of service.

3.9.7.13.1 Standards. Table 3.9-49 presents standards for database security.

TABLE 3.9-49 Database security standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Database Language SQL (Adopts ANSI X3.135-1992 (same as ISO 9075:1992))	FIPS PUB 127-2:1993	Informational (Approved)
GPC	NIST	Information Resource Dictionary System (IRDS) (adopts ANSI X3.138-1988 and X3.138A-1991)	FIPS PUB 156:1989	Informational (Approved)
NPC	ANSI	Database Language SQL	X3.135-1992	Informational (Approved)
IPC	ISO	Database Language SQL (same as ANSI X3.135-1992)	9075:1992	Informational (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Framework	10027:1990	Informational (Approved)
IPC	ISO/IEC	OSI Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element	9804:1990	Informational (Approved)
IPC	ISO/IEC	OSI Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Service Element	9805:1990	Informational (Approved)
NPC	ANSI	Information Resource Dictionary System (IRDS)	X3.138-1988	Informational (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Services Interface Amendment 1: C Language Binding	10728 AMD 1:1994	Informational (Draft)

3.9.7.13.2 Alternate specifications. There are no alternative specifications.

3.9.7.13.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.9.7.13.4 Portability caveats. Portability problems with the existing standards are unknown.

3.9.7.13.5 Related standards. DOD 5200.28-STD, 26 December 1995, DOD Trusted Computer Systems Evaluation Criteria, is related to NCSC-TG-021. The following specifications are related to DOD 5200.28-STD:

a. NCSC-TG-018, Version 1, July 1992, A Guide to Understanding Object Reuse in Trusted Systems

b. NCSC-TG-025, Version 2, September 1991, A Guide to Understanding Data Remnants in Automated Information Systems

3.9.7.13.6 Recommendations. The mandated standard is recommended.

3.9.7.14 Security association and key management. (This BSA appears in part 7, part 9, and part 10.) A security association is the totality of communication and security mechanisms and functions (e.g., communications protocols, security protocols, doctrinal mechanisms, security-critical mechanisms and functions) that securely binds together two security contexts in different end systems or relay systems supporting the same information domain. A security association is an application association that includes additional support from security functions and mechanisms. Key management provides procedures for handling cryptographic keying material to be used in symmetric or asymmetric cryptographic mechanisms. It includes key generation, key distribution, key storage, key archiving, and key deletion.

3.9.7.14.1 Standards. Table 3.9-50 presents standards for security association and key management.

TABLE 3.9-50 Security association and key management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NSA	Key Exchange Algorithm	R21-TECH-23-94: 1994	Mandated (Approved)
GPC	NSA	Secure Data Network System (SDNS) Key Management Protocol (KMP)	SDN.903, Version 3.2: 1989	Mandated (Approved)
GPC	NIST	Key Management Using ANSI X9.17	FIPS PUB 171:1992	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 2:Security Exchange Service Element Definition	11586-2:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 3: Security Exchange Service Element Protocol Specification	11586-3:1994	Informational (Approved)
IPC	ISO	Banking Key Management (wholesale)	8732:1988	Informational (Approved)
NPC	ANSI	Financial Institution Key Management (wholesale)	X9.17-1991	Informational (Approved)
NPC	IEEE	Standard for Interoperable LAN Security - Part C: Key Management Protocol (KMP)	802.10c	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems Part 6: Key Management	10181-6	Informational (Draft)
CPC	IETF	Internet Security Association and Key Management Protocol (ISAKMP)	draft-ietf-ipsec-isakmp-07.txt, pp. 21 February 1997	Informational (Draft)
CPC	IETF	The Photuris Session Key Management Protocol	draft-simpson-photuris-11.txt, 13 June 1996	Informational (Draft)
CPC	IETF	Simple Key Management for Internet Protocols (SKIP)	draft-ietf-ipsec-skip-07.txt, August 1996	Informational (Draft)
CPC	IETF	The Oakley Key Determination Protocol	draft-ietf-ipsec-oakley-01.txt, 5/10/96	Informational (Draft)
NPC	IEEE	Standard for Public-Key Cryptography	P1363	Informational (Formative)

3.9.7.14.2 Alternate specifications. There are no alternative specifications.

3.9.7.14.3 Standards deficiencies. There is a lack of guidance for establishing a Public Key Infrastructure (PKI) to automatically manage public keys through the use of public key certificates. In April 1994, NIST, in conjunction with seven other federal agencies, completed a study on automated management of public keys and associated public key certificates on a nationwide basis. Based on the recommendations of the study, NIST is establishing a PKI pilot project to provide public key certificate services for several participating government agencies.

3.9.7.14.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.9.7.14.5 Related standards. There are no related standards.

3.9.7.14.6 Recommendations. The mandated standards are recommended. In FORTEZZA applications, the NSA-developed Key Exchange Algorithm, R21-TECH-23-94, must be used.

IEEE P1363, Standard for Public-Key Cryptography, is under development, with the first version expected to be ready for balloting in 1997.

The IETF's IP Security Protocol (IPSEC) Working Group (WG) is developing an Internet Key Management Protocol (IKMP) that will be specified as an application layer protocol independent of the lower layer security protocol. The IKMP will be based on ISAKMP/Oakley work begun in the Internet Draft documents for ISAKMP and the Oakley Key Determination Protocol.

3.9.7.15 Registration of cryptographic techniques. (This BSA appears in part 9 and part 10.) These standards provide procedures for the registration of cryptographic algorithms in a standard format with a registration authority. The need for these registration services is determined by the security architecture of the system in question. These are not implementable specifications and no conformance test is required.

3.9.7.15.1 Standards. Table 3.9-51 presents standards for registration of cryptographic techniques.

TABLE 3.9-51 Registration of cryptographic techniques standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Procedures for the Registration of Cryptographic Algorithms	9979:1991	Informational (Approved)

3.9.7.15.2 Alternate specifications. No other consortia or de facto specifications are available.

3.9.7.15.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.9.7.15.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.9.7.15.5 Related standards. No standards are related to registration of cryptographic techniques.

3.9.7.15.6 Recommendations. Procurements requiring that all cryptographic algorithms offered are registered with a registration authority in a standard format should specify conformance with ISO 9979. The NIST document, NISTIR 5308, "General Procedures for Registering Computer Security Objects," December 1993, describes the object-independent procedures for operating the Computer Security Objects Register (CSOR) established by NIST. Initially, the only family of objects registered in the CSOR is network security labels; however, plans include adding cryptographic algorithm modes of operation to the CSOR.

3.9.8 Other management services.

3.9.8.1 Database administration. (This BSA appears in part 4 and part 9.) Data administration is the process of the analysis, classification, and maintenance of an organization's data and data relationships. It includes the development of data models, data warehousing, and data dictionaries, which combined with transaction processing, are the raw materials for database design.

3.9.8.1.1 Standards. Table 3.9-52 presents standards for database administration.

TABLE 3.9-52 Database administration standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Data Element Standardization Procedures, January 1993	Manual 8320.1-M-1	Mandated (Approved)
GPC	NIST	Guide to Data Entity Naming Conventions	NBS SP 500-149 of Oct. 1987	Informational (Approved)
GPC	DOD	Defense Data Repository System	End User Manual ver. 2.0 of 10 August 1993	Informational (Approved)
IPC	ISO/IEC	Specification and Standardization of Data Elements, Part 3: Basic Attributes of Data Elements	11179-3:1994	Informational (Approved)
IPC	ISO/IEC	Specification and Standardization of Data Elements, Part 4: Rules and Guidelines for the Formulation of Data Definitions	11179-4:1995	Informational (Approved)
IPC	ISO/IEC	Specification and Standardization of Data Elements, Part 5: Naming and Identification Principles for Data Elements	11179-5:1995	Informational (Approved)
IPC	ISO/IEC	Specification and Standardization of Data Elements, Part 6: Registration of Data Elements	11179-6	Informational (Draft)
GPC	DOD	DOD Data Administration	DODD 8320.1 of 9/26/1991	Informational (Superseded)

3.9.8.1.2 Alternative specifications. The only other available specifications are proprietary database utilities.

3.9.8.1.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard.

3.9.8.1.4 Portability caveats. This is a high portability risk area because no standards exist.

3.9.8.1.5 Related standards. The following standards are related to database administration or database administration standards:

a. ISO 7498-4:1989: Management Framework
b. ISO 9075: SQL
c. ISO 9579-1: RDA (Generic Model, Service and Protocols)
d. ISO 9579-2: RDA (SQL Specialization)
e. ISO 9595:1991: CMIS.

f. ISO 9596-1:1991: CMIP.
g. ISO/IEC 9945-1: (IEEE P1003.1)
h. ISO 10164-1:1993: Object Management Function
i. ISO 10165-1:1991: SMI - Part 1 Management Information Model
j. ISO 10165-2:1991: SSMI - Part 2 DMI
k. ISO 10165-4:1992: Guidelines for the Definition of Managed Objects (GDMO)
l. ANSI X3.135-1992: SQL
m. ANSI X3.168-1989: Embedded SQL
n. NIST FIPS 127-2: Database Language SQL
o. NIST FIPS 146-1: Government Open Systems Interconnection Profile (GOSIP)
p. NIST FIPS 156: IIRDS
q. NIST FIPS 193: SQL Environments

3.9.8.1.6 Recommendations. DODD 8320.1 is recommended for data administration. Database administration systems should be compatible with and integrated with the SQL database language set forth in FIPS PUB 127-2. Furthermore, all database administration systems offered as a result of this procurement's requirements shall be integrated with ISO 9579-1 RDA (Generic Model, Service and Protocol), ISO 9579-2 Remote Database Access (SQL Specialization) of December 1993, and NIST FIPS PUB 193, SQL Environments.

3.9.8.2 Object-oriented database management. (This BSA appears in both Part 4 and Part 9.) Standards for object-oriented database management provide facilities and interfaces to manage object databases (databases that store, manipulate, and retrieve data represented as objects).

3.9.8.2.1 Standards. Table 3.9-53 presents standards for object-oriented database management.

TABLE 3.9-53 Object-oriented database management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	ODMG	Object Database Management Group (ODMG) - 93	ODMG-93, Release 1.1	Informational (Approved)
CPC	ODMG	Object Database Management Group (ODMG) 9x	ODMG-9x	Emerging (Formative)
NPC	ANSI	X3 Database System Study Group (DBSSG)	X3 Study	Informational (Formative)
CPC	ORD	Preliminary work on object-oriented database management	TBD-Preliminary work on object-oriented database management	Informational (Formative)

3.9.8.2.2 Alternative specifications. Microsoft's Object Database Connectivity (OBDC) API specification for MS-Windows applications is also available.

3.9.8.2.3 Standards deficiencies. Deficiencies in the standards are unknown, since these services are not part of any formal standard, but the Microsoft specification has insufficient drivers available.

3.9.8.2.4 Portability caveats. This is a high portability risk area because no standards exist, and many Microsoft PC products do not comply with most Unix- and Portable Operating System Interfaces for Computers (POSIX)-based systems.

3.9.8.2.5 Related standards. No standards are related to object-oriented database management standards.

3.9.8.2.6 Recommendations. There is no recommendation at this time.

3.9.8.3 Floppy disk format and handling. (This BSA appears both in part 8 and part 9.) Floppy disk format and handling standards provide formats and interfaces for the exchange, backup, and restoration of data to or from floppy disks.

3.9.8.3.1 Standards. Table 3.9-54 presents standards for floppy disk format and handling.

TABLE 3.9-54 Floppy disk format and handling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
CPC	X/Open	Single UNIX Specification (Spec. 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C436 (9/94)	Emerging (Approved)
GPC	NIST	Portable Operating System Interface (POSIX) - System Application Program Interface/ C Language (adopts ISO/IEC 9945-1:1990)	FIPS PUB 151-2:1993	Informational (Approved)
IPC	IEEE	POSIX - Part 1: System API Supplement - Removable Media Support	P1003.1k	Emerging (Formative)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)[C language] (as profiled by FIPS PUB 151-2:1993)	9945-1:1990	Informational (Superseded)
CPC	X/Open	System V Interface Definition (SVID) (replaced by Single UNIX Specification (Spec. 1170))	SVID Issue 4	Informational (Superseded)

3.9.8.3.2 Alternative specifications. The following alternative specifications are also available:

a. Sun Microsystems' SunOS/Solaris command "bar"
b. OSF: OSF/1 "tar" and "cpio" utilities.

3.9.8.3.3 Standards deficiencies. POSIX and Unix have very poor floppy disk handling capabilities. Most standards related to floppy disks concern logical interfaces that permit the interconnection of floppy disk peripherals.

3.9.8.3.4 Portability caveats. The "bar" is not a standard. However, it is widely used because of Sun's large installed base. It is presented as an example of a capability needing to be standardized, as well as an example of the kind of capability that could be specified.

3.9.8.3.5 Related standards. No standards are related to floppy disk format standards.

3.9.8.3.6 Recommendations. ISO/IEC 9945-2 disk format services "pax" are expected to replace "tar" and "cpio" utilities in POSIX.1. X/Open SUS includes the POSIX.2 utilities.

3.9.8.4 POSIX tape labeling and tape volume processing. (This BSA appears bou. in part 8 and part 9.) Tape labels are a fixed portion of data stored on tape media and containing certain types of administrative information automatically readable by tape-handling software. Among the information typically stored on tape labels are the identification of the media content, ownership of the media content, access control information for the media content, and the format of the rest of the information on the media.

3.9.8.4.1 Standards. Table 3.9-55 presents standards for POSIX tape labeling and tape volume processing.

TABLE 3.9-55 POSIX tape labeling and tape volume processing standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ECMA	File Structure and Labeling of Magnetic Tapes for Information Interchange	13 (1985)	Informational (Approved)
IPC	ECMA	Magnetic Tape Cassette Labeling and File Structure for Information Interchange	41 (1973)	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment 1: System API [Generic (C language)]	P1003.1a	Emerging (Draft)
NPC	IEEE	POSIX - Part 1: System API Supplement - Removable Media Support	P1003.1f	Emerging (Formative)

3.9.8.4.2 Alternative specifications. The only other available specifications are proprietary.

3.9.8.4.3 Standards deficiencies. The P1003.1a draft standard does not address the issue of processing several files as if they were a single entity.

Traditional Unix systems do not provide mechanisms for protected access to devices or media, nor do they generally provide mechanisms for label processing or transparent volume switching.

3.9.8.4.4 Portability caveats. To provide tape handling portability, a standard must specify the handling of ANSI/ISO labeled tape and IBM labeled tape. IBM labeled tapes, although not a strict standard, represent vast numbers of labeled tapes already in existence. IBM labeled tapes are roughly analogous to the ANSI standard, except the labels are written with the EBCDIC character set rather than with ASCII.

It is not certain, even within the proposed standard, how to process information when some of it is on 9-track tape and some on 8mm (Exabyte) tape, or some on labeled and some on unlabeled tape. This may be a limitation of the standard.

3.9.8.4.5 Related standards. The following standards are related to POSIX tape labeling and tape volume processing standards:

a. ISO/IEC 9945-1:1996: POSIX Part 1: System Application Programming Interface.
b. ISO/IEC 9945-2:1992: POSIX Part 2: Shell and Utility.

c. IEEE 1003.5:1992: Ada Language Binding to POSIX.
d. IEEE P1003.1e: Security Interface Standards for POSIX.
e. IEEE P1387.1: POSIX System Administration - Part 1: Overview.
f. IEEE 1003.9:1992: Standard Fortran Language Bindings to POSIX.

3.9.8.4.6 Recommendations. There are no recommendations.

3.9.8.5 Print management. (This BSA appears both in part 8 and part 9.) The print services are used by management and user applications to send a file to the printer, cancel the print job, and get printer status information. The printing systems program interface is used as the base for the POSIX printing management standard. Printing management standards also provide services and interfaces for transparent remote printing, output spooling, spool queue management, and scheduling.

3.9.8.5.1 Standards. Table 3.9-56 presents standards for print management.

TABLE 3.9-56 Print management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (as profiled by FIPS PUB 189:1994)	9945-2:1993	Mandated (Approved)
CPC	X/Open	Common Desktop Environment (CDE); XCDE Services and Applications	C323 (4/95)	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
CPC	X/Open	Single UNIX Specification (Spec. 1170) Commands and Utilities, Issue 4, Version 2 (part of XPG4)	C436 (9/94)	Emerging (Approved)
IPC	ECMA	Method for Measuring Printer Throughput	132 (1991)	Informational (Approved)
IPC	ISO/IEC	Information Technology - Text and office systems - Document Printing Application (DPA). Part 1: Abstract service definition and procedures	10175-1:1996	Informational (Approved)
IPC	ISO/IEC	Information Technology - Text and office systems - Document Printing Application (DPA) - Part 2: Protocol specification	10175-2:1996	Informational (Approved)
IPC	IEEE	POSIX, System Administration - Part 4: Print Administration (former P1003.7.1)	P1387.4	Emerging (Draft)
CPC	OSF	DCE/Print Service (PRS) (part of OSF Personal Computer Services)	DME PRS	Informational (Not Recommended (No commercial products))

3.9.8.5.2 Alternative specifications. The following specifications are also available:

a. MIT: Palladium (the basis for DME print management).

b. Berkeley 4.2/4.3 Unix.

c. Siemens/Nixdorf: Printing Management (the basis for UI's distributed printing management specification and USL's reference implementation).

3.9.8.5.3 Standards deficiencies. SVID, OSF/1, and Berkeley Unix have no features to control the formatting or scheduling of print jobs. The SVID, OSF/1, and Berkeley Unix are designed for centralized environments. No Ada bindings exist for print management standards. POSIX.2

specifies only a minimal "lp" command, suitable for submitting print jobs; no printer administration facilities are provided.

3.9.8.5.4 Portability caveats. The System V Unix "lp" printing system, from which the POSIX "lp" command is derived, is not compatible with the Berkeley Unix "lpr" printing system.

The OSF DME distributed print management is based on MIT's Palladium. It has a different interface from UI/USL's distributed print management, which is based on the Siemens-Nixdorf Xprint program and, therefore, is incompatible.

3.9.8.5.5 Related standards. The following standards are related to print management services or standards:

a. ISO/IEC 9945-1:1996: POSIX Part 1 - System Application Programming Interface.

b. ISO 8824:1990: Abstract Syntax Notation 1 (ASN.1).

c. ISO 8825:1990: Basic Encoding Rules for ASN.1.

d. ISO 9072:1989: Remote Operations Service Element (ROSE).

e. ISO/IEC 9595: Common Management Information Service (CMIS).

f. ISO/IEC 9596: Common Management Information Protocol (CMIP).

g. ISO/IEC DIS 11578.2: Remote Procedure Call.

h. IEEE P1003.1e: Security Interface Standards for POSIX.

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

j. Internet RFC 1157: Simple Network Management Protocol.

k. Internet RFC 1158: Management Information Base for Network Management of TCP/IP-based Internets (MIB-II).

l. Network Management Forum: OMNIPoint 1.

3.9.8.5.6 Recommendations. The recommendation is to specify POSIX "lp" only for traditional, centralized systems for imminent procurements. Then look to ISO 10175 or IEEE 1387.4 in the long term.

3.9.9 Additional areas to be added. The following Open Systems Operations, Administration, and Maintenance services are under consideration for addition:

a. Problem reporting and tracking standards
b. Operations standards
c. Diagnostic standards
d. Fault isolation standards
e. System performance metrics and standards
f. Standard mechanisms to initiate remotely both OSE and proprietary diagnostics
g. End user support (help desks)
h. Systems integration standards

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 10 of 14 parts)

SECURITY SERVICES

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

TABLE OF CONTENTS

LIST OF TABLES

Cross-Reference of Security Service BSAs to Other Parts of the ITSG

3.10.2.1	Security models and architectures	3.2.5.1	
3.10.2.2	System development	3.2.5.2	3.9.7.1
3.10.2.3	Database security	3.4.2.1	3.9.7.13
3.10.2.4	Network security architecture	3.7.9.1	
3.10.2.5	Operating system security	3.8.5.1	
3.10.3.1	Certification and accreditation	3.2.5.4	3.9.7.10
3.10.3.2	Security risk management	3.2.5.5	3.7.9.2 3.9.7.3
3.10.3.3	Security management	3.7.9.3	3.8.5.4 3.9.7.2
3.10.3.4	Security association and key management	3.7.9.4	3.9.7.14
3.10.3.5	Security audit	3.7.9.5	3.9.7.4 3.11.5.3
3.10.3.6	Security alarm reporting	3.7.9.6	3.9.7.5 3.11.5.7
3.10.4.1	Personal authentication	3.2.5.3	3.3.8.2 3.9.7.6
3.10.4.2	Network authentication	3.7.9.7	
3.10.4.3	Entity authentication	3.8.5.3	3.9.7.7 3.11.5.2
3.10.5.1	System access control	3.4.2.2	3.9.7.8 3.11.5.1
3.10.5.2	Network access control	3.7.9.8	3.9.7.9
3.10.6.1	Systems confidentiality	3.5.10.1	
3.10.6.2	Registration of cryptographic techniques	3.9.7.15	
3.10.6.3	Data encryption security	3.5.10.2	3.7.9.9 3.11.5.5
3.10.6.4	Traffic flow confidentiality	3.7.9.10	
3.10.7.1	Systems integrity	3.4.2.4	
3.10.7.2	Data integrity techniques	3.4.2.5	
3.10.7.3	Network integrity	3.7.9.11	
3.10.8.1	Systems non-repudiation	3.5.10.4	3.7.9.12 3.11.5.6
3.10.8.2	Electronic signature	3.5.10.5	3.7.9.13
3.10.8.3	Electronic hashing	3.5.10.6	3.7.9.14 3.8.5.2
3.10.9.1	Detection and notification	3.2.5.6	3.9.7.11
3.10.9.2	Recovery	3.2.5.7	3.9.7.12
3.10.10.1	User interface security labeling	3.3.8.1	
3.10.10.2	Data management security labeling	3.4.2.3	
3.10.10.3	Data interchange security labeling	3.5.10.3	
3.10.10.4	Graphics security labeling	3.6.7.1	
3.10.10.5	Data communications security labeling	3.7.9.15	
3.10.10.6	Operating system security labeling	3.8.5.5	
3.10.10.7	Distributed computing security labeling	3.11.5.4	

3.10 Security services. The security services portion of the ITSG presents standards, guidelines, models, frameworks, and other documents related to the protection of information that is stored, transferred, or processed in automated systems. Use and compliance with the security standards identified in this document do not constitute authorization to process classified data. DOD policy covering the accreditation process must still be adhered to in order to obtain approval for processing of classified data.

3.10.1 Introduction and overview of security services. Security represents a cross-functional area in the ITSG. Consequently the security services identified in this part of the ITSG can be found in other parts as well. The intent of this chapter is to provide a single location where one can go to identify the standards, guidelines, etc. related to any pertinent security service area. All security-related BSAs in ITSG, Part 10 are "grounded" in the security service area; that is, the security service area is the foundation for all security BSAs. In turn, each security BSA is "cloned" into at least one other service area. The discussion and recommendations for these cloned BSAs are identical to that contained in Part 10, Security Services, and the standards tables for the cloned security BSAs are identical to the standards tables for the corresponding BSAs in Part 10. The presentation of this chapter is guided by two concerns. The first is to be consistent with the security principles and concepts of the DOD Goal Security Architecture (DGSA). Thus sections 3.10.4 through 3.10.9 correspond to the security services presented in the DGSA. The second is to provide an overview of the major security architectures, applications, and management concerns to ITSG users at all levels of expertise (sections 3.10.2 and 3.10.3).

For users of the ITSG who are not familiar with security terminology, the following references are suggested:

a. National Information Systems Security (INFOSEC) Glossary, National Security Telecommunications and Information Systems Security (NTISSI) No. 4009, 5 June 1992.

b. Glossary of Telecommunications Terms, FED-STD-1037B, 3 June 1991.

c. Dictionary of Information Systems, ANSI X3.172, 1990.

d. Security in Open Systems - Data Elements and Service Definitions, ECMA 138:1989 (based on ECMA TR46:1988).

e. Glossary of Computer Security Terms, NCSC-TG-004, version 1, 21 October 1988.

NOTE: Throughout Part 10, all tables shall have abbreviations listed under the column (Standard Type) as follows:

a. National Public Consensus = NPC
b. International Public Consensus = IPC
c. Government Public Consensus = GPC

d. Consortia Public Consensus = CPC
e. Corporate Private Non-Consensus = CPN-C

3.10.2 Architectures and applications. Standards, guidance, and frameworks that help to define security architectures and the placement of security into specific applications, are intended to provide guidance to standards developers. They do not provide implementable specifications against which conformance can be claimed.

3.10.2.1 Security models and architectures. (This BSA appears in part 2 and part 10.) Security models provide the necessary basis for the development of security-related protocols and security-related protocol elements.

3.10.2.1.1 Standards. Table 3.10-1 presents standards for security models and architectures.

TABLE 3.10-1 Security models and architectures standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
CPC	CEN/CENELEC/ ITAEGV	Taxonomy of Security Standardization	ITAEGV N69 Ver 2 of 4/30/1992	Informational (Approved)
IPC	ECMA	Security in Open Systems - Data Elements and Service Definitions	138 (1989)	Informational (Approved)
IPC	ECMA	Security in Open Systems - A Security Framework	TR/46 (1988)	Informational (Approved)
GPC	NIST	Guidelines for Security of Computer Applications	FIPS PUB 73:1980	Informational (Approved)
IPC	ITU-T	Security Architecture for OSI for CCITT Applications: Security, Structure, and Applications	X.800 (1991)	Informational (Approved)
CPC	X/Open	Security Guide (Second Edition)	G010 (2/91)	Informational (Approved)
IPC	ITU-T	Reference Model of OSE for CCITT Applications-Data Communications Networks-OSI Model and Notation, Services Definition	X.200 (1989)	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 3: Naming and Addressing	7498-3:1989	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 4: Management Framework	7498-4:1989	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Abstract Service Definition: (same as ITU-T X.511 (1993))	9594-3:1993 (or 1994)	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Procedures for Distributed Operations:(same as ITU-T X.519(1993))	9594-4:1993 (or 1994)	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Authentication Framework (same as ITU-T X.509 (1993))	9594-8:1993 (or 1994)	Informational (Approved)
IPC	ISO	OSI Upper Layer Security Model	10745:1993	Informational (Approved)
CPC	X/Open	Distributed Security Framework	G410 (12/94)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
NPC	IEEE	Guide to the POSIX Open Systems Environment - A Security Framework	P1003.22: 1995	Informational (Draft)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems, Part 1: Overview	10181-1	Informational (Draft)
IPC	ISO/IEC	Guide to Open Systems Security	TR by JTC1/SC21/N8380	Informational (Draft)
IPC	ISO/IEC	Management Plan for Security	JTC1/SC21 SD-7	Informational (Draft)

3.10.2.1.2 Alternative specifications. There are no alternate specifications.

3.10.2.1.3 Standards deficiencies. FIPS PUB 73 does not include information about modern security concepts.

3.10.2.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.2.1.5 Related standards. There are no related standards.

3.10.2.1.6 Recommendations. The DGSA, Volume 6 of the TAFIM, is the abstract and generic security architecture of the TAFIM. The DGSA provides security principles and target security capabilities to guide system security architects in creating specific security architectures consistent with the DGSA. The DGSA should be used by system security architects to develop logical and specific security architectures.

3.10.2.2 System development. (This BSA appears in part 2, part 9, and part 10.) Development of secure systems requires that security engineering be a key discipline in conjunction with other system, software, and hardware engineering activities.

3.10.2.2.1 Standards. Table 3.10-2 presents standards for system development.

TABLE 3.10-2 System development standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Network Interpretation	NCSC-TG-005, Version 1: 1987	Mandated (Approved)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
GPC	DOD	FORTEZZA Cryptologic Programmers' Guide	MD40000501-1.52: 1996	Mandated (Approved)
GPC	DOD	FORTEZZA Application Implementors' Guide	MD4002101-1.52: 1996	Mandated (Approved)
GPC	DOD	Software Development and Documentation	MIL-STD-498	Informational (Approved)
IPC	ISO/IEC	Software Life Cycle Processes	12207:1995	Informational (Approved)
NPC	EIA	Trial Use Standard - Standard for Information Technology - Software Life-Cycle Processes - Software Development - Acquirer-Supplier Agreement	EIA/IEEE J-STD-016: 1995	Informational (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Guidelines for Security of Computer Applications	FIPS PUB 83:1980	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Abstract Service Definition: (same as ITU-T X.511 (1993))	9594-3:1993 (or 1994)	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Procedures for Distributed Operations:(same as ITU-T X.519(1993))	9594-4:1993 (or 1994)	Informational (Approved)
IPC	ISO/IEC	OSI The Directory: Authentication Framework (same as ITU-T X.509 (1993))	9594-8:1993 (or 1994)	Informational (Approved)
CPC	X/Open	Generic Security Service API (GSS-API) Base	C441 (12/95)	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment n: Protection, Audit, and Control Interfaces (C Language), Draft 15	P1003.1e: 1995	Legacy (Draft)
NPC	IEEE	POSIX Part 2: Shell and Utilities - Amendment n: Protection and Control Utilities, Draft 15	P1003.2c: 1995	Emerging (Draft)
CPC	IETF	Generic Security Service - Application Program Interface, Version 2	RFC 2078: 1997	Emerging (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	IETF	Independent Data Unit Protection Generic Security Application Program Interface (IDUP-GSS-API)	draft-ietf-cat-idup-gss-06.txt, 26 November 1996	Emerging (Draft)
NPC	IEEE	Standard for Information Technology - Software Life Cycle Processes	IEEE/EIA 12207US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data	IEEE/EIA 12207.1US-date	Informational (Draft)
NPC	IEEE	Guide for Information Technology - Software Life Cycle Processes - Implementation Considerations	IEEE/EIA 12207.2US-date	Informational (Draft)

3.10.2.2.2 Alternative specifications. There are no alternative specifications.

3.10.2.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.2.2.4 Portability caveats. There are no portability caveats.

3.10.2.2.5 Related standards. DOD Directive 5200.28 "Security Requirements for Automated Information Systems (AISs)," provides the DOD-wide program for AIS security. It provides mandatory, minimum AIS security requirements for systems processing classified, sensitive but unclassified, and unclassified information. For intelligence systems, Director, Central Intelligence Directive (DCID) 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks," and "Security Manual for Uniform Protection of Intelligence Information Processed in Automated Information Systems and Networks," should be used in conjunction with DOD 5200.28-STD. The following guidelines also are for use with DOD 5200.28-STD:

a. NCSC-TG-006, Version 1, 28 March 1988, A Guide to Understanding Configuration Management in Trusted Systems

b. NCSC-TG-007, Version 1, 2 October 1988, A Guide to Understanding Design Documentation in Trusted Systems

c. NCSC-TG-008, Version 1, 15 December 1988, A Guide to Understanding Trusted Distribution in Trusted Systems

d. NCSC-TG-018, Version 1, July 1992, A Guide to Understanding Object Reuse in Trusted Systems

e. NCSC-TG-023, Version 1, July 1993, A Guide to Understanding Security Testing and Test Documentation in Trusted Systems

3.10.2.2.6 Recommendations. The standards listed as mandated are recommended.

MIL-STD-498 merges and supersedes DOD-STD-2167A and DOD-STD-7935A and has been approved for use by DOD with a waiver. Requirements for usage waivers are determined by each Service or Agency. MIL-STD-498 contains requirements for security and privacy for software development and documentation. EIA/IEEE J-STD-016: 1995 (formerly IEEE 1498/EIA IS 640) is based on MIL-STD-498 and was issued 30 September 1995 as a joint EIA/IEEE trial use standard. It is anticipated that J-STD-016 will be upgraded from trial use to full use and issued as an ANSI standard in 1997. It is also anticipated that IEEE/EIA 12207US, the U.S. adaptation of ISO/IEC 12207, will be sent to ANSI as a joint standard. IEEE/EIA 12207US will consist of a base standard (12207.0US) and two guides (12207.1US and 12207.2US). The base standard will contain ISO/IEC 12207 and is expected to be approved prior to July 1997. The guide IEEE/EIA 12207.1US, Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data, will contain the contents lists of the product descriptions from EIA/IEEE J-STD-016. The guide IEEE/EIA 12207.2US will provide guidance for: software reuse, software process management indicator categories for problem reporting, software/system architecture, development strategies, tailoring and build planning, software product evaluations, alternate means of compliance for joint reviews, configuration management and acquirer-supplier interaction. The two guides are expected to be final by Sept[illegible] The long range goal is migration to full use of IEEE/EIA 12207US; however, EIA/IEEE J-STD-016 is authorized for transition from MIL-STD-498, subject to Agency/Service approval, until organizational processes for IEEE/EIA 12207US are in place.

If FORTEZZA services are used, the following two guidelines should be consulted:

a. MD4002101-1.52, 3/5/96, FORTEZZA Application Implementors' Guide

b. MD4000502-1.52, 1/30/96, FORTEZZA Cryptologic Programmers' Guide, Revision 1.52

3.10.2.3 Database security. (This BSA ears in part 4, part 9, and part 10.) Database security standards provide protection for stored data from unauthorized access, modification, and denial of service.

3.10.2.3.1 Standards. Table 3.10-3 presents standards for database security.

TABLE 3.10-3 Database security standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Database Language SQL (Adopts ANSI X3.135-1992 (same as ISO 9075:1992))	FIPS PUB 127-2:1993	Informational (Approved)
GPC	NIST	Information Resource Dictionary System (IRDS) (adopts ANSI X3.138-1988 and X3.138A-1991)	FIPS PUB 156:1989	Informational (Approved)
NPC	ANSI	Database Language SQL	X3.135-1992	Informational (Approved)
IPC	ISO	Database Language SQL (same as ANSI X3.135-1992)	9075:1992	Informational (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Framework	10027:1990	Informational (Approved)
IPC	ISO/IEC	OSI Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element	9804:1990	Informational (Approved)
IPC	ISO/IEC	OSI Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Service Element	9805:1990	Informational (Approved)
NPC	ANSI	Information Resource Dictionary System (IRDS)	X3.138-1988	Informational (Approved)
IPC	ISO/IEC	Information Resource Dictionary System (IRDS) Services Interface Amendment 1: C Language Binding	10728 AMD 1:1994	Informational (Draft)

3.10.2.3.2 Alternative specifications. There are no alternative specifications.

3.10.2.3.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.2.3.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.2.3.5 Related standards. DOD 5200.28-STD, 26 December 1995, DOD Trusted Computer Systems Evaluation Criteria, is related to NCSC-TG-021. The following specifications are related to DOD 5200.28-STD:

a. NCSC-TG-018, Version 1, July 1992, A Guide to Understanding Object Reuse in Trusted Systems

b. NCSC-TG-025, Version 2, September 1991, A Guide to Understanding Data Remnants in Automated Information Systems

3.10.2.3.6 Recommendations. The mandated standard is recommended.

3.10.2.4 Network security architecture. (This BSA appears in both part 7 and part 10.) OSI security architecture defines the general security-related architectural elements, provides a general description of security services and related mechanisms, and defines the positions within the OSI Reference Model at which the services and mechanisms may be provided. Open systems security frameworks address data elements and sequences of operations that are used to obtain security services.

Note: The security architecture and framework standards are intended to provide guidance and background information to developers. In general, these standards do not provide implementable specifications against which conformance can be claimed.

3.10.2.4.1 Standards. Table 3.10-4 presents standards for network security architecture.

TABLE 3.10-4 Network security architecture standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Network interpretation	NCSC-TG-005, Version 1: 1987	Mandated (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems - Part 2: Authentication Framework	10181-2:1996	Informational (Approved)
IPC	ISO	OSI Upper Layer Security Model	10745:1993	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO/IEC	Lower Layer Security Model	TR 13594:1995	Informational (Approved)
CPC	IETF	Security Architecture for the Internet Protocol	RFC 1825: 1995	Emerging (Draft)
CPC	IETF	Security Architecture for the Internet Protocol	draft-ietf-ipsec-arch-sec-01.txt, 10 November 1996	Informational (Draft)
NPC	IEEE	Standard for Interoperable LAN Security - Part A: The Model	802.10a: 1989	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems, Part 1: Overview	10181-1	Informational (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 3: Access Control	10181-3	Informational (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 4: Non-Repudiation (same as ITU-TS X.813)	10181-4	Informational (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 5: Confidentiality	10181-5	Informational (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 6: Integrity (same as ITU-TS X.815)	10181-6	Informational (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems, Part 7: Security Audit Framework	10181-7	Informational (Draft)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems Part 8: Key Management	10181-8	Informational (Draft)

3.10.2.4.2 Alternative specifications. There are no alternative specifications.

3.10.2.4.3 Standards deficiencies. The Upper Layer Security Model (ISO 10745) primarily addresses FTAM requirements and does not deal with Directory, Transaction Processing, and X.400.

3.10.2.4.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.10.2.4.5 Related standards. NCSC-TG-011, Version 1, 1 August 1990, Trusted Network Interpretation Environments Guideline - Guidance for Applying the Trusted Network Interpretation is a guideline supporting the TCSEC.

3.10.2.4.6 Recommendations. The standards listed as mandated are recommended. Implementations involving security services should require conformance to the security principles and concepts of the DGSA (TAFIM, Volume 6) and supporting standards. RFC 1825 is an emerging standard that provides the current view of how to implement security functions within an Internet Protocol (IP) suite network. The Internet Draft document draft-ietf-ipsec-arch-sec-01.txt is a "work-in-progress" revision of RFC 1825.

3.10.2.5 Operating system security. (This BSA appears in both part 8 and part 10.) Operating system security services provide basic reference monitor services. These security mechanisms control the flow of data and use of applications to ensure the system security policy is adhered to.

3.10.2.5.1 Standards. Table 3.10-5 presents standards for operating system security.

TABLE 3.10-5 Operating system security standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	NIST	Password Usage	FIPS PUB 112: 1985	Mandated (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Guidelines on Evaluation of Techniques for Automated Personal Identification	FIPS PUB 48:1977	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 7: Security Alarm Reporting Function (same as ITU-T X.736)	10164-7:1992	Informational (Approved)
NPC	IEEE	POSIX, Part 1: System API - Amendment n: Protection, Audit, and Control Interfaces (C Language), Draft 15	P1003.1e: 1995	Emerging (Draft)
NPC	IEEE	POSIX Part 2: Shell and Utilities - Amendment n: Protection and Control Utilities, Draft 15	P1003.2c: 1995	Emerging (Draft)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
NPC	IEEE	Guide to the POSIX Open Systems Environment - A Security Framework	P1003.22: 1995	Informational (Draft)
NPC	SAE	Avionics Operating System API Requirements for the Society of Automotive Engineers	ARD 50067: 1996	Informational (Draft)
NPC	IEEE	Portable Operating System (POSIX), Part 1: System API/C Language (same as ISO 9945-1:1990)	1003.1:1990	Informational (Superseded)

3.10.2.5.2 Alternative specifications. No alternative specifications are available.

3.10.2.5.3 Standards deficiencies. General operating systems for personal computers are inherently insecure and should not be used in DOD acquisitions without an assurance of "add-on" security features and an approved security risk analysis providing at least a C2 level of trust per DOD Directive 5200.28.

The DGSA stresses the need for separation mechanisms, such as a separation kernel, to maintain strict isolation, that is, information domains must be completely isolated from each other. The DGSA concept requires that information transfers between domains may occur if, and only if, a relationship is explicitly defined in each information domain's security policy. There are no current or emerging standards for design and implementation of separation kernels nor for programming interfaces for separation kernels.

Due to its age, FIPS 48 does not include information on modern security concepts.

3.10.2.5.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.2.5.5 Related standards. ISO/IEC 9945-1 as profiled by FIPS 151-2 is related to IEEE P1003.1e and IEEE P1003.2c.

The following Compartmented Mode Workstation (CMW) specifications are related to operating system security:

a. DDS-2600-5502-87, Security Requirements for System High and Compartmented Mode Workstations

b. DDS-2600-6243-92, Compartmented Mode Workstation (CMW) Evaluation Criteria

c. DDS-2600-6216-91, Compartmented Mode Workstation (CMW) Labeling: Encoding Format

d. DDS-2600-6243-91, Compartmented Mode Workstation (CMW) Labeling: Source Code and User Interface Guidelines, Revision 1

3.10.2.5.6 Recommendations. The mandated standards are recommended.

3.10.3 System management. System management encompasses those security functions required to maintain an operationally secure system. This area includes analysis areas such as certification and accreditation and risk management, as well as operationally motivated concerns such as alarm reporting, audit, and cryptographic key management.

3.10.3.1 Certification and accreditation. (This BSA appears in part 2, part 9, and part 10.) Certification and accreditation constitute a set of procedures and judgments leading to a determination of the suitability of the system to operate in the targeted operational environment.

Accreditation is the official management authorization to operate a system. The accreditation normally grants approval for the system to operate (a) in a particular security mode, (b) with a prescribed set of countermeasures (administrative, physical, personnel, communications security, emissions, and computer security controls), (c) against a defined threat and with stated vulnerabilities and countermeasures, (d) within a given operational concept and environment, (e) with stated interconnections to other systems, (f) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility, and (g) for a specified period of time. The Designated Approving Authority(s) (DAA) formally accepts security responsibility for the operation of the system and officially declares that the specified system will adequately protect against compromise, destruction, or unauthorized modification under stated parameters of the accreditation. The accreditation decision affixes security responsibility with the DAA and shows that due care has been taken for security in accordance with the applicable policies.

An accreditation decision is in effect after the issuance of a formal, dated statement of accreditation signed by the DAA, and remains in effect for the specified period of time (varies according to applicable policies). A system processing classified or sensitive unclassified information should be accredited prior to operation or testing with live data unless a written waiver is granted by the DAA. In some cases (e.g., when dealing with new technology, during a transition phase, or when additional time is needed for more rigorous testing), the DAA may grant an interim approval to operate for a specified period of time. At the end of the specified time period, the DAA must make the final accreditation decision.

Certification is conducted in support of the accreditation process. It is the comprehensive analysis of both the technical and nontechnical security features and other safeguards of a system to establish the extent to which a particular system meets the security requirements for its mission and operational environment. A complete system certification must consider factors dealing with the system in its .nique environment, such as its proposed security mode of operation, specific users, applications, data sensitivity, system configuration, site/facility location, and interconnections with other systems. Certification should be done by personnel who are technically competent to assess the systems ability to meet the security requirements according to an acceptable methodology. The resulting documentation of the certification activities is provided to the DAA to support the accreditation decision. Many security activities support certification, such as risk analysis, security test and evaluation, and various types of evaluations.

Ideally, certification and accreditation procedures encompass the entire life cy 'e of the system. Ideally, the DAA is involved from the inception of the system to ensure that the accreditation

goals are clearly defined. A successful certification effort implies that system security attributes were measured and tested against the threats of the intended operational scenarios. Additionally, certification and accreditation are seen as continuing and dynamic processes; the security state of the system needs to be tracked and assessed through changes to the system and its operational environment. Likewise, the management decision to accept the changing system for continued operation is an ongoing decision process.

Standards for certification and accreditation services provide definitions and procedures for the testing and accreditation of computer systems in so far as their conformance with security standards is concerned.

3.10.3.1.1 Standards. Table 3.10-6 presents standards for certification and accreditation.

TABLE 3.10-6 Certification and accreditation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	NIST	Guideline for Computer Security Certification and Accreditation	FIPS PUB 102:1983	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
GPC	DOD	DOD Information Technology Certification and Accreditation Process	DITSCAP: 1996	Informational (Draft)

3.10.3.1.2 Alternative specifications. No other consortia or de facto specifications are available.

3.10.3.1.3 Standards deficiencies. Because of its age, FIPS PUB 102 does not include services for the certification and accreditation of all modern security concepts.

Certification and accreditation evaluation criteria that address current information technology, such as distributed computing and networking, are needed. As new criteria such as the Common Criteria emerge, revision of existing certification and accreditation guidelines may be required.

3.10.3.1.4 Portability caveats. There are no portability problems related to the existing specifications.

3.10.3.1.5 Related standards. NCSC-TG-029, "Introduction to Certification and Accreditation," January 1994, discusses basic concepts related to certification and accreditation and is the first of a series of guidelines in the "Rainbow Series" supporting the Trusted Computer System Evaluation Criteria (TCSEC) standard.

3.10.3.1.6 Recommendations. The mandated standard is recommended.

Procurements that require that an AIS be certified and/or accredited must reference DOD Directive 5200.28 and applicable designated approving authority guidance. DOD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," requires certification and accreditation of AIS. FIPS PUB 102, Guidelines for Computer Security and Accreditation provides Federal guidelines for certification and accreditation. Because of its age, this FIPS PUB does not include services for the certification and accreditation of all modern security concepts. DOD 5200.28-STD provides criteria to assess security assurances of trusted systems to specific classes. DCID 1/16 provides security requirements for systems processing intelligence information.

The DISA CISS and NSA are each developing documents that will standardize the certification and accreditation process within DOD. Each document is in draft form; final documents are expected to be issued in 1997. The NSA document, "Certification and Accreditation Process Handbook for Certifiers," will be published as a "Rainbow" series document supporting the TCSEC standard. This NSA handbook focuses on certification and accreditation of standalone systems. The DISA CISS document, "DOD Information Technology Certification and Accreditation Process" (DITSCAP), will be published as a DOD publication. The DITSCAP focuses on certification and accreditation in conjunction with the programmatic aspects of the DII.

3.10.3.2 Security risk management. (This BSA appears in part 2, part 7, part 9, and part 10.) Security risk management supports accreditation through a risk analysis of an information system and its operational environment, and the steps taken to manage the risk requirements.

3.10.3.2.1 Standards. Table 3.10-7 presents standards for security risk management.

TABLE 3.10-7 Security risk management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	NIST	Guideline for the Analysis of Local Area Network Security	FIPS PUB 191:1994	Informational (Approved)
GPC	NIST	Guideline for Automated Data Processing Risk Analysis	FIPS PUB 65:1979	Informational (Approved)
GPC	NIST	Guidelines for Automatic Data Processing Physical Security and Risk Management	FIPS PUB 31:1974	Informational (Approved)

3.10.3.2.2 Alternative specifications. There are no alternative specifications.

3.10.3.2.3 Standards deficiencies. Because of its age, FIPS PUB 31 does not include information about modern security concepts.

3.10.3.2.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.3.2.5 Related standards. The following standards are related to the TCSEC standard:

a. CSC-STD-003-85 25 June 1985, Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer Security Evaluation Criteria in Specific Environments

b. CSC-STD-004-85, 25 June 1985, Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements - Guidance for Applying the Department of Defense Trusted Computer Security Evaluation Criteria in Specific Environments

3.10.3.2.6 Recommendations. The mandated standard is recommended. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," provides guidance on effective security risk management of federal information systems. NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook" provides additional guidance on risk management. DOD Directive 5200.28 requires a risk analysis of an information system be conducted in its operational environment to support accreditation of the information system. System implementors should perform the risk analysis in accordance with CSC-STD-003-85 and CSC-STD-004-85 to determine the appropriate DOD-5200.28-STD class.

3.10.3.3 Security management. (This BSA appears in part 7, part 8, part 9, and part 10.) Security management is a particular instance of information system management. Security management provides supporting services that contribute to the protection of information and resources in open systems in accordance with information domain and information security policies. The basic elements that must be managed are users, security policies, information, information processing systems that support one or more security policies, and the security functions that support the security mechanisms (automated, physical, personnel, or procedural) used to implement security services. For each of these elements, the managed objects that constitute them must be identified and maintained. For example, users must be known and registered, security policies must be represented and maintained and information objects must be identified and maintained. Security policies, security services and security mechanisms are the first classes of managed objects.

3.10.3.3.1 Standards. Table 3.10-8 presents standards for security management.

TABLE 3.10-8 Security management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Network Interpretation	NCSC-TG-005, Version 1: 1987	Mandated (Approved)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
IPC	ITU-T	The Directory: Procedures for Distributed Operation (X-ref: ISO 9594-4)	X.518: 1993	Informational (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) - Part 1: Specification (Includes amendment 1 and 2 of ISO/IEC 9596-1:1990)	9596-1:1991	Informational (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 7: Security Alarm Reporting Function (same as ITU-T X.736)	10164-7:1992	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 8: Security Audit Trail Function (same as ITU-T X.740)	10164-8:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 9: Objects and Attributes for Access Control	10164-9:1995	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	IEEE	POSIX Part 2: Shell and Utilities - Amendment n: Protection and Control Utilities, Draft 15	P1003.2c: 1995	Emerging (Draft)
NPC	IEEE	POSIX, Part 1: System API - Amendment n: Protection, Audit, and Control Interfaces (C Language), Draft 15	P1003.1e: 1995	Emerging (Draft)
CPC	OMG	Common Object Request Broker Architecture (CORBA) Security	OMG 95-12-1: 1995	Emerging (Draft)
CPC	IETF	Domain Name System (DNS) Security Extensions	RFC 2065:1997	Emerging (Draft)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179:1992	Informational (Superseded)
NPC	IEEE	Standard for Interoperable LAN Security - Part D: Security Management	802.10d	Informational (Formative)
IPC	ISO/IEC	Management Plan for Security	JTC1/SC21 SD-7	Informational (Draft)

3.10.3.3.2 Alternative specifications. There are no alternative specifications.

3.10.3.3.3 Standards deficiencies. Deficiencies exist in standardization of security policy rule representation; key management, including generation, distribution, and accounting; audit information formats; exchange of security management information; and remote security management.

The DGSA principle of decision and enforcement separation requires that the functions determining how to enforce a security policy and the actual enforcement of the policy be implemented independently. That is, the enforcement mechanisms do not need any knowledge of security policy. Standards are needed for object class definitions for classes of managed objects and for methods of representing security policy.

The DGSA calls for a separation mechanism, such as separation kernel, to mediate all calls to security critical functions to ensure that strict isolation is maintained. Standardization of object class definitions for management of critical functions used within the separation kernel is needed.

The present ISO/IEC 10164-7 "Security Alarm Reporting Function," and 10164-8, "Security Audit Trail Function," standards were designed with network security in mind. Little work has been done, either in standards groups or in products, on how to use these standards for general system management (e.g., computer systems and software).

FIPS PUB 179-1 supersedes FIPS PUB 179. The present GNMP specifications require ISO CMIS/CMIP to communicate management information and ISO OSI networking protocols. Plans are for the GNMP eventually to provide a capability to integrate the present GNMP with SNMP. One reason for this goal is the widespread use of SNMP.

No Ada bindings exist for any of the ISO or consortia system management specifications.

The IEEE POSIX Security Working Group (formerly P1003.6) is defining security extensions to the base POSIX interface standard (ISO 9945-1), to include support for audit, privilege, discretionary and mandatory access control, and information labels. These have been redesignated IEEE P1003.1e and IEEE P1003.2c. The draft standards are still incomplete, and the specifications may change.

The POSIX/UNIX permission bits are inadequate for fine-grained control over exactly which users can perform specified actions to particular files.

In the IETF, efforts to develop an acceptable security standard for SNMPv2 have been on hold since September 1995 when the IETF SNMP Working Group failed to agree on the proposals submitted. Since then, two sets of proposals for providing SNMPv2 security have emerged. The first set of proposed specifications, the User-based Security Model (USEC), also referred to as SNMPv2u, consists of two documents: RFC 1909, "An Administrative Infrastructure for SNMPv2" and RFC 1910, "The User-based Security Model for SNMPv2." Both RFCs were issued 28 February 1996 and are classified by the IETF as experimental RFCs. The other proposal is known as SNMPv2*, which its proponents claim is heavily based on USEC. Neither USEC nor SNMPv2* has been approved for a standards track by IETF.

3.10.3.3.4 Portability caveats. The structure of certain traditional UNIX directories, such as the familiar "/tmp," "/usr/spool," and "/usr/spool/mail" directories must be expressly managed to accommodate the P1003.1e and P1003.2c security stand[illegible]. This is because these are directories to which all users have access and to which many programs write. A change in the way programs write to directories has the potential for causing software portability and systems administrator portability problems.

The traditional UNIX permission bits that have been carried into POSIX are inadequate for defining exactly which user can perform specific actions on specific files. Eliminating the permission bits in favor of Access Control Lists could make the secure POSIX systems incompatible with non-POSIX compliant systems and many applications.

OSF DCE Version 1.1's authentication service is based on Kerberos Version 5 (RFC 1510), but is not totally compatible wth RFC 1510. DCE 1.2.2 adds testing and official support for Kerberos Version 5.

3.10.3.3.5 Related standards. ISO/IEC 9945-1 as profiled by FIPS PUB 151-2 is related to IEEE P1003.1e and IEEE P1003.2c.

3.10.3.3.6 Recommendations. The mandated standards are recommended.

All IEEE P1003.1e and IEEE P1003.2c security systems should incorporate Access Control Lists as an optional feature in addition to permission bits (not "in place of" permission bits). The incompatibilities between the two access control methods (permission bits and access control lists) are not resolvable. The best method for resolving the overall problems seem to be incorporation Access Control Lists as an optional feature on top of permission bits. The

permission bits would represent the lowest common denominator of security, showing the maximum amount of openness possible in a system. Organizations needing only the lowest level of security could continue to use the familiar permission bits and associated "chmod" command. Use of access control lists will require a change in security policy such that access is granted if and only if permission is granted and access control permits it.

3.10.3.4 Security association and key management. (This BSA appears in part 7, part 9, and part 10.) A security association is the totality of communication and security mechanisms and functions (e.g., communications protocols, security protocols, doctrinal mechanisms, security-critical mechanisms and functions) that securely binds together two security contexts in different end systems or relay systems supporting the same information domain. A security association is an application association that includes additional support from security functions and mechanisms. Key management provides procedures for handling cryptographic keying material to be used in symmetric or asymmetric cryptographic mechanisms. It includes key generation, key distribution, key storage, key archiving, and key deletion.

3.10.3.4.1 Standards. Table 3.10-9 presents standards for security association and key management.

TABLE 3.10-9 Security association and key management standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NSA	Key Exchange Algorithm	R21-TECH-23-94: 1994	Mandated (Approved)
GPC	NSA	Secure Data Network System (SDNS) Key Management Protocol (KMP)	SDN.903, Version 3.2: 1989	Mandated (Approved)
GPC	NIST	Key Management Using ANSI X9.17	FIPS PUB 171:1992	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 2:Security Exchange Service Element Definition	11586-2:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 3: Security Exchange Service Element Protocol Specification	11586-3:1994	Informational (Approved)
IPC	ISO	Banking Key Management (wholesale)	8732:1988	Informational (Approved)
NPC	ANSI	Financial Institution Key Management (wholesale)	X9.17-1991	Informational (Approved)
NPC	IEEE	Standard for Interoperable LAN Security - Part C: Key Management Protocol (KMP)	802.10c	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems Part 8: Key Management	10181-8	Informational (Draft)
CPC	IETF	Internet Security Association and Key Management Protocol (ISAKMP)	draft-ietf-ipsec-isakmp-07.txt,.ps, 21 February 1997	Informational (Draft)
CPC	IETF	The Photuris Session Key Management Protocol	draft-simpson-photuris-11.txt, 13 June 1996	Informational (Draft)
CPC	IETF	Simple Key Management for Internet Protocols (SKIP)	draft-ietf-ipssec-skip-07.txt, August 1996	Informational (Draft)
CPC	IETF	The Oakley Key Determination Protocol	draft-ietf-ipsc-oakley-01.txt, 5/10/96	Informational (Draft)
NPC	IEEE	Standard for Public-Key Cryptography	P1363	Informational (Formative)

3.10.3.4.2 Alternative specifications. There are no alternative specifications.

3.10.3.4.3 Standards deficiencies. There is a lack of guidance for establishing a Public Key Infrastructure (PKI) to automatically manage public keys through the use of public key certificates. In April 1994, NIST, in conjunction with seven other federal agencies, completed a study on automated management of public keys and associated public key certificates on a nationwide basis. Based on the recommendations of the study, GSA is establishing a PKI pilot project to provide public key certificate services for participating government agencies.

3.10.3.4.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.10.3.4.5 Related standards. There are no related standards.

3.10.3.4.6 Recommendations. The mandated standards are recommended. In FORTEZZA applications, the NSA-developed Key Exchange Algorithm, R21-TECH-23-94, must be used.

IEEE P1363, Standard for Public-Key Cryptography, is under development, with the first version expected to be ready for balloting in 1997.

The IETF's IP Security Protocol (IPSEC) Working Group (WG) is developing an Internet Key Management Protocol (IKMP) that will be specified as an application layer protocol independent of the lower layer security protocol. The IKMP will be based on ISAKMP/Oakley work begun in the Internet Draft documents for ISAKMP and the Oakley Key Determination Protocol.

3.10.3.5 Security audit. (This BSA appears in part 7, part 9, part 10, and part 11.) Security auditing is a review or examination of records and activities to test controls, ensure compliance with policies and procedures, detect breaches in security, and indicate changes in operation (paraphrased from ISO 7498-2).

3.10.3.5.1 Standards. Table 3.10-10 presents standards for security audit.

TABLE 3.10-10 Security audit standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
CPC	NMF	OMNIPoint I (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 8: Security Audit Trail Function (same as ITU-T X.740)	10164-8:1993	Informational (Approved)
CPC	X/Open	Security Interface Specification: Auditing and Authentication	S020: 1990	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems, Part 7: Security Audit Framework	10181-7	Informational (Draft)
IPC	ISO/IEC	OSI Distributed Transaction Processing (DTP) - Draft Amendments to Parts 1-3: Transaction Processing Security	WDAMs ((SC21 N6232) to ISO 10026-1,2,3) 1994	Informational (Draft)

3.10.3.5.2 Alternative specifications. There are no alternative specifications.

3.10.3.5.3 Standards deficiencies. ISO Transaction Processing Security work (WDAMs to ISO 10026-1,2,3) is in the early stages. Its content is not defined, and it cannot be used for procurement. ISO 10164-8 does not define a security audit, or explain how to perform one. It does not define implementation aspects, occasions where the use of the security audit trail function is appropriate, or the services necessary for the establishment and normal or abnormal release of a management association.

There is a need for a standard for programming interfaces to support development of portable tools for audit trail analysis and configuration.

3.10.3.5.4 Portability caveats. Proposed amendments to ISO 10026 have ceased. This is a high portability risk area.

3.10.3.5.5 Related standards. The following guidelines support the TCSEC standard:

a. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation

b. NCSC-TG-011, Version 1, 1 August 1990, Trusted Network Interpretation Environments Guideline - Guidance for Applying the Trusted Network Interpretation

c. NCSC-TG-001, Version 2, June 1988, A Guide to Understanding Audit in Trusted Systems

3.10.3.5.6 Recommendations. The mandated standard is recommended.

3.10.3.6 Security alarm reporting. (This BSA appears in part 7, part 9, part 10, and part 11.) Security alarm reporting is the capability to receive notifications of security-related events, alerts of any misoperations in security services and mechanisms, alerts of attacks on system security, and information as to the perceived severity of any misoperation, attack, or breach of security.

3.10.3.6.1 Standards. Table 3.10-11 presents standards for security alarm reporting.

TABLE 3.10-11 Security alarm reporting standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 7: Security Alarm Reporting Function (same as ITU-T X.736)	10164-7:1992	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179:1992	Informational (Superseded)

3.10.3.6.2 Alternative specifications. There are no alternative specifications.

3.10.3.6.3 Standards deficiencies. FIPS PUB 179-1 supersedes FIPS PUB 179. ISO 10164-7 does not define implementation aspects, specify the manner in which management is accomplished by the user of the Security Alarm Reporting Function (SARF), define interactions that result in the use of the SARF, or specify the services necessary for the establishment and normal and abnormal release of a management association.

3.10.3.6.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.3.6.5 Related standards. There are no related standards.

3.10.3.6.6 Recommendations. There are no recommended standards for security alarm reporting.

3.10.4 Authentication. Authentication and identification objectives ensure processes, systems, and personnel are uniquely identified and authenticated. The granularity of identification must be sufficient to determine the processes, system, and personnel's access rights. The authentication process must provide an acceptable level of assurance as to the professed identity of the processes, systems, and personnel.

3.10.4.1 Personal authentication. (This BSA appears in part 2, part 3, part 9, and part 10.) Personal authentication supports the accountability objective of being able to trace all security relevant events to individual users. In addition to supporting unique identification, standards are provided to authenticate the claimed identity.

3.10.4.1.1 Standards. Table 3.10-12 presents standards for personal authentication.

TABLE 3.10-12 Personal authentication standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
GPC	NIST	Password Usage	FIPS PUB 112: 1985	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
GPC	NIST	Guidelines on Evaluation of Techniques for Automated Personal Identification	FIPS PUB 48:1977	Informational (Approved)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - The Directory: Authentication Framework edition 2 (Same as ITU-T X.509:1993)	9594-8.2:1993	Informational (Approved)
GPC	NIST	Guideline for Use of Advanced Authentication Technology Alternatives	FIPS PUB 190:1994	Informational (Approved)
CPC	IETF	A One-Time Password System	RFC 1938: 1996	Emerging (Draft)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
CPC	IETF	The Kerberos Network Authentication Service (V5)	RFC 1510:1993	Informational (Draft)

3.10.4.1.2 Alternative specifications. There are no alternative specifications.

3.10.4.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.4.1.4 Portability caveats. OSF DCE Version 1.1's authentication service is based on Kerberos Version 5 (RFC 1510), but is not totally compatible with RFC 1510. DCE 1.2.2 adds testing and official support for Kerberos Version 5.

3.10.4.1.5 Related standards. The following standards are related to personal authentication standards (particularly TCSEC):

a. DOD 5200.28-STD, DOD Trusted Computer Systems Evaluation Criteria

b. NCSC-TG-017, Version 1, "A Guide to Understanding Identification and Authentication in Trusted Systems

c. CSC-STD-002-85, "Password Management Guideline"

d. NCSC-WA-002-85, "Personal Computer Security Considerations"

e. ITU-T X.509 (1993) (same as ISO 9594-8), The Directory: Authentication Framework

3.10.4.1.6 Recommendations. The mandated standards are recommended.

3.10.4.2 Network authentication. (This BSA appears in part 7 and part 10.) Network authentication services establish the validity of a claimed identity (peer-entity) or origin (data) (paraphrased from ISO 7498-2).

3.10.4.2.1 Standards. Table 3.10-13 presents standards for network authentication.

TABLE 3.10-13 Network authentication standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Information Technology - Defense Standardized Profiles AMHXn(D)- Message Handling Systems - Message Security Protocol (MSP) Parts 1-5	MIL-STD-2045-18500: 1993	Mandated (Approved)
IPC	ITU-T	The Directory: Authentication Framework (X-ref: ISO 9594-8)	X.509, Version 3: 1993	Mandated (Approved)
GPC	DOD	Trusted Network Interpretation	NCSC-TG-005, Version 1: 1987	Mandated (Approved)
GPC	NIST	Digital Signature Standard (DSS)	FIPS PUB 186:1994	Mandated (Approved)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180-1:1995	Mandated (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 3 (SP3)	SDN.301, Revision 1.5: 1989	Mandated (Approved)
GPC	DOD	FORTEZZA Interface Control Document	FORTEZZA ICD Rev P1.5: 1994	Mandated (Approved)
GPC	DOD	FORTEZZA Plus Interface Control Document	FORTEZZA Plus ICD Rel 3.0: 1995	Mandated (Approved)
NPC	IEEE	Standard for Interoperable LAN Security - Part B: Secure Data Exchange (SDE)	802.10b:1992	Legacy (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, Rev. 3.0: 1994	Legacy (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, v. 4.0, Rev. A: 1997	Emerging (Approved)
IPC	ISO	Information Processing Systems - Open Systems Interconnection - Service Definition for the Association Control Service Element (ACSE), Revised Edition	8649:1992 (Incorporates AM 1&2)	Informational (Approved)
IPC	ISO	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the ACSE, Revised Edition	8650:1992 (Incorporates AM 1)	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 2:Security Exchange Service Element Definition	11586-2:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 3: Security Exchange Service Element Protocol Specification	11586-3:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 4: Protecting Transfer Syntax Specification	11586-4:1994	Informational (Approved)
IPC	ISO	Transport Layer Security Protocol (TLSP) (Includes Amendment 1)	10736:1994	Informational (Approved)
IPC	ISO	Network Layer Security Protocol (NLSP)	11577:1994	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems - Part 2: Authentication Framework	10181-2:1996	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 4 (SP4)	SDN.401, Rev. 1.3:1989	Informational (Approved)
GPC	NSA	Message Security Protocol (MSP) with MIME	SDN.704, Rev. 1.4: 1996	Informational (Approved)
CPC	IETF	Privacy Enhancement for Internet Electronic Mail	RFC 1421-1424:1993	Informational (Draft)
CPC	IETF	The Secure Sockets Layer (SSL) Protocol Version 3.0	draft-ietf-tls-ssl-version3-00.txt, 18 November 1996	Emerging (Draft)
CPC	IETF	S/MIME Message Specification: PKCS Security Services for MIME	draft-dusse-mime-msg-spec-00.txt, September 1996	Informational (Draft)
IPC	ISO	OSI File Transfer, Access and Management (FTAM) - Parts 1-4: Amendment 4: Enhancement to FTAM Security Services	8571-1,2,3,4:1988/ WDAM4:1993	Informational (Draft)
GPC	NSA	Use of X.509 Certificates	SDN.706, Rev. 2.0: 1997	Informational (Draft)
GPC	NSA	X.509 Certificates and Certification Revocation List Profiles and Certificate Path Processing Rules for the Multilevel Information Systems Security Initiative (MISSI)	SDN.706, Rev. 1.1: 1996	Informational (Draft)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179:1992	Informational (Superseded)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180:1993	Informational (Superseded)

3.10.4.2.2 Alternative specifications. There are no alternative specifications.

3.10.4.2.3 Standards deficiencies. FIPS PUB 179-1 supersedes FIPS PUB 179. Procurements requiring authentication in FTAM cannot specify a standard at this time. The ISO FTAM security effort is in its early stages. Current proprietary FTAM security is based on passwords for authentication. ISO TP security work is in the early stages. Its content is not defined, and it cannot be used in a procurement.

3.10.4.2.4 Portability caveats. Proposed security enhancements to FTAM (WDAM4 to ISO 8571) have ceased. This is a high portability risk area.

3.10.4.2.5 Related standards. NCSC-TG-011, Version 1, 1 August 1990, Trusted Network Interpretation Environments Guideline - Guideline for Applying the Trusted Network Interpretation, supports NCSC-TG-005.

3.10.4.2.6 Recommendations. The mandated standards are recommended.

MIL-STD-2045-18500 describes the security provided by MSP. It should be used for DOD message systems that are required to exchange classified and sensitive but unclassified information. It is based on Version 3.0 of the MSP documented in SDN701, "Secure Data Network System (SDNS) Message Security Protocol," Revision 1.5, 1 August 1989. MSP is under revision to Version 4.0 to accommodate, in part, Allied requirements. This DOD Standardized Profile (DSP) standard will be replaced by a portion of the U.S. Supplement to Allied Communications Publication (ACP) 123 or ACP 120, Common Security Protocol, when the revision to MSP is complete.

SP3 provides connectionless security services and is the basis for ISO 11577. SP3 is designed to be used at the top of layer 3.

DSS is intended to specify general security requirements for generating digital signatures. Conformance to this standard does not assure that a particular implementation is secure. The responsible authority in each Government agency or department shall assure that an overall implementation provides an acceptable level of security. DSS can be used in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication. It uses the Secure Hash Algorithm (SHA) specified in FIPS PUB 180-1, which supersedes FIPS PUB 180. NIST is developing a validation program to test implementations for conformance to DSS.

The following two documents should be consulted for systems required to interface with the Defense Message System (DMS):

a. FORTEZZA Interface Control Document, Rev. 1.5, 22 December 1994
b. FORTEZZA Plus Interface Control Document, Release 3.0, 1 June 1995

SDN.701, Rev.3.0, is used with DMS, Phase 1. It is for use with legacy systems only.

IEEE 802.10b is for use with l\ cy LANs only.

3.10.4.3 Entity authentication. (This BSA appears in part 8, part 9, part 10, and part 11.) Entity authentication standards address data, processes, systems, and enterprises.

3.10.4.3.1 Standards. Table 3.10-14 presents standards for entity authentication.

TABLE 3.10-14 Entity authentication standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
GPC	NIST	Computer Data Authentication	FIPS PUB 113:1985	Informational (Approved)
GPC	NIST	Entity Authentication Using Public Key Cryptography	FIPS PUB 196:1996	Emerging (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO	Financial Transactions - Retail Banking Security Requirements for Message Authentication	9807	Informational (Approved)
IPC	ISO	Entity Authentication Mechanisms - Part 1: General Model	9798-1:1991	Informational (Approved)
IPC	ISO	Entity Authentication Mechanisms - Part 3: Entity Authentication Using a Public Key Algorithm	9798-3:1993	Informational (Approved)
GPC	NIST	Guideline for Use of Advanced Authentication Technology Alternatives	FIPS PUB 190:1994	Informational (Approved)
IPC	ISO	Entity Authentication - Part 2: Mechanisms Using Symmetric Encipherment Algorithms	9798-2:1994	Informational (Approved)
IPC	ISO	Entity Authentication - Part 4: Mechanisms Using a Cryptographic Check Function	9798-4:1995	Informational (Approved)
CPC	X/Open	Security Interface Specification: Auditing and Authentication	S020: 1990	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
CPC	IETF	The Kerberos Network Authentication Service (V5)	RFC 1510:1993	Informational (Draft)
IPC	ISO	Entity Authentication Mechanisms, Part 5: Entity Authentication Using Zero Knowledge Techniques	9798-5:1993	Informational (Draft)

3.10.4.3.2 Alternative specifications. There are no alternative specifications.

3.10.4.3.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.4.3.4 Portability caveats. OSF DCE Version 1.1's authentication service is based on Kerberos Version 5 (RFC 1510), but is not totally compatible with RFC 1510. DCE 1.2.2 adds testing and official support for Kerberos Version 5.

3.10.4.3.5 Related standards. The following standards are related to entity authentication:

a. DOD NCSC-TG-017, Version 1, September 1991, Guide to Understanding Identification and Authentication in Trusted Systems.

b. FIPS PUB 196, 11 October 1996.

FIPS PUB 196 becomes effective 6 April 1996. It is based on ISO/IEC 9798-3:1993 and specifies two challenge-response protocols by which entities in a computer system may authenticate their identities to one another. FIPS PUB 196 is for use in public key based challenge-response and authentication systems at the application layer within computer and digital telecommunications systems.

3.10.4.3.6 Recommendations. The mandated standards are recommended.

3.10.5 Access control. Access control is the prevention of unauthorized use of a resource including its use in an unauthorized manner. The following areas present standards which ensure that information and resources are accessed only by authorized processes, systems, and personnel, and are used only for their intended purposes.

3.10.5.1 System access control. (This BSA appears in part 4, part 9, part 10, and part 11.) System access control standards provide high-level guidance on access control frameworks and implementation.

3.10.5.1.1 Standards. Table 3.10-15 presents standards for system access control.

TABLE 3.10-15 System access control standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 9: Objects and Attributes for Access Contro.	10164-9:1995	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 3: Access Control	10181-3	Informational (Draft)

3.10.5.1.2 Alternative specifications. There are no alternative specifications.

3.10.5.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.5.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.5.1.5 Related standards. The following guidelines support the TCSEC standard:

a. NCSC-TG-003, Version 1, September 1987, A Guide to Understanding Discretionary Access Control in Trusted Systems

b. NCSC-TG-028, Version 1, May 1992, Assessing Controlled Access Protection

c. NCSC-TG-020-A, August 1989, Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX System

3.10.5.1.6 Recommendations. The mandated standards are recommended.

3.10.5.2 Network access control. (This BSA appears in part 7, part 9, and part 10.) Access control is the prevention of unauthorized use of a resource, including its use in an unauthorized manner.

3.10.5.2.1 Standards. Table 3.10-16 presents standards for network access control.

TABLE 3.10-16 Network access control standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Information Technology - Defense Standardized Profiles AMHXa(D)- Message Handling Systems - Message Security Protocol (MSP) Parts 1-5	MIL-STD-2045-18500: 1993	Mandated (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 3 (SP3)	SDN.301, Revision 1.5: 1989	Mandated (Approved)
NPC	IEEE	Standard for Interoperable LAN Security - Part B: Secure Data Exchange (SDE)	802.10b:1992	Legacy (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO	Transport Layer Security Protocol (TLSP) (Includes Amendment 1)	10736:1994	Informational (Approved)
IPC	ISO	Network Layer Security Protocol (NLSP)	11577:1994	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
GPC	NIST	Guidelines for Security of Computer Applications	FIPS PUB 83:1980	Informational (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 4 (SP4)	SDN.401, Rev. 1.3:1989	Informational (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, v. 4.0, Rev. A: 1997	Emerging (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, Rev. 3.0: 1994	Legacy (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179:1992	Informational (Superseded)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - The Directory - Parts 1-4 DAM1: Access Control	9594-1,2,3,4:1990/ DAM1	Informational (Draft)
IPC	ISO/IEC	Information Technology - Open Systems Interconnection - The Directory - Part 8: Authentication Framework, DAM1: Access Control	9594-8:1990/ DAM1	Informational (Draft)
IPC	ISO	OSI File Transfer, Access and Management (FTAM) - Parts 1-4: Amendment 4: Enhancement to FTAM Security Services	8571-1,2,3,4:1988/ WDAM4:1993	Informational (Draft)

3.10.5.2.2 Alternative specifications. There are no alternative specifications.

3.10.5.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown. FIPS PUB 179-1 supersedes FIPS PUB 179.

3.10.5.2.4 Portability caveats. Proposed security enhancements to FTAM (WDAM4 to ISO 8571) has ceased. This is a high portability risk area because no standards exist.

3.10.5.2.5 Related standards. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation, and NCSC-TG-011, Version 1, August 1990, Trusted Networks Interpretation Environments Guideline - Guideline for Applying the Trusted Network Interpretation, supports the DOD 5200.28-STD.

3.10.5.2.6 Recommendations. The mandated standards are recommended.

MIL-STD-2045-18500 describes the security provided by MSP. It should be used for DOD message systems that are required to exchange classified and sensitive but unclassified information. It is based on Version 3.0 of the MSP documented in SDN.701, "Secure Data Network System (SDNS) Message Security Protocol," Revision 1.5, 1 August 1989. MSP is under revision to Version 4.0 to accommodate, in part, Allied requirements. This DOD Standardized Profile (DSP) standard will be replaced by a portion of the U.S. Supplement to ACP 123 or ACP 120, Common Security Protocol, when the revision to MSP is complete.

SDN.701, Rev.3.0, is used with DMS, Phase 1. It is for use with legacy systems only.

SP3 provides connectionless security services and is the basis for ISO 11577. SP3 is designed to be used at the top of layer 3.

The work on File Transfer, Access, and Management (FTAM) security (WDAM4 to ISO 8571) security enhancements has been suspended. Procurements requiring access control for FTAM and transaction processing should not use these standards.

IEEE 802.10b is for use with legacy LANs only.

3.10.6 Confidentiality. Confidentiality objectives ensure the protection of the system's varied information and resources from unauthorized access. This section provides open systems standards guidance as well as the specifics of cryptography and traffic flow confidentiality.

3.10.6.1 Systems confidentiality. (This BSA appears in part 5 and part 10.) These standards provide the high-level framework with which to view the security service of confidentiality in systems.

3.10.6.1.1 Standards. Table 3.10-17 presents standards for systems confidentiality.

TABLE 3.10-17 Systems confidentiality standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	NIST	Computer Security Guidelines for Implementing the Privacy Act of 1974	FIPS PUB 41:1975	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 5: Confidentiality	10181-5	Informational (Draft)

3.10.6.1.2 Alternative specifications. There are no alternative specifications.

3.10.6.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.6.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.6.1.5 Related standards. DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information. DDS-2600-6243-92, Compartmented Mode Workstation Evaluation Criteria, Version 1 (final), defines minimum security requirements for workstations to be accredited in the Compartmented Mode under the policy set forth in DCID 1/16. Public Law (PL) 93-579, Privacy Act of 1974, and PL 100-235, Computer Security Act of 1987, contain confidentiality requirements. FIPS PUB 41 provides guidance for conformance with PL 93-579.

3.10.6.1.6 Recommendations. The mandated standard is recommended. The DGSA, Volume 6 of the TAFIM, provides security principles and target security capabilities to guide system security architects in creating specific security architectures consistent with the DGSA. The

DGSA should be used by system security architects to develop logical and specific security architectures.

3.10.6.2 Registration of cryptographic techniques. (This BSA appears in part 9 and part 10.) These standards provide procedures for the registration of cryptographic algorithms in a standard format with a registration authority. The need for these registration services is determined by the security architecture of the system in question. These are not implementable specifications and no conformance test is required.

3.10.6.2.1 Standards. Table 3.10-18 presents standards for registration of cryptographic techniques.

TABLE 3.10-18 Registration of cryptographic techniques standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Procedures for the Registration of Cryptographic Algorithms	9979:1991	Informational (Approved)

3.10.6.2.2 Alternative specifications. No [illegible] de facto specifications are available.

3.10.6.2.3 Standards deficiencies. Deficiencies in the [illegible] standards are unknown.

3.10.6.2.4 Portability caveats. Portability problems [illegible] the existing specifications are unknown.

3.10.6.2.5 Related standards. No standards are related to registration of cryptographic techniques.

3.10.6.2.6 Recommendations. Procurements requiring that all cryptographic algorithms offered are registered with a registration authority in a standard format should specify conformance with ISO 9979. The NIST document, NISTIR 5308, "General Procedures for Registering Computer Security Objects," December 1993, describes the object-independent procedures for operating the Computer Security Objects Register (CSOR) established by NIST. Initially, the only family of objects registered in the CSOR is network security labels; however, plans include adding cryptographic algorithm modes of operation to the CSOR.

3.10.6.3 Data encryption security. (This BSA appears in part 5, part 7, part 10, and part 11.) Encryption is the cryptographic transformation of data to produce cipher text. Standards for data encryption security services describe services such as definitions/algorithms, modes of operation, and guidelines for use for those systems that require their data to be encrypted using data encryption security services. None of these standards are for systems processing classified information.

3.10.6.3.1 Standards. Table 3.10-19 presents standards for data encryption security.

TABLE 3.10-19 Data encryption security standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Escrowed Encryption Standard (EES)	FIPS PUB 185: 1994	Mandated (Approved)
GPC	NIST	Data Encryption Standard (DES) (related to ANSI X3.92-1981/R1987/R1993)	FIPS PUB 46-2:1993 (Reaffirmed until 1998)	Informational (Approved)
GPC	NIST	Guidelines for Implementation and using the NBS Data Encryption Standard	FIPS PUB 74:1981	Informational (Approved)
GPC	NIST	Data Encryption Standard (DES) Modes of Operation (related to ANSI X3.106-1983)	FIPS PUB 81:1980	Informational (Approved)
GPC	NIST	Security Requirements for Cryptographic Modules	FIPS PUB 140-1:1994	Informational (Approved)
IPC	ISO	Modes of Operation for a 64-Bit Block Cipher Algorithm (Related to ANSI X3.106)	8372:1987	Informational (Approved)
NPC	ANSI	Data Encryption Algorithm	X3. 92-1981 (R1993)	Informational (Approved)
NPC	ANSI	Digital Encryption Algorithm - Modes of Operation	X3.106-1983 (R1990)	Informational (Approved)
GPC	NIST	Advanced Encryption Standard	FIPS PUB JJJ	Informational (Formative)

3.10.6.3.2 Alternative specifications. The only other available specifications are proprietary, for example, RSA.

3.10.6.3.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.6.3.4 Portability caveats. DES applications are not interoperable with non-DES systems. Portability problems related to EES are unknown. The U.S. controls export of cryptographic technologies, products, and related technologies as munitions. On October 1, 1996, a new federal policy allowing U.S. vendors to export products using up to 56-bit encryption, provided the vendors sign an agreement to make their 56-bit encryption technologies key-recovery-compliant within 24 months.

3.10.6.3.5 Related standards. FIPS PUB 113, Computer Data Authentication, is related to DES security mechanisms and their standards.

3.10.6.3.6 Recommendations. The mandated standard is recommended. FIPS PUB 185, EES, supports lawful authorized access to the keys required to decipher enciphered information for systems requiring strong encryption protection of sensitive but unclassified information. EES provides stronger protection than DES against unauthorized access. Devices conforming to EES may be used when replacing Type II and Type III (DES) encryption devices owned by the Government. Implementations requiring use of EES should require conformance with FIPS PUB 140-1.

On 2 January 1997, NIST announced plans to develop a FIPS, Advanced Encryption Standard, incorporating an advanced encryption algorithm to replace DES (FIPS PUB 46-2).

3.10.6.4 Traffic flow confidentiality. (This BSA appears in part 7 and part 10.) Traffic flow confidentiality is a service to protect against unauthorized traffic analysis (ISO 7498-2) by concealing presence, absence, amount, direction, and frequency of traffic.

3.10.6.4.1 Standards. Table 3.10-20 presents standards for traffic flow confidentiality.

TABLE 3.10-20 Traffic flow confidentiality standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 3 (SP3)	SDN.301, Revision 1.5: 1989	Informational (Approved)
IPC	ISO	Network Layer Security Protocol (NLSP)	11577:1994	Informational (Approved)
IPC	ISO	OSI Distributed Transaction Processing (DTP) - Draft Amendments to Parts 1 to 3: Transaction Processing Security	WDAMs (SC21 N 5232 to ISO 10026-1,2,3) 1991	Informational (Draft)

3.10.6.4.2 Alternative specifications. There are no alternative specifications.

3.10.6.4.3 Standards deficiencies. There are no mandated standards for traffic flow confidentiality.

3.10.6.4.4 Portability caveats. Work on proposed amendments to ISO 10026 has ceased. This is a high portability risk area, because no standards exist.

3.10.6.4.5 Related standards. There are no related standards.

3.10.6.4.6 Recommendations. No standards are recommended.

SP3 is the basis for ISO 11577.

3.10.7 Integrity. Integrity includes systems integrity, data integrity techniques, and network integrity.

3.10.7.1 Systems integrity. (This BSA appears in part 4 and part 10.) Systems integrity objectives ensure the integrity of information and resources by providing a level of protection in response to the threats of unauthorized modification, manipulation, and destruction which is commensurate with the importance and priority of the content. These standards provide the high-level framework with which to view the security service of integrity in open systems.

3.10.7.1.1 Standards. Table 3.10-21 presents standards for systems integrity.

TABLE 3.10-21 Systems integrity standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 6: Integrity (same as ITU-TS X.815)	10181-6	Informational (Draft)
IPC	ITU-T	Security Frameworks in Open Systems: Integrity Framework (same as ISO 10181-6)	X.815: 1993	Informational (Draft)

3.10.7.1.2 Alternative specifications. There are no alternative specifications.

3.10.7.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.7.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.7.1.5 Related standards. The following NSA documents supplement the information on integrity found in the TCSEC:

a. C Technical Report 79-91, September 1991, "Integrity in Automated Information Systems:

b. C Technical Report 111-91, October 1991, "Integrity-Oriented Control Objectives: Proposed Revisions to the Trusted Computer System Evaluation (TCSEC), DOD 5200.28-STD."

3.10.7.1.6 Recommendations. The mandated standards are recommended.

3.10.7.2 Data integrity techniques. (This BSA appears in part 4 and part 10.) Data integrity techniques provide services that allow data integrity between communicating applications to be confirmed by means of a cryptographic check function using a block cipher algorithm, by electronic signature, electronic hashing, and encryption.

3.10.7.2.1 Standards. Table 3.10-22 presents standards for data integrity techniques.

TABLE 3.10-22 Data integrity techniques standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180-1:1995	Mandated (Approved)
GPC	NIST	Digital Signature Standard (DSS)	FIPS PUB 186:1994	Mandated (Approved)
IPC	ISO	Data Cryptographic Techniques - Data Integrity Mechanism Using a Cryptographic Check Function Employing a Block Cipher Algorithm	9797:1989	Informational (Approved)
CPC	IETF	IP Authentication Header (AH)	RFC 1826: 1995	Emerging (Draft)
CPC	IETF	IP Encapsulating Security Payload (ESP)	RFC 1827: 1995	Emerging (Draft)
CPC	IETF	Domain Name System (DNS) Security Extensions	RFC 2065:1997	Emerging (Draft)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180:1993	Informational (Superseded)

3.10.7.2.2 Alternative specifications. Alternative de facto specifications include RSA and MD-5.

3.10.7.2.3 Standards deficiencies. Deficiencies in the existing specifications are unknown.

3.10.7.2.4 Portability caveats. Portability problems with the existing specifications are unknown.

3.10.7.2.5 Related standards. There are no related standards.

3.10.7.2.6 Recommendations. The mandated standards re recommended.

FIPS PUB 180-1, which supersedes FIPS PUB 180, specifies a Secure Hash Algorithm (SHA-1) which can be used to generate a message digest. The SHA-1 is required for use with the Digital Signature Algorithm (DSA) as specified in FIPS PUB 186 and whenever an SHA is required in federal applications.

3.10.7.3 Network integrity. (This BSA appears in part 7 and part 10.) Network integrity ensures that data is not altered or destroyed in an unauthorized manner when transmitted across a network.

3.10.7.3.1 Standards. Table 3.10-23 presents standards for network integrity.

TABLE 3.10-23 Network integrity standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Information Technology - Defense Standardized Profiles AMHXn(D)- Message Handling Systems - Message Security Protocol (MSP) Parts 1-5	MIL-STD-2045-18500: 1993	Mandated (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 3 (SP3)	SDN.301, Revision 1.5: 1989	Mandated (Approved)
NPC	IEEE	Standard for Interoperable LAN Security - Part B: Secure Data Exchange (SDE)	802.10b:1992	Legacy (Approved)
IPC	ISO	Transport Layer Security Protocol (TLSP) (Includes Amendment 1)	10736:1994	Informational (Approved)
IPC	ISO	Network Layer Security Protocol (NLSP)	11577:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 4: Protecting Transfer Syntax Specification	11586-4:1994	Informational (Approved)
GPC	NSA	Secure Data Network System (SDNS) Security Protocol 4 (SP4)	SDN.401, Rev. 1.3:1989	Informational (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, v. 4.0, Rev. A: 1997	Emerging (Approved)

3.10.7.3.2 Alternative specifications. There are no alternative specifications.

3.10.7.3.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.10.7.3.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.10.7.3.5 Related standards. ITU-T X.500 (1993) (same as ISO 9594-1), Information Technology - Open Systems Interconnection - The Directory - Overview of Concepts, Models and Services, is a related standard.

3.10.7.3.6 Recommendations. The mandated standards are recommended.

MIL-STD-2045-18500 describes the security provided by MSP. It should be used for DOD message systems that are required to exchange classified and sensitive but unclassified information. It is based on Version 3.0 of the MSP documented in SDN.701, Secure Data Network System (SDNS) Message Security Protocol," Revision 1.5, 1 August 1989. MSP is

under revision to Version 4.0 to accommodate, in part, Allied requirements. This DSP standard will be replaced by a portion of the U.S. Supplement to ACP 123 or ACP 120, Common Security Protocol, when the revision to MSP is complete.

SP3 provides connectionless security services and is the basis for ISO 11577. SP3 is designed to be used at the top of layer 3.

SP4 is the basis for ISO 10736.

IEEE 802.10b is for use with legacy LANs only.

3.10.8 Non-repudiation. Non-repudiation base service areas include systems non-repudiation, electronic signature, and electronic hashing. Non-repudiation services ensure that senders and recipients cannot deny the origin or delivery of data. Non-repudiation mechanisms can be used to validate the source of software packages or verifying that hardware is unchanged from its manufactured state.

3.10.8.1 Systems non-repudiation. (This BSA appears in part 5, part 7, part 10, and part 11.) These standards provide the security services for non-repudiation in systems.

3.10.8.1.1 Standards. Table 3.10-24 presents standards for systems non-repudiation.

TABLE 3.10-24 Systems non-repudiation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Digital Signature Standard (DSS)	FIPS PUB 186:1994	Mandated (Approved)
GPC	DOD	Information Technology - Defense Standardized Profiles AMHXn(D)- Message Handling Systems - Message Security Protocol (MSP) Parts 1-5	MIL-STD-2045-18500: 1993	Mandated (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, Rev. 3.0: 1994	Legacy (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, v. 4.0, Rev. A: 1997	Emerging (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 4: Protecting Transfer Syntax Specification	11586-4:1994	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
CPC	IETF	IP Authentication Header (AH)	RFC 1826: 1995	Emerging (Draft)
CPC	OMG	Common Object Request Broker Architecture (CORBA) Security	OMG 95-12-1: 1995	Emerging (Draft)
CPC	IETF	S/MIME Message Specification: PKCS Security Services for MIME	draft-dusse-mime-msg-spec-00.txt, September 1996	Informational (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 4: Non-Repudiation (same as ITU-TS X.813)	10181-4	Informational (Draft)
IPC	ISO	Non-Repudiation Mechanisms Part 1: General Model	13888-1:1992 (SC27 N868 (Project 1.27.06.01))	Informational (Draft)
IPC	ISO	Non-Repudiation Mechanisms Part 2: Using Symmetric Encipherment Algorithms	13888-2:1994 (SC27 N864 (Project 1.27.06.02))	Informational (Draft)
IPC	ISO	Non-Repudiation Mechanisms Part 3: Using Asymmetric Techniques	13888-3:1992 (SC27 N869 (Project 1.27.06.03))	Informational (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	OSI Distributed Transaction Processing (DTP) - Draft Amendments to Parts 1 to 3: Transaction Processing Security	WDAMs (SC21 N 5232 to ISO 10026-1,2,3) 1991	Informational (Draft)

3.10.8.1.2 Alternative specifications. There are no alternative specifications.

3.10.8.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.8.1.4 Portability caveats. Portability problems in the existing standards are unknown.

3.10.8.1.5 Related standards. FIPS PUB 180-1, Secure Hash Standard, must be used with FIPS PUB 186. FIPS PUB 180-1 provides the Secure Hash Algorithm used in generating and verifying electronic signatures.

3.10.8.1.6 Recommendations. The mandated standards are recommended for non-repudiation.

MIL-STD-2045-18500 describes the security provided by MSP. It should be used for DOD message systems that are required to exchange classified and sensitive but unclassified information. It is based on Version 3.0 of the MSP documented in SDN.701, "Secure Data Network System (SDNS) Message Security Protocol," Revision 1.5, 1 August 1989. MSP is under revision to Version 4.0 to accommodate, in part, Allied requirements. This DSP standard will be replaced by a portion of the U.S. Supplement to ACP 123 or ACP 120, Common Security Protocol, when the revision to MSP is complete.

MSP provides for signed receipts. S/MIME, an Internet Draft specification, does not provide for signed receipts.

3.10.8.2 Electronic signature. (This BSA appears in part 5, part 7, and part 10.) Electronic signature is the process that operates on a message to ensure message source authenticity and integrity, and source non-repudiation. Electronic signatures are composed so that the identity of a signatory and integrity of the data can be verified.

3.10.8.2.1 Standards. Table 3.10-25 presents standards for electronic signature.

TABLE 3.10-25 Electronic signature standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Digital Signature Standard (DSS)	FIPS PUB 186:1994	Mandated (Approved)
IPC	ISO	Digital Signature Scheme Giving Message Recovery	9796:1991	Informational (Approved)
CPC	IETF	Privacy Enhancement for Internet Electronic Mail	RFC 1421-1424:1993	Informational (Draft)
IPC	ISO	Digital Signature with Appendix - Part 1: General	SC27/WG2 N294 (Project 1.27.08.01)	Informational (Formative)
IPC	ISO	Digital Signature with Appendix - Part 2: Identity-Based Mechanisms	SC27/WG2 N295 (Project 1.27.08.02)	Informational (Formative)
IPC	ISO	Digital Signature with Appendix - Part 3: Certificate-Based Mechanisms	SC27/WG2 N296 (Project 1.27.08.03)	Informational (Formative)

3.10.8.2.2 Alternative specifications. Rivest-Shamir-Adelman (RSA) Public Key Algorithm RC-5 was developed and published in 1994. It is proprietary, but RSA Data Security is working to have it included in numerous Internet standards. At present, RC-5 is not recommended for DOD use because it is proprietary.

3.10.8.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.8.2.4 Portability caveats. DSS applications are not interoperable with non-DSS systems.

3.10.8.2.5 Related standards. FIPS PUB 180-1, Secure Hash Standard, must be used with FIPS PUB 186. FIPS PUB 180-1 provides the Secure Hash Algorithm used in generating and verifying electronic signatures.

3.10.8.2.6 Recommendations. The mandated standard is recommended. FIPS PUB 186 is implemented in the FORTEZZA cryptographic card, a PC card (formerly called a Personal Computer Memory Card International Association (PCMCIA) standard card) that can be integrated into personal computers and workstations to provide security in commercial applications. FORTEZZA is being used in the Defense Message System. FIPS PUB 186 is the government-wide key cryptographic signature system.

3.10.8.3 Electronic hashing. (This BSA appears in part 5, part 7, part 8, and part 10.) Electronic hashing services compute a condensed representation of a message or a data file, often used as a measure of data integrity checking.

3.10.8.3.1 Standards. Table 3.10-26 presents standards for electronic hashing.

TABLE 3.10-26 Electronic hashing standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180-1:1995	Mandated (Approved)
IPC	ISO	Hash Functions, Part 1: General Model	10118-1:1994	Informational (Approved)
IPC	ISO	Hash Functions, Part 2: Hash Functions Using an N-Bit Block Cipher Algorithm	10118-2:1994	Informational (Approved)
GPC	NIST	Secure Hash Standard (SHS)	FIPS PUB 180:1993	Informational (Superseded)
IPC	ISO	Hash Functions, Part 3: Dedicated Hash Functions	WD 10118-3, JTC1/SC27 N883 (Project 1.27.09.03)	Informational (Draft)
IPC	ISO	Hash Functions, Part 4: Hash Functions Using Modular Arithmetic	WD 10118-4, JTC1/SC27 N884 (Project 1.27.09.04)	Informational (Draft)

3.10.8.3.2 Alternative specifications. There are no alternative specifications.

3.10.8.3.3 Standards deficiencies. Deficiencies in the existing specifications are unknown.

3.10.8.3.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.8.3.5 Related standards. FIPS PUB 180-1 supersedes FIPS PUB 180 and is required for use with FIPS PUB 186, Digital Signature Standard.

3.10.8.3.6 Recommendations. The mandated standard is recommended. FIPS PUB 180-1 specifies SHA, which can be used to generate a message digest. SHA is required for use with the DSA as specified in FIPS PUB 186 and whenever an SHA is required for federal applications.

3.10.9 Systems availability. System availability objectives ensure service availability consistent with the operational importance of the information or valued assets.

3.10.9.1 Detection and notification. (This BSA appears in part 2, part 9, and part 10.) Detection and notification objectives ensure that a secure system has the capability to recognize that it is: under attack; may potentially enter a non-available state; has been compromised; or has failed in a potentially compromising manner. Guidance in this area focuses on reporting detected security critical conditions to proper authorities, and implementing predetermined corrective actions.

3.10.9.1.1 Standards. Table 3.10-27 presents standards for detection and notification.

TABLE 3.10-27 Detection and notification standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)

3.10.9.1.2 Alternative specifications. There are no alternative specifications.

3.10.9.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.9.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.9.1.5 Related standards. NSA's C-Technical Report-001, Computer Viruses: Prevention, Detection, and Treatment, and NIST SP 800-5, A Guide to the Selection of Anti-Virus Tools and Techniques, provide guidance on computer viruses. The following specifications support the TCSEC standard:

a. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation

b. NCSC-TG-015, Version 1, October 1989, A Guide to Understanding Trusted Facility Management

c. NCSC-TG-016, Version 1, October 1992, Guidelines for Writing Trusted Facility Manuals

3.10.9.1.6 Recommendations. The mandated standard is recommended.

3.10.9.2 Security recovery. (This BSA appears in part 2, part 9, and part 10.) Recovery guidance defines provisions to allow system personnel or processes with the proper authorizations to repair or eliminate the cause of security relevant failures, isolate compromised portions of the system, and revalidate proper operations prior to returning the system to a fully operational secure state.

3.10.9.2.1 Standards. Table 3.10-28 presents standards for security recovery.

TABLE 3.10-28 Security recovery standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)

3.10.9.2.2 Alternative specifications. There are no alternative specifications.

3.10.9.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.9.2.4 Portability caveats. Portability problems in the existing standards are unknown.

3.10.9.2.5 Related standards. The following specifications are related to the TCSEC standard:

a. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation

b. NCSC-TG-022, Version 1, December 1991, A Guide to Understanding Trusted Recovery in Trusted Systems

c. NCSC-TG-015, Version 1, October 1989, A Guide to Understanding Trusted Facility Management

d. NCSC-TG-016, Version 1, October 1992, Guidelines for Writing Trusted Facility Manuals

3.10.9.2.6 Recommendations. The mandated standard is recommended.

3.10.10 Security labeling. Security labeling is the data bound to a resource (which may be a data unit) that names or designates the security attributes of that resource. Security labeling includes security labeling for the following major service areas: user interface, data management, data interchange, graphics, network (data communications), system, and distributed computing.

3.10.10.1 User interface security labeling. (This BSA appears in part 3 and part 10.) User interface security labeling provides a human readable representation of the internal security labels associated with data management, data interchange, graphics, data communications, system, and distributed computing services.

3.10.10.1.1 Standards. Table 3.10-29 presents standards for user interface security labeling.

TABLE 3.10-29 User interface security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Adopted (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	Defense Intelligence Agency Standard User Interface Style Guide for Compartmented Mode Workstations	DIA Style Guide: 1983	Informational (Approved)

3.10.10.1.2 Alternative specifications. There are no alternative specifications.

3.10.10.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.10.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.10.1.5 Related standards. DOD 5200.28-STD is a related standard. DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

Security-related interface requirements for workstations operating in System High or Compartmented Mode are discussed in DDS-2600-6243-91 and the DIA Style Guide, which provide the basis for the security portion of the HCI Style Guide (TAFIM Volume 8).

3.10.10.1.6 Recommendations. Appendix A of the TAFIM, Volume 8, DOD HCI Style Guide, outlines security presentation guidelines for workstations and is recommended.

3.10.10.2 Data management security labeling. (This BSA appears in part 4 and part 10.) Data management security labeling provides a security service for ensuring that data includes labeling information in support of mandatory access control security services, marking security services, handling security services, aggregation security services, sanitization security services, and release security services. Security labeling services produce and maintain the integrity of the security label and its binding to the data with which it is associated.

3.10.10.2.1 Standards. Table 3.10-30 presents standards for data management security labeling.

TABLE 3.10-30 Data management security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Informational (Approved)

3.10.10.2.2 Alternative specifications. There are no alternative standards.

3.10.10.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.10.2.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.10.2.5 Related standards. Data management security labeling should be compatible with MIL-STD-2045-48501, Common Security Label, for any system with a communications interface.

DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

3.10.10.2.6 Recommendations. The mandated standard is recommended. Data management security labeling should be based of the operating system security label standards. Data management security labeling should employ binding of strength equal to or greater than that of the operating system. Compatible security labeling standards include the ability to perform a one-for-one mapping or translation between security labeling standards.

3.10.10.3 Data interchange security labeling. (This BSA appears in part 5 and part 10.) Data interchange security labeling provides a security service to define the format and correctly parse a security label into the security attributes used by other security services.

3.10.10.3.1 Standards. Table 3.10-31 presents standards for data interchange security labeling.

TABLE 3.10-31 Data interchange security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Common Security Label (CSL)	MIL-STD-2045-48501: 1995	Mandated (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Informational (Approved)
GPC	NIST	Standard Security Label (SSL) for Information Transfer	FIPS PUB 188:1994	Informational (Approved)
IPC	ITU-T	Message Handling Systems: Message Transfer System: Abstract Service Definition and Procedures	X.411: 1992	Informational (Approved)
CPC	TSIG	Trusted Security Information Exchange for Restricted Environments	TSIX (RE) 1.1	Emerging (Draft)

3.10.10.3.2 Alternative specifications. There are no alternative specifications.

3.10.10.3.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.10.3.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.10.3.5 Related standards. DOD 5200.28-STD is a related standard.

DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

3.10.10.3.6 Recommendations. The mandated standard is recommended. TSIG TSIX(RE) 1.1 includes options compatible with MIL-STD-2045-48501.

3.10.10.4 Graphics security labeling. (This BSA appears in part 6 and part 10.) Graphics security labeling provides a security service for ensuring that graphical data includes labeling information in support of mandatory access control security services, marking security services, handling security services, aggregation security services, sanitization security services, and release security services. Security labeling services produce and maintain the integrity of the security label and its binding to the data with which it is associated.

3.10.10.4.1 Standards. Table 3.10-32 presents standards for graphics security labeling.

TABLE 3.10-32 Graphics security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Informational (Approved)

3.10.10.4.2 Alternative specifications. There are no other specifications.

3.10.10.4.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.10.4.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.10.4.5 Related standards. Graphics security labeling should be compatible with MIL-STD-2045-48501, Common Security Label, for any system with a communications interface.

DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

3.10.10.4.6 Recommendations. The mandated standard is recommended. Graphics security labeling should be based on the operating system security label standards. Graphics security labeling should employ binding of strength equal to or greater than that of the operating system. Compatible security labeling standards include the ability to perform a one-for-one mapping or translation between security labeling standards.

3.10.10.5 Data communications security labeling. (This BSA appears in part 7 and part 10.) Data communications security labeling encompasses the application of security labeling, which is used as the basis for mandatory access control security services and release security services.

3.10.10.5.1 Standards. Table 3.10-33 presents standards for data communications security labeling.

TABLE 3.10-33 Data communications security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Common Security Label (CSL)	MIL-STD-2045-48501: 1995	Mandated (Approved)
IPC	ISO	Transport Layer Security Protocol (TLSP) (Includes Amendment 1)	10736:1994	Informational (Approved)
IPC	ISO	Network Layer Security Protocol (NLSP)	11577:1994	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Informational (Approved)
GPC	NIST	Standard Security Label (SSL) for Information Transfer	FIPS PUB 188:1994	Informational (Approved)
CPC	IETF	DoD Security Options for the Internet Protocol	RFC 1108:1991	Legacy (Draft)
CPC	IETF	Revised Internet Protocol Security Options (RIPSO)	RFC 1038:1988	Informational (Draft)
CPC	TSIG	Trusted Security Information Exchange for Restricted Environments	TSIX (RE) 1.1	Emerging (Draft)
NPC	IEEE	Standard for Interoperable LAN Security-Part G: Standard for Security Labeling within Secure Data Exchange	802.10g/D7	Emerging (Draft)

3.10.10.5.2 Alternative specifications. There are no alternative specifications.

3.10.10.5.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.10.5.4 Portability caveats. Portability problems related to the existing standards are unknown.

3.10.10.5.5 Related standards. DOD 5200.28-STD is a related standard. DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for

safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

3.10.10.5.6 Recommendations. The mandated standard is recommended and should be used for new acquisitions. MIL-STD-2045-48501 supports the exchange of security attributes, for example, sensitivity labels. It provides a means to label and protect data as it passes through communications systems and implements FIPS PUB 188 for the DOD environment. MIL-STD-2045-48501 and FIPS PUB 188 apply only to layers 3 and 4. TSIG TSIX(RE) 1.1, "Trusted Systems Interoperability Group, Trusted Security Information Exchange for Restricted Environments," includes options compatible with MIL-STD-2045-48501.

IEEE 802.10g is consistent with the SSL and the CSL.

RFC 1108 makes RFC 1038 obsolete. RFC 1108 should be used for legacy systems only. RFC 1038 is not recommended.

3.10.10.6 Operating system security labeling. (The BSA appears in part 8 and part 10.) Operating system security labeling provides a security labeling service in support of end system processing. This service is required to support similar or shared service for all other MSAs having security labels. This service includes any translation services to support other MSAs, achieve host system independence, or protect host identity.

3.10.10.6.1 Standards. Table 3.10-34 presents standards for operating system security labeling.

TABLE 3.10-34 Operating system security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Informational (Approved)
NPC	IEEE	Standard for Interoperable LAN Security-Part G: Standard for Security Labeling within Secure Data Exchange	802.10g/D7	Emerging (Draft)

3.10.10.6.2 Alternative specifications. There are no alternative specifications.

3.10.10.6.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.10.10.6.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.10.6.5 Related standards. DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

3.10.10.6.6 Recommendations. The mandated standard is recommended.

3.10.10.7 Distributed computing security labeling. (This BSA appears both in part 10 and part 11.) Distributed computing security labeling provides a security labeling service to support mandatory access controls within a distributed environment.

3.10.10.7.1 Standards. Table 3.10-35 presents standards for distributed computing security labeling.

TABLE 3.10-35 Distributed computing security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Pvt 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)

3.10.10.7.2 Alternative specifications. There are no alternative specifications.

3.10.10.7.3 Standards deficiencies. The subjects and objects requiring security labeling in a distributed computing environment have not been standardized or identified in any standardized framework.

3.10.10.7.4 Portability caveats. Portability problems with the existing standards are unknown.

3.10.10.7.5 Related standards. DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

3.10.10.7.6 Recommendations. The mandated standards are recommended.

The DGSA (TAFIM Volume 6) provides general architectural guidance for information domains which can exist in a distributed environment. The properties of information domains share some similarities with security labels in a distributed environment.

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 11 of 14 parts)

DISTRIBUTED COMPUTING SERVICES

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

TABLE OF CONTENTS

LIST OF TABLES

3.11 Distributed computing. Distributed computing provides services and tools that support the creation, use, and maintenance of distributed applications in a heterogeneous computing environment. This includes specialized support for applications that may be physically or logically dispersed among computer systems in a heterogeneous network, but yet wish to maintain a cooperative processing environment. The classical definition of a computer becomes blurred as the processes that contribute to information processing become distributed across a facility or a network. As with other cross-cutting services the requisite components of distributed computing services typically exist within particular service areas. They are described in subsequent paragraphs but include global time, data, file, name, remote procedure call, security and threads. NOTE: throughout Part 11, all tables shall have abbreviations listed under the column (Standard Type) as follows:

a. National Public Consensus=NPC
b. International Public Consensus=IPC
c. Government Public Consensus=GPC
d. Consortia Public Consensus=CPC
e. Consortia Private Non-Concensus=CPN-C
f. National Public Non-Consensus=NPN-C

3.11.1 Introduction and overview of distributed computing (general discussion). Distributed computing services allow users and application developers to maximize the computing power found in today's networks by transparently assigning tasks to the most appropriate processors. The software in distributed computing systems will mask the specific data formats of each machine and allow access to all applications from any platform on the network. (Air Force Technical Reference Code)

3.11.2 Client/Server. Architecture in which the client (personal computer or workstation) is the requesting machine and the server is the supplying machine (LAN file server, mini, or mainframe). The client provides the user interface and performs some or all of the application processing. The server maintains the database and processes requests from the client to extract data from or update the database. The server also controls the application's integrity and security.

Distributed client/server systems allow applications to interoperate on a variety of platforms regardless of the manufacturer of the underlying hardware, operating system, or networking software. They include such services as: remote procedure call which lets applications, or portions of applications, call for a procedure from a remote system; naming services which let users access network services by name without the necessity of knowing where the resource is located; and timing services which regulate system clocks on each network computer so that they match each other.

3.11.2.1 Threads. (This BSA appears in both part 8 and part 11.) A traditional UNIX process has a single thread of control. A thread of control, or more simply a thread, is a sequence of instructions executed in a program. A thread has a program counter (PC) and a stack to keep track of local variables and return addresses. A thread is one transaction or message in a

multithreaded system or an individual process within a single application. Thread interfaces are specifications for interfacing with these processes.

Thread services provide an underlying service for multiple concurrent executions within a single computer process. They are designed to allow independent operation and are essential for functions such as multiple process communications in a distributed computing environment. Threads provide improved software responsiveness through increased use of the inherent synchronous execution (i.e., parallelism) of programs. The threads service in DCE allows all DCE-enabled applications to execute multiple actions simultaneously. Applications can accept information from users, execute RPCs, and access databases at the same time. The threads service is used by several DCE services, including the RPC, Security, Directory, and Time Services. The OSF has designed the threads service to be easily accessible by programmers wishing to use it in applications. Services can be accessed through the C programming language, and through other high-level programming languages.

3.11.2.1.1 Standards. Table 3.11-1 presents standards for threads.

TABLE 3.11-1 Threads standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Portable Operating System Interface (POSIX) Part 1: System API (Replaces ISO 9945-1:1990 and incorporates IEEE 1003.1b, 1003.1c, and 1003.1i)	9945-1:1996	Mandated (Approved)
CPN-C	Microsoft	Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers' Reference Manual, 1993, Microsoft Press	Win32 APIs	Mandated (Approved)
NPC	IEEE	POSIX Part 1: System Application Program Interface (API) Amendment 2: Threads Extension [C Language]	1003.1c:1995	Informational (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Threads (based on the draft 4 version of IEEE 1003.1c.)	DCE 1.1 Threads:1994	Informational (Approved)
NPC	IEEE	POSIX-Part 1: System API - Amend. n: Technical Corrigenda to Threads API Extensions (C Language)	P1003.1n	Emerging (Formative)
CPC	X/Open	Aspen Threads Extension	Aspen Threads	Informational (Formative)

3.11.2.1.2 Alternative specification. The OSF/1 Operating System's Mach-Based Multithreaded Kernel is also available.

3.11.2.1.3 Standard deficiencies. Because the Pthreads interface is not designed specifically for Ada, it can impose a great overhead burden on an Ada run-time system. The Ada rendezvous feature is not supported by Pthreads, which is a major problem for real time applications.

OSF DCE Threads are incompatible with Ada Tasking. Programmers can use one or the other, but not both. Since DCE Threads underlie OSF RPC, Ada programmers should be cautious in the use of tasking. (Reference: Understanding DCE by Rosenberry, Kenney, and Fisher)

3.11.2.1.4 Portability caveats. Ada83 and, to an even greater extent, Ada9x already contain many of the capabilities defined in the 1003.1c standard. This can cause many conflicts with Ada. Vendors may implement Ada tasks in a way that interferes with the implementation of Pthreads. Also, if the Ada vendor does not implement tasks as Pthreads, conflicts may arise between what Ada can and cannot do and what Pthreads can do. For example, the Ada rendezvous feature is not supported by Pthreads. On the other hand, Pthreads provides some extended features, such as dynamic priorities, that have not been standardized by the Ada language, but that are in demand, especially by real time users.

3.11.2.1.5 Related standards. The following standards are related to threads services:

a. IEEE P1003.1e: Security Interface Standards for POSIX.

b. IEEE P1003.21: POSIX - Real Time Distributed Systems Communication.

c. NIST FIPS 151-2:1993, Portable Operating System Interface (POSIX)-System Application Program Interface [C Language] (ISO/IEC 9945-1:1990) 1993.

3.11.2.1.6 Recommendations. The mandated standards are recommended. The operating system standards mandated by the JTA Version 1.0:1996 (ISO/IEC 9945-1:1990, IEEE 1003.1b:1993, IEEE 1003.1c:1995, and IEEE 1003.1i:1995) are all incorporated in the new ISO/IEC 9945-1:1996. The OSF DCE threads is based on a draft version of IEEE P1003.1c Pthreads. OSF intends to move to the new IEEE 1003.1c standard in a future version of DCE. In the meantime, DCE users should specify DCE threads to ensure compatibility with currently available DCE products. However, they should also specify that these products will be able to migrate to the new version of DCE when OSF adopts the approved 1003.1c standard.

To the extent an Ada runtime system uses standard POSIX interfaces, it will be portable across operating systems compliant with POSIX. Some of the problems caused by Ada operations not currently mapped to Pthreads will be resolved by the Ada binding to the 1003.1c Pthreads standard.

3.11.2.2 Remote procedure call. (This BSA appears in part 8 and part 11.) Remote procedure call (RPC) is a communication service to transfer procedure calls to a remote server and return results, errors, or associated call backs (ECMA 127). The RPC extends the local procedure call to a distributed environment. In a RPC, a process can invoke a remote procedure as if it were invoking a local procedure. SC21/WG6 proposes to address RPC using Interface Definition Notation (IDN) that is based on abstract data types rather than on a union of programming language-specific data types.

3.11.2.2.1 Standards. Table 3.11-2 presents standards for remote procedure call.

TABLE 3.11-2 Remote procedure call standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Remote Procedure Call (RPC)	DCE 1.1 RPC:1994	Mandated (Approved)
CPC	X/Open	X/Open DCE: Remote Procedure Call	C309 (8/94)	Informational (Approved)
CPC	IETF	Open Network Computing (SUN ONC) Remote Procedure Call (RPC)	RFC 1057:1988	Informational (Approved)
IPC	ISO	OSI Remote Procedure Call (RPC) (Replaces DIS 11578 PT 1 Thru PT 4)	11578.2	Informational (Draft)
NPC	IEEE	POSIX - Part 1: Protocol Independent Interfaces	P1003.1g	Emerging (Draft)
NPC	IEEE	POSIX - Part 1: System API Amendment: Real-Time Distributed Systems Communications	P1003.21	Emerging (Draft)

3.11.2.2.2 Alternative specifications. There are no alternative specifications.

3.11.2.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.11.2.2.4 Portability caveats. All the indicated RPCs are unique. They do not interoperate. Systems using different RPCs are not interoperable, nor are their applications portable across different RPCs. No RPC conformance tests are available.

3.11.2.2.5 Related standards. The following standards are related to RPC:

a. Common Language Independent Data Types (CLID) (ISO 11404).

b. Common Language Independent Procedure Call Mechanism (CLIP or CLIPCM). SC22/WG11 has recommended that there should be a cross reference between the standards.

c. NIST FIPS 146-1:1991: Government Open Systems Interconnection Profile (GOSIP), ISO 8822, ISO 8823 (SIA-5.8) Presentation (Layer 6), Session (Layer 5) ISO 8327 (SIA-5.9).

d. NIST FIPS 146-2 POSIT: May 1995.

3.11.2.2.6 Recommendations. The Open Software Foundation (OSF) Distributed Computing Environment (DCE) is recommended. A migration path to the ISO RPC also should be required as soon as that standard is in final form.

The IEEE P1003.21 draft standard includes interfaces for the support of request/response services.

3.11.2.3 Distributed timing service. (This BSA appears in part 8 and part 11.) Distributed timing service (DTS) guarantees synchronization among all system clocks in a distributed network. Synchronized timing is necessary to maintain scheduling of activities and sequencing of events. DTS uses RPC in the communications between DTS clients and DTS servers. It also uses RPC in the protocol between a Time Server and a Time Provider. Since DTS is based on DCE RPC, which uses DCE Threads, DTS also uses Threads. DTS depends on CDS to find Time Servers and their locations. GDS may be used indirectly if a Global Time Server is registered in a foreign cell registered in the X.500 namespace. DTS uses the DCE Security Service to authenticate its interactions.

3.11.2.3.1 Standards. Table 3.11-3 presents standards for distributed timing service.

TABLE 3.11-3 Distributed timing service standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Distributed Time Service (DTS)	DCE 1.1 DTS:1994	Mandated (Approved)
CPC	IETF	Network Time Protocol (V3)	RFC 1305:1992	Mandated (Approved)
CPC	X/Open	X/Open DCE: Time Services	C310 (11/94)	Informational (Approved)
NPC	IEEE	POSIX - Part 1: Advanced Realtime System API Extension (C Language Binding)	P1003.1j	Emerging (Draft)
NPC	IEEE	POSIX - Part 1: System API Amendment: Real-Time Distributed Systems Communications	P1003.21	Emerging (Draft)

3.11.2.3.2 Alternative specifications. The following specification is available:

a. SAE ARD 50067 Draft: Avionics Operating System API Requirements.

3.11.2.3.3 Standards deficiencies. ISO/IEC 9945-1:1996 which incorporates IEEE 1003.1b contains time services related to high resolution real time timers, but internationalization and highly functional, system-wide clocks are beyond its scope. The IEEE P1003.1j draft standard extends the model of 1003.1b Clocks and Timers to include access to a monotonic clock and a synchronized clock; however, like 1003.1b, the actual implementation of these clocks is beyond the scope of the standard.

To date, there is no standardized API for the management of distributed time services. However, the IEEE P1003.21 working group intends to develop an API for time management services, which would include such time management protocols as NTP and DTS.

3.11.2.3.4 Portability caveats. If the time services are to be used in building internationalized programs, portability is unlikely. Behavior is not portable across systems in which one supports the nanosecond-resolution timers specified by the SVID and Berkeley Unix. However, the IEEE P1003.1j draft standard provides applications with explicit access to a synchronized clock,

utilizing the portable standard interfaces provided in IEEE 1003.1b (incorporated in ISO 9945-1:1996).

When several applications are executed simultaneously, problems may occur when remote application components are out of time synchronization with each other. DCE takes care of this by synchronizing all the host clocks on the system through its DTS.

One component of the DTS clerk reads the clocks for a certain time interval on each of the host machines through software called the DTS server. The DTS clerk then computes the midpoint between all the time intervals to determine a new average time and resets the clocks of each host. The DTS also can read time from an outside source, such as the Universal Coordinated Time Standard through a telephone or radio, then set host clocks to this time.

3.11.2.3.5 Related standards. IEEE 1003.1b is related to this service.

3.11.2.3.6 Recommendations. Procurements should use the time services corresponding to the operating system being specified in the procurement. OSF DCE Timing should be specified for distributed systems.

3.11.2.4 Distributed file services. (This BSA appears in part 8 and part 11.) Distributed file services (DFS) is a distributed client/server application, built on the underlying DCE services. It takes full advantage of the lower-level DCE services (such as RPC, Security, Threads, and Directory) and the distributed computing system. DFS provides many advantages over centralized systems. It provides a higher availability of data and resources, the ability to share information throughout a very large heterogeneous system, and efficient use of special computing functionality. Files are made highly available through replication, or caching, making it possible to access a copy of a file even when one of the machines on which a file is stored goes down. Further, users are able to work with unfamiliar file systems without having to know the unique commands for each system.

File Transfer, Access, and Management (FTAM) allows for the effective transfer, access, and management of different file types on remote systems by creating a virtual filestore that emulates the file services offered by existing file service systems.

Remote file access is the ability to access and/or change a file type or content at a location other than the user's. Remote file access is associated with distributed processing/client-server architectures, and is not used in host-terminal architectures.

3.11.2.4.1 Standard. Table 3.11-4 presents standards for distributed file services.

TABLE 3.11-4 Distributed file services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Distributed File Service (DFS)	DCE 1.1 DFS:1994	Mandated (Approved)
GPC	DOD	DoD Standardized Profiles - File Transfer, Access and Management (FTAM) - Parts 1,4, and 5 (References ISO 8571 parts 1-5)	MIL-STD-2045-17508 - Parts 1,4, and 5: 7/94	Informational (Approved)
CPC	X/Open	Protocols for X/Open PC Interworking: SMB, Version 2	C209 (10/92)	Informational (Approved)
CPC	X/Open	Protocols for X/Open Interworking: XNFS, Issue 4	C218 (10/92)	Informational (Approved)
NPC	IEEE	OSI API - File Transfer, Access, and Management (FTAM) (C Language)	1238.1:1994	Informational (Approved)
NPC	IEEE	POSIX, Part 1: Network-Transparent File Access	P1003.1f	Emerging (Draft)
CPC	IETF	NFS: Network File System Protocol Specification	RFC 1094:1989	Informational (Not Recommended)

3.11.2.4.2 Alternative specification. The only other available specifications are proprietary.

3.11.2.4.3 Standard deficiencies. Limited-Purpose File Transfer, Access and Management (FTAM) subsets do not provide file access capabilities. Only Full-Purpose FTAM subsets provide such capabilities. Limited-Purpose FTAM subsets cannot interoperate fully with Full-Purpose FTAM subsets.

IEEE Transparent File Access (TFA) addresses the POSIX.1 refinements needed for file access, but ignores the behavior of other facilities needed for file access between nodes, such as signals.

The Remote File System (RFS) is associated mostly with Unix-based systems rather than with heterogeneous operating systems on legacy systems as the Network File System (NFS) is.

NFS security uses the not very secure traditional Unix authentication and permissions. Secure NFS is not as secure as it could be because it ships security information around the network.

Although the Andrew File System (AFS) can provide good networked performance because it supports client caching, this requires large amounts of memory and disk buffer space, as well as a potentially long time for the first remotely accessed data to be downloaded

3.11.2.4.4 Portability caveats. The SVID provides facilities for getting file system information about a mounted file system, but none of the SVID functions ("statvfs()," "sftatvfs()," and "ustat()") are compatible with OSF/1's comparable functions ("statfs()," "fstatfs()," and "ustat()"). X/Open specifies enhancements to the "popen" and "pclose" system calls.

Because TFA does not go beyond the POSIX.1 refinements needed for file access and address the behavior of other facilities (e.g., signals) between nodes, a portability risk exists in using TFA between nodes. The TFA has two specifications, full TFA (which provides all of the file access services specified in ISO 9945-1) and Subset TFA (which defines file access semantics, which are less stringent than POSIX requires. Subset TFA also is designed for use with non-P1003.1 file systems. Consequently, it is possible to have two systems compliant with TFA, which are not compatible with each other, and which also may not be totally compatible with the core POSIX.1 file system.

The AFS is a superset of NFS, and IEEE TFA is a superset of AFS and NFS. Thus, a little backward compatibility exists between TFA and AFS and between AFS and NFS.

Systems using different FTAM subsets cannot be assured of portable applications or interoperability.

3.11.2.4.5 Related standards. The following standards are related to distributed files or distributed file standards:

a. ISO 9945-1:1996: (POSIX.1) System Interfaces.
b. IEEE 1224:1993: OSI Abstract Data Manipulation - API.
c. IEEE P1351: Association Control Service Element (ACSE) API.
d. RFC 1057: ONC Remote Procedure Call (RPC).
e. OSF:DCE RPC.

3.11.2.4.6 Recommendations. The OSF Distributed Computing Environment (DCE) Distributed File System is recommended for distributed computing environments based on TCP/IP.

MIL-STD-2045-17508 is recommended for legacy systems interoperability. Parts 1, 3, and 6 of the MIL-STD support only the Limited-Purpose FTAM (simple file transfer and management) system. This system does not provide file access capabilities. The MIL-STD-2045-17508, parts 4 and 5 support Full-Purpose FTAM (Positional file transfer, simple file access, and management)) system. Users requiring remote file access capabilities, based on OSI standards, should use parts 1, 4, and 5 of the MIL-STD.

An API to FTAM is provided by IEEE 1238.1.

3.11.2.5 Distributed directory services. (This BSA appears in part 4, part 9, and part 11.) A directory or naming service provides a standardized naming scheme, a standardized interface with the naming facilities, and the ability for the interface to provide transparent access to a variety of naming schemes and mechanisms (e.g., DCE).

Directory service applications convert a name into a physical address on a network, providing logical to physical conversion. Names can be user names, computers, printers, servers, or files. This enables users to find these resources without knowing their locations. The transmitting station sends a name to the server containing the naming service software, which sends back the actual address of the user or resource.

3.11.2.5.1 Standards. Table 3.11-5 presents standards for distributed directory services.

TABLE 3.11-5 Distributed directory services standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OSF	Distributed Computing Environment (DCE) Directory (Global and Cell) Service	DCE 1.1 Directory:1994	Mandated (Approved)
IPC	ISO	Open Systems Interconnection-Session Service Definition	8326:1987	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Connection-Oriented Session Protocol	8327:1987	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Basic Connection Oriented Presentation Service Definition	8822:1988	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Connection-Oriented Presentation Protocol	8823:1988	Informational (Approved)
IPC	ITU-T	The Directory: Models (X-ref: ISO 9594-2)	X.501 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Authentication Framework (X-ref: ISO 9594-8)	X.509, Version 3: 1993	Informational (Approved)
IPC	ITU-T	The Directory: Abstract Service Definition (X-ref: ISO 9594-3)	X.511 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Procedures for Distributed Operation (X-ref: ISO 9594-4)	X.518: 1993	Informational (Approved)
IPC	ITU-T	The Directory: Protocol Specification (X-ref: ISO 9594-5)	X.519 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Selected Attributes Types (X-ref: ISO 9594-6)	X.520 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Selected Object Classes (X-ref: ISO 9594-7)	X.521 (1993)	Informational (Approved)
IPC	ITU-T	The Directory: Replication (X-ref: ISO 9594-9)	X.525 (1993)	Informational (Approved)
CPC	X/Open	Federated Naming: The XFN Specification	C403 (7/95)	Informational (Approved)
NPC	IEEE	Directory services/Name space API	1224.2:1993	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Domain Name Service Profile (References IAB STD 13 (RFC 1034, 1035))	MIL-STD-2045-17505:1994	Informational (Approved)

3.11.2.5.2 Alternative specification. There are no alternative specifications available.

3.11.2.5.3 Standard deficiencies. Deficiencies in the existing specifications are unknown.

3.11.2.5.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.11.2.5.5 Related standards. There are no related standards.

3.11.2.5.6 Recommendations. OSF DCE directory services are recommended for DCE applications. For more information on non-DCE directory services, see the Host Application Support BSA in part 7, Communication Services.

3.11.3 Objects. These services define the rules for creating, deleting, and managing objects.

3.11.3.1 Object request broker. (This BSA appears both in part 8 and in part 11.) The Object Request Broker (ORB) provides a mechanism for accessing objects anywhere in a distributed computing environment. It provides a method for defining objects and their interfaces. In operation, the ORB provides routing, address resolution, and authentication services, as well as parameter marshaling and conversion if necessary.

3.11.3.1.1 Standards. Table 3.11-6 presents standards for object request brokers.

TABLE 3.11-6 Object request broker standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	OMG	Common Object Request Broker Architecture (CORBA) Version 2.0 (includes CORBAservices and CORBAfacilities)	CORBA 2.0:1995	Mandated (Approved)
CPC	X/Open	Common Object Request Broker: Architecture and Specification	C432 (8/94)	Informational (Approved)
CPC	X/Open	Common Object Services, Vol 1 & 2	P432/P502	Informational (Approved)
CPC	OMG	Common Object Request Broker Architecture (CORBA) Version 1.2, (Same as X/Open C432)	CORBA Specification Ver. 1.2 93-12-43	Informational (Approved)
CPC	OSF	Distributed Computing Environment (DCE)	DCE 1.1:1994	Informational (Approved)
CPC	TOG	Distributed Common Object Model/ActiveX	DCOM/ActiveX	Informational (Draft)
CPC	X/Open	Common Object Request Broker Architecture (CORBA), Version 1.0 (8/92) (Same as OMG specification 91-12-1)	P210	Informational (Superseded)

3.11.3.1.2 Alternative specifications. There are no alternative specifications available.

3.11.3.1.3 Standards deficiencies. At present, there is no independent test for conformance to any version of the CORBA specification.

CORBA 1.2 (also called CORBA 1.X) includes a standard Interface Definition Language (IDL) for defining objects. The IDL is not the same as OSF DCE Remote Procedure Call IDL, although there are similarities. CORBA 1.2 also defines a standard API for accessing ORB services, such as those needed to declare that an object is available for use, or to access an object.

CORBA 1.2 does not include a specification for interoperability between ORB's, therefore ORB's from different vendors are likely to be incompatible. This is a major feature of the new CORBA 2.0. OMG's CORBA 2.0 specification allows for two types of RPC mechanisms: (1) a mandatory General Inter-ORB Protocol (GIOP), and an optional DCE RPC protocol. ORB's that use different methods will still not be interoperable. CORBA 2.0 does not specify other types of distributed computing services (e.g. remote procedure call(RPC), security, directory, time,

threads, file system, and administration). Therefore, while CORBA 2.0 ORBs will interoperate, higher level distributed services (security, directory, etc.) may not.

CORBA requires a "mapping" of IDL into each application programming language that is used. Mappings exist for C, C++, and Smalltalk, and an Ada95 mapping is under development.

3.11.3.1.4 Portability caveats. Applications developed for one ORB are likely to be portable to a different ORB. However, the lack of interoperability specifications means that an object implemented on one ORB can usually not be accessed from a different ORB. In order to be interoperable, a system must select a single vendor's ORB for use across the enterprise.

All vendor claims for conformance to CORBA 2.0 should be matched by product demonstrations in the target environment before final contract award is made. If no such demonstration is made, serious interoperability and security problems could result, particularly in multi-vendor environments.

3.11.3.1.5 Related standards. The following standards are related to ORBs or their standards:

a. Component Integration Laboratories Inc. (CILabs):OpenDoc
b. Taligent Inc.:CommonPoint
c. Next Computer Inc.:OpenStep

3.11.3.1.6 Recommendations. Users buying distributed object technology from multiple vendors must be cautious. The use of ORB technology should be limited to pilot projects and programs with a limited number of sites. If an ORB is used, the Object Management Group (OMG) CORBA (Common Object Request Broker Architecture) Version 2.0 is recommended. The vendor must provide a plan to migrate to CORBA 2.0 with the DCE RPC as soon as possible. The vendor should also be required to state his proposed solutions to the other distributed computing services listed above, and to identify how these solutions relate to the distributed computing services already in the user's inventory.

Because of the lack of ORB interoperability, OSF DCE is the preferred solution to distributed computing requirements in the near term. OSF DCE provides the following distributed computing services: RPC, security, directory, time, threads, file system, and administration.

3.11.4 Remote access. These services support applications that use a partitioned database acting like a single coherent database. Also included are services for remote login and file transfer.

3.11.4.1 Remote login. (This BSA appears in part 8 and part 11.) Remote login is the ability of a user from a local machine to be an authorized user and access a remote machine.

3.11.4.1.1 Standards. Table 3.11-7 presents standards for remote login.

TABLE 3.11-7 Remote login standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	TELNET Protocol	Standard 8/RFC-854/RFC-855	Mandated (Approved)
IPC	IAB	Host Requirements	Standard 3/RFC-1122/RFC-1123	Mandated (Approved)
IPC	ISO	Open Systems Interconnection-Protocol Specification for the Association Control Service Element (ACSE)	8650:1988	Informational (Approved)
GPC	DOD	DoD Standardized Profile - Internet Remote Login Profile for DoD Communications (References IAB Std 8 (RFC 854 and RFC 855 - Telnet Protocol:1983) and IAB Std 3 (RFC 1123 - Requirements for Internet hosts:1989))	MIL-STD-2045-17506:7/94	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Virtual Terminal Basic Class Protocol	9041:1990	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Basic Connection Oriented Presentation Service Definition	8822:1988	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Connection-Oriented Presentation Protocol	8823:1988	Informational (Approved)
IPC	ISO	Open Systems Interconnection-Connection-Oriented Session Protocol	8327:1987	Informational (Approved)

3.11.4.1.2 Alternative specifications. None

3.11.4.1.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.11.4.1.4 Portability caveats. A procurement may specify Simple Systems or Forms-Capable Systems or both. However, the two systems cannot interoperate, and applications are not portable from one system to another. Each system is distinguished by the VT profile it supports: a Simple System supports the TELNET profile, and a Forms-Capable System supports the Forms profile. The Basic Class VT protocol is required in all cases; it operates independently of the Simple or Forms-Capable Systems.

3.11.4.1.5 Related standards. None

3.11.4.1.6 Recommendations. All new systems and systems undergoing major upgrades should use the Internet Architecture Board (IAB) STD 8 (RFC 854 and 855) and IAB STD 3 (RFC 1123). Those persons conducting procurements that involve IAB standards should review the

latest version of the IAB official protocol standards list to ensure that the appropriate RFCs are specified.

The OSI Virtual Terminal (VT) standard is recommended for legacy systems interoperability. A clear migration path to page, scroll, graphics, and mixed mode virtual terminal profiles that are being defined by the OSE Implementors' Workshop (OIW)/NIST should be required. Otherwise, systems capable of employing only TELNET and Forms will not interoperate with future VT systems. The "rlogin" facilities are delivered with Berkeley BSD-based UNIX operating systems. Those facilities are not in the System V Interface Definition (SVID).

Currently, a Simple VT and a Forms-Capable VT exist. Few vendors have implemented a simple version of VT. Procurements need to determine if Simple or Forms-Capable VT Systems are sufficient for the application. No tests have been developed for VT to test conformance. Remote login is associated with distributed processing/client-server architectures. It is not used in host-terminal architectures.

No standards exist for VT API. A procurement for a VT final system must include a vendor's offering of virtual terminal API. This API should accommodate as many VT types as possible.

3.11.4.2 Remote data access. (This BSA appears in part 4 and part 11.) RDA specifications are extensions of a data access (RDA) language to allow remote access to a database in a client-server environment. RDA refers to the interfaces, protocols, and formats needed to allow remote database access in a client-server environment, where the databases may be heterogeneous and from multiple vendors.

3.11.4.2.1 Standards. Table 3.11-8 presents standards for remote data access.

TABLE 3.11-8 Remote data access standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	OSI Remote Database Access (RDA), Part 1: Generic Model, Service and Protocol	9579-1:1993	Adopted (Approved)
IPC	ISO/IEC	OSI Remote Database Access, Part 2: SQL Specialization	9579-2:1993	Adopted (Approved)
CPC	X/Open	Data Management: SQL Remote Database Access	C307 (8/93)	Informational (Approved)
CPC	X/Open	Data Management: SQL Call Level Interface (CLI)	C451 (4/95) (Supersedes P303)	Informational (Approved)
CPC	SAG	Database Language SQL, Access Formats & Protocols (FAP) Specification:1991 (Based on SQL)	SQL Access FAP Specs:1991	Informational (Approved)
CPC	SAG	Database Language SQL Call Level Interface (CLI)	SQL-89	Informational (Approved)

3.11.4.2.2 Alternative specifications. The only other available specifications are proprietary.

3.11.4.2.3 Standards deficiencies. RDA specifies the service and protocol between only a single client and server. This is one reason that caused the formation of the SAG to put more distributed functionality into RDA. RDA does not consider multiple connections and, therefore, does not specify distributed database access. APIs and Ada bindings to the RDA standards are not defined.

RDA is aligned closely with the SQL-2 Entry Level. However, the integrity enhancement is optional. Also, RDA is not aligned currently with the FIPS 127-2 Transition Level, which the NIST considers very important for SQL use.

The ISO RDA and CLI are only a subset of the SAG's RDA and CLI.

3.11.4.2.4 Portability caveats. RDA's use of ISO Remote Operations Service Elements (ROSE) hinders precision, adds needlessly to the text and Abstract Syntax Notation (ASN).1, and incorporates assumptions that limit the usefulness of RDA. Furthermore, an implementation conforming to ISO 9545 (the OSI standard that refines the basic OSI Reference Model to provide a framework for coordinating the development of existing and future application layer standards) could not use ROSE, since they both claim to be application service elements.

RDA's optional integrity enhancement and the lack of alignment with the FIPS 127-2 Transition Level can result in differences among systems compliant with RDA that impede portability and interoperability.

3.11.4.2.5 Related standards. The following standards are related to remote data access or remote data access standards:

a. ISO 9072: ROSE
b. ISO 9075:1992: SQL Third Edition (same as NIST FIPS PUB 127-2:1993)
c. ISO 10026-1..3: Distributed Transaction Processing Model, Service, & Protocol
d. ANSI X3.135-1989: SQL
e. ANSI X3.168-1989: Embedded SQL
f. X/Open C193: Distributed TP: The XA Specification

3.11.4.2.6 Recommendations. The first choice for a standard would be RDA, ISO 9579, and RDA: SQL Specialization, ISO 9579-2, unless the additional functionalities provided by the SAG are needed.

Where RDA lacks desired capabilities for a procurement, consider SQL Access Formats and Protocols Specifications or the X/Open RDA. The SAG and X/Open are tracking the RDA standard and both support RDA extensions that are being adopted by the emerging RDA standard. Consider the X/Open specified ASN.1 replacement module that eliminates the use of ROSE.

3.11.4.3 File transfer. File transfer is a service that provides transmission of a variety of file types across electronic media.

MIL-STD-2045-17508 uses OSI FTAM, Association Control Service Element (ACSE), presentation, and session protocols as base standards. The FTAM standards specify services and protocols for three different types of software file activities. The File Transfer portion of the standard supports bulk file transfer between networked systems. The File Access portion of the standard allows users to retrieve and update one record at a time from the middle of a file, to add or insert a record into the file, and to delete files. The File Management portion of the standard allows users to create new files and file attributes, to inspect and change the properties of a file, and to handle the naming of files. In addition, the protocol manages file ownership functions such as who has access rights to read, write, or modify a file.

3.11.4.3.1 Standards. Table 3.11-9 presents standards for file transfer.

TABLE 3.11-9 File transfer standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	IAB	Host Requirements	Standard 3/RFC-1122/RFC-1123	Mandated (Approved)
IPC	IAB	TELNET Protocol	Standard 8/RFC-854/RFC-855	Mandated (Approved)
IPC	IAB	File Transfer Protocol	Standard 9/RFC-959	Mandated (Approved)
CPC	IETF	Network Time Protocol (V3)	RFC 1305:1992	Mandated (Approved)
CPC	IETF	Hypertext Transfer Protocol -- HTTP/1.0	RFC 1945:1996	Mandated (Approved)
GPC	DOD	Common Messaging Strategy and Procedures, November 1995	ACP 123 US Supplement No. 1	Mandated (Approved)
IPC	ITU-T	The Directory - Overview of Concepts, Models and Services - Data Communication Networks Directory, 1993	X.500	Mandated (Approved)
GPC	DOD	Connectionless Data Transfer Application Layer Standard, July 27, 1995	MIL-STD-2045-47001	Mandated (Approved)

3.11.4.3.2 Alternative specifications. Alternative specifications are unknown.

3.11.4.3.3 Standards deficiencies. No deficiencies have been identified in the existing standards.

3.11.4.3.4 Portability caveats. Systems using different FTAM subsets cannot be assured of portable applications or interoperability.

3.11.4.3.5 Related standards. None

3.11.4.3.6 Recommendations. New acquisitions requiring file transfer services should use Internet Architecture Board (IAB) standard 9 and IAB standard 3. The IAB standard 9 should be implemented with Store unique (STOU) and Abort (ABOR) command mandated on reception. The IAB standard 3 updates the IAB standard 9 by correcting errors in the protocol specification.

MIL-STD-2045-17504 and MIL-STD-2045-17508 and TFTP are recommended for legacy systems interoperability. The MIL-STD-2045-17508, parts 1, 3 and 6 support only the Limited-Purpose FTAM (simple file transfer and management) system. They do not support the Full-Purpose FTAM (positional file transfer, simple file access, and management) system. Users requiring the Full-Purpose FTAM system also should use parts 4 and 5 of the MIL-STD-2045-17508. These parts are identical to parts 4 and 5 of the International Standardized Profile (ISP) 10607.

MIL-STD-2045-14503, Internet Transport Service Supporting OSI Applications, specifies a standard for the operation of OSI applications over TCP/IP. It uses RFC 1006, ISO Transport service on top of the TCP, Version 3, as one of its base standards. Implementations requiring use of MIL-STD-2045-17508 over TCP/IP should use MIL-STD-2045-14503. An application level gateway will be necessary for interoperation between systems implementing MIL-STD-2045-17508 and systems implementing MIL-STD-2045-17504 or FTP. The Internet Engineering Steering Group has approved the Internet draft FTP-FTAM Gateway Specification.

If recommended standards do not meet system requirements, or are cost prohibitive, standards from the legacy systems use may be used as long as interoperability is not impacted. The use of legacy standards may require a waiver from the appropriate authority. Those persons conducting procurements that involve FTP should review the latest version of the Internet Architecture Board (IAB) official protocol standards list to ensure that the appropriate Request For Comments (RFCs) are specified.

The DOD is developing a file and record transfer protocol to meet the specific requirements for resource constrained environments. The Unix-Unix Communications Protocol (UUCP) permits file transfer between two UNIX-based systems via a dial-up connection. Kermit, Xmodem, and Zmodem are other dial-up file transfer protocols.

3.11.5 Distributed computing security. Security-oriented services protect the information, components, and mechanisms of the information system. Use and compliance with the security standards identified in this document do not constitute authorization to process classified data. DoD policy covering the accreditation process must still be adhered to in order to obtain approval for the processing of classified data.

3.11.5.1 System access control. (This BSA appears in part 4, part 9, part 10, and part 11.) System access control standards provide high-level guidance on access control frameworks and implementation.

3.11.5.1.1 Standards. Table 3.11-10 presents standards for system access control.

TABLE 3.11-10 System access control standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
IPC	ISO/IEC	OSI Common Management Information Services (CMIS) Definition, with Amendment 4: Access Control	9595:1991/ AM4:1992	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 9: Objects and Attributes for Access Control	10164-9:1995	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 3: Access Control	10181-3	Informational (Draft)

3.11.5.1.2 Alternate specifications. There are no alternative specifications.

3.11.5.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.11.5.1.4 Portability caveats. Portability problems in the existing standards are unknown.

3.11.5.1.5 Related standards. The following guidelines support the TCSEC standard:

a. NCSC-TG-003, Version 1, September 1987, A Guide to Understanding Discretionary Access Control in Trusted Systems

b. NCSC-TG-028, Version 1, May 1992, Assessing Controlled Access Protection

c. NCSC-TG-020-A, August 1989, Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX System

3.11.5.1.6 Recommendations. The mandated standards are recommended.

3.11.5.2 Entity authentication. (This BSA appears in part 8, part 9, part 10, and part 11.) Entity authentication standards address data, processes, systems, and enterprises.

3.11.5.2.1 Standards. Table 3.11-11 presents standards for entity authentication.

TABLE 3.11-11 Entity authentication standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Security Services	DCE 1.1 Security Services: 1994	Mandated (Approved)
GPC	NIST	Computer Data Authentication	FIPS PUB 113:1985	Informational (Approved)
GPC	NIST	Entity Authentication Using Public Key Cryptography	FIPS PUB 196:1996	Emerging (Approved)
CPC	OSF	Distributed Computing Environment (DCE) Rev. 1.2.2	DCE Rev. 1.2.2:1996	Informational (Approved)
IPC	ISO	Financial Transactions - Retail Banking Security Requirements for Message Authentication	9807	Informational (Approved)
IPC	ISO	Entity Authentication Mechanisms - Part 1: General Model	9798-1:1991	Informational (Approved)
IPC	ISO	Entity Authentication Mechanisms - Part 3: Entity Authentication Using a Public Key Algorithm	9798-3:1993	Informational (Approved)
GPC	NIST	Guideline for Use of Advanced Authentication Technology Alternatives	FIPS PUB 190:1994	Informational (Approved)
IPC	ISO	Entity Authentication - Part 2: Mechanisms Using Symmetric Encipherment Algorithms	9798-2:1994	Informational (Approved)
IPC	ISO	Entity Authentication - Part 4: Mechanisms Using a Cryptographic Check Function	9798-4:1995	Informational (Approved)
CPC	X/Open	Security Interface Specification: Auditing and Authentication	S020: 1990	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
CPC	IETF	The Kerberos Network Authentication Service (V5)	RFC 1510:1993	Informational (Draft)
IPC	ISO	Entity Authentication Mechanisms, Part 5: Entity Authentication Using Zero Knowledge Techniques	9798-5:1993	Informational (Draft)

3.11.5.2.2 Alternate specifications. There are no alternative specifications.

3.11.5.2.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.11.5.2.4 Portability caveats. OSF DCE Version 1.1's authentication service is based on Kerberos Version 5 (RFC 1510), but is not totally compatible with RFC 1510. DCE 1.2.2 adds testing and official support for Kerberos Version 5.

3.11.5.2.5 Related standards. The following standards are related to entity authentication:

a. DOD NCSC-TG-017, Version 1, September 1991, Guide to Understanding Identification and Authentication in Trusted Systems.

b. FIPS PUB 196, 11 October 1996.

FIPS PUB 196 becomes effective 6 April 1996. It is based on ISO/IEC 9798-3:1993 and specifies two challenge-response protocols by which entities in a computer system may authenticate their identities to one another. FIPS PUB 196 is for use in public key based challenge-response and authentication systems at the application layer within computer and digital telecommunications systems.

3.11.5.2.6 Recommendations. The mandated standards are recommended.

3.11.5.3 Security audit. (This BSA appears in part 7, part 9, part 10, and part 11.) Security auditing is a review or examination of records and activities to test controls, ensure compliance with policies and procedures, detect breaches in security, and indicate changes in operation (paraphrased from ISO 7498-2).

3.11.5.3.1 Standards. Table 3.11-12 presents standards for security audit.

TABLE 3.11-12 Security audit standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 8: Security Audit Trail Function (same as ITU-T X.740)	10164-8:1993	Informational (Approved)
CPC	X/Open	Security Interface Specification: Auditing and Authentication	S020: 1990	Informational (Approved)
IPC	CCEB	Common Criteria for Information Technology Security Evaluation, (CC) Version 1.0	CC Version 1.0: 1996	Emerging (Draft)
IPC	ISO/IEC	OSI Security Frameworks for Open Systems, Part 7: Security Audit Framework	10181-7	Informational (Draft)
IPC	ISO/IEC	OSI Distributed Transaction Processing (DTP) - Draft Amendments to Parts 1-3: Transaction Processing Security	WDAMs ((SC21 N6232) to ISO 10026-1,2,3) 1994	Informational (Draft)

3.11.5.3.2 Alternate specifications. There are no alternative specifications.

3.11.5.3.3 Standards deficiencies. ISO Transaction Processing Security work (WDAMs to ISO 10026-1,2,3) is in the early stages. Its content is not defined, and it cannot be used for procurement. ISO 10164-8 does not define a security audit, or explain how to perform one. It does not define implementation aspects, occasions where the use of the security audit trail function is appropriate, or the services necessary for the establishment and normal or abnormal release of a management association.

There is a need for a standard for programming and interfaces to support development of portable tools for audit trail analysis and configuration.

3.11.5.3.4 Portability caveats. Proposed amendments to ISO 10026 have ceased. This is a high portability risk area.

3.11.5.3.5 Related standards. The following guidelines support the TCSEC standard:

a. NCSC-TG-005, Version 1, July 1987, Trusted Network Interpretation

b. NCSC-TG-011, Version 1, 1 August 1990, Trusted Network Interpretation Environments Guideline - Guidance for Applying the Trusted Network Interpretation

c. NCSC-TG-001, Version 2, June 1988, A Guide to Understanding Audit in Trusted Systems

3.11.5.3.6 Recommendations. The mandated standard is recommended.

3.11.5.4 Distributed computing security labeling. (This BSA appears both in part 10 and part 11.) Distributed computing security labeling provides a security labeling service to support mandatory access controls within a distributed environment.

3.11.5.4.1 Standards. Table 3.11-13 presents standards for distributed computing security labeling.

TABLE 3.11-13 Distributed computing security labeling standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	The DOD Trusted Computer Systems Evaluation Criteria	DOD 5200.28-STD: 1985	Mandated (Approved)
GPC	DOD	Trusted Database Management System Interpretation of the Trusted Computer Systems Evaluation Criteria	NCSC-TG-021, Version 1: 1991	Mandated (Approved)
GPC	DOD	Compartmented Mode Workstation (CMW) Evaluation Criteria	DDS-2600-6243-92	Informational (Approved)
GPC	DOD	CMW Labeling: Source Code and User Interface Guidelines, Revision 1	DDS-2600-6243-91	Informational (Approved)
GPC	DOD	CMW Labeling: Encoding Format	DDS-2600-6216-91	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)

3.11.5.4.2 Alternate specifications. There are no alternative specifications.

3.11.5.4.3 Standards deficiencies. The subjects and objects requiring security labeling in a distributed computing environment have not been standardized or identified in any standardized framework.

3.11.5.4.4 Portability caveats. Portability problems with the existing standards are unknown.

3.11.5.4.5 Related standards. DOD 5200.1-R, "Information Security Program Regulation," June 1986, establishes DOD policy for security classification, declassification, and marking of DOD information. It also contains DOD policy for safeguarding of classified information, including accountability, storage, transmission, and destruction of the information.

3.11.5.4.6 Recommendations. The mandated standards are recommended.

The DGSA (TAFIM Volume 6) provides general architectural guidance for information domains which can exist in a distributed environment. The properties of information domains share some similarities with security labels in a distributed environment.

3.11.5.5 Data encryption security. (This BSA appears in part 5, part 7, part 10, and part 11.) Encryption is the cryptographic transformation of data to produce cipher text. Standards for data encryption security services describe services such as definitions/algorithms, modes of operation, and guidelines for use for those systems that require their data to be encrypted using data encryption security services. None of these standards are for systems processing classified information.

3.11.5.5.1 Standards. Table 3.11-14 presents standards for data encryption security.

TABLE 3.11-14 Data encryption security standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Escrowed Encryption Standard (EES)	FIPS PUB 185: 1994	Mandated (Approved)
GPC	NIST	Data Encryption Standard (DES) (related to ANSI X3.92-1981/R1987/R1993)	FIPS PUB 46-2:1993 (Reaffirmed until 1998)	Informational (Approved)
GPC	NIST	Guidelines for Implementation and using the NBS Data Encryption Standard	FIPS PUB 74:1981	Informational (Approved)
GPC	NIST	Data Encryption Standard (DES) Modes of Operation (related to ANSI X3.106-1983)	FIPS PUB 81:1980	Informational (Approved)
GPC	NIST	Security Requirements for Cryptographic Modules	FIPS PUB 140-1:1994	Informational (Approved)
IPC	ISO	Modes of Operation for a 64-Bit Block Cipher Algorithm (Related to ANSI X3.106)	8372:1987	Informational (Approved)
NPC	ANSI	Data Encryption Algorithm	X3. 92-1981 (R1993)	Informational (Approved)
NPC	ANSI	Digital Encryption Algorithm - Modes of Operation	X3.106-1983 (R1990)	Informational (Approved)
GPC	NIST	Advanced Encryption Standard	FIPS PUB JJJ	Informational (Formative)

3.11.5.5.2 Alternate specifications. The only other available specifications are proprietary, for example, RSA.

3.11.5.5.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.11.5.5.4 Portability caveats. DES applications are not interoperable with non-DES systems. Portability problems related to EES are unknown. The U.S. controls export of cryptographic technologies, products, and related technologies as munitions. On October 1, 1996, a new federal policy allowing U.S. vendors to export products using up to 56-bit encryption, provided the vendors sign an agreement to make their 56-bit encryption technologies key-recovery-compliant within 24 months.

3.11.5.5.5 Related standards. FIPS PUB 113, Computer Data Authentication, is related to DES security mechanisms and their standards.

3.11.5.5.6 Recommendations. The mandated standard is recommended. FIPS PUB 185, EES, supports lawful authorized access to the keys required to decipher enciphered information for systems requiring strong encryption protection of sensitive but unclassified information. EES provides stronger protection than DES against unauthorized access. Devices conforming to EES may be used when replacing Type II and Type III (DES) encryption devices owned by the Government. Implementations requiring use of EES should require conformance with FIPS PUB 140-1.

On 2 January 1997, NIST announced plans to develop a FIPS, Advanced Encryption Standard, incorporating an advanced encryption algorithm to replace DES (FIPS PUB 46-2).

3.11.5.6 Systems non-repudiation. (This BSA appears in part 5, part 7, part 10, and part 11.) These standards provide the security services for non-repudiation in systems.

3.11.5.6.1 Standards. Table 3.11-15 presents standards for systems non-repudiation.

TABLE 3.11-15 Systems non-repudiation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Digital Signature Standard (DSS)	FIPS PUB 186:1994	Mandated (Approved)
GPC	DOD	Information Technology - Defense Standardized Profiles AMHXn(D)- Message Handling Systems - Message Security Protocol (MSP) Parts 1-5	MIL-STD-2045-18500: 1993	Mandated (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, Rev. 3.0: 1994	Legacy (Approved)
GPC	NSA	Message Security Protocol (MSP)	SDN.701, v. 4.0, Rev. A: 1997	Emerging (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 1: Overview, Models, and Notation	11586-1:1994	Informational (Approved)
IPC	ISO	Generic Upper Layer Security (GULS) - Part 4: Protecting Transfer Syntax Specification	11586-4:1994	Informational (Approved)
IPC	ISO	OSI Basic Reference Model, Part 2: Security Architecture (same as CCITT X.800:1991)	7498-2:1989	Informational (Approved)
CPC	IETF	IP Authentication Header (AH)	RFC 1826: 1995	Emerging (Draft)
CPC	OMG	Common Object Request Broker Architecture (CORBA) Security	OMG 95-12-1: 1995	Emerging (Draft)
CPC	IETF	S/MIME Message Specification: PKCS Security Services for MIME	draft-dusse-mime-msg-spec-00.txt, September 1996	Informational (Draft)
IPC	ISO/IEC	OSI Security Frameworks in Open Systems, Part 4: Non-Repudiation (same as ITU-TS X.813)	10181-4	Informational (Draft)
IPC	ISO	Non-Repudiation Mechanisms Part 1: General Model	13888-1:1992 (SC27 N868 (Project 1.27.06.01))	Informational (Draft)
IPC	ISO	Non-Repudiation Mechanisms Part 2: Using Symmetric Encipherment Algorithms	13888-2:1994 (SC27 N864 (Project 1.27.06.02))	Informational (Draft)
IPC	ISO	Non-Repudiation Mechanisms Part 3: Using Asymmetric Techniques	13888-3:1992 (SC27 N869 (Project 1.27.06.03))	Informational (Draft)
IPC	ISO	OSI Distributed Transaction Processing (DTP) - Draft Amendments to Parts 1 to 3: Transaction Processing Security	WDAMs (SC21 N 5232 to ISO 10026-1,2,3) 1991	Informational (Draft)

3.11.5.6.2 Alternate specifications. There are no alternative specifications.

3.11.5.6.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.11.5.6.4 Portability caveats. Portability problems in the existing standards are unknown.

3.11.5.6.5 Related standards. FIPS PUB 180-1, Secure Hash Standard, must be used with FIPS PUB 186. FIPS PUB 180-1 provides the Secure Hash Algorithm used in generating and verifying electronic signatures.

3.11.5.6.6 Recommendations. The mandated standards are recommended for non-repudiation.

MIL-STD-2045-18500 describes the security provided by MSP. It should be used for DOD message systems that are required to exchange classified and sensitive but unclassified information. It is based on Version 3.0 of the MSP documented in SDN.701, "Secure Data Network System (SDNS) Message Security Protocol," Revision 1.5, 1 August 1989. MSP is under revision to Version 4.0 to accommodate, in part, Allied requirements. This DSP standard will be replaced by a portion of the U.S. Supplement to ACP 123 or ACP 120, Common Security Protocol, when the revision to MSP is complete.

MSP provides for signed receipts. S/MIME, an Internet Draft specification, does not provide for signed receipts.

3.11.5.7 Security alarm reporting. (This BSA appears in part 7, part 9, part 10, and part 11.) Security alarm reporting is the capability to receive notifications of security-related events, alerts of any misoperations in security services and mechanisms, alerts of attacks on system security, and information as to the perceived severity of any misoperation, attack, or breach of security.

3.11.5.7.1 Standards. Table 3.11-16 presents standards for security alarm reporting.

TABLE 3.11-16 Security alarm reporting standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	NMF	OMNIPoint 1 (Adopts ISO Profile Sets 11183-X, 12059-X, and 12060-X, includes ISO/IEC 10164-X)	OMNIPoint 1:1993	Informational (Approved)
IPC	ISO/IEC	OSI Systems Management, Part 7: Security Alarm Reporting Function (same as ITU-T X.736)	10164-7:1992	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179-1:1995	Informational (Approved)
GPC	NIST	Government Network Management Profile (GNMP)	FIPS PUB 179:1992	Informational (Superseded)

3.11.5.7.2 Alternate specifications. There are no alternative specifications.

3.11.5.7.3 Standards deficiencies. FIPS PUB 179-1 supersedes FIPS PUB 179. ISO 10164-7 does not define implementation aspects, specify the manner in which management is accomplished by the user of the Security Alarm Reporting Function (SARF), define interactions that result in the use of the SARF, or specify the services necessary for the establishment and normal and abnormal release of a management association.

3.11.5.7.4 Portability caveats. Portability problems with the existing specifications are unknown.

3.11.5.7.5 Related standards. There are no related standards.

3.11.5.7.6 Recommendations. There are no recommended standards for security alarm reporting.

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 12 of 14 parts)

MULTIMEDIA SERVICES

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

TABLE OF CONTENTS

LIST OF TABLES

3.12 Multimedia. For purposes of this part of the ITSG, multimedia is defined as: "Two or more media types (audio, video, imagery, text, and data) electronically manipulated, integrated, and reconstructed in synchrony." This definition was developed by the Interactive Multimedia Association (IMA). Part 12 covers multimedia data interchange, programming environments and systems, presentation, and multimedia aspects of video and audiographic teleconferencing.

By definition, multimedia encompasses a broad range of media types and associated standards. Because multimedia is an emerging technology, many related standards are industry-based de facto standards or emerging official standards. Therefore, as a general rule, any procurement involving multimedia should proceed with caution in standards selection and ensure that selected standards are compatible. Often, interim solutions may be required to meet immediate mission requirements. Therefore original source materials should always be maintained for archival and re-use purposes.

The first step in selecting and adhering to the right multimedia standards is assuring that end-users, designers, and acquisition staff have a clear vision of what the final product must do. The DOD model for process definition is the Integration Definition (IDEF) process. Through it, process owners and decision makers can visualize how selected technologies will enhance the core operation. Following the process through the steps in the model helps assure sufficient vision, imagination, and scope have gone into the project. This increases the likelihood that the multimedia solution meets as many of the present and planned mission requirements as possible. It also demonstrates when, where, and to what degree multimedia standards apply.

Multimedia standards apply differently according to the types of products or services required and the individual's role in the process. However, regardless of how wide or narrow the frame of reference, understanding the multimedia principles of portability, interoperability, and interchangeability will help achieve the ultimate goal of compatibility to the maximum extent possible.

Portability means software (e.g., a multimedia application or title) can run without regard to system hardware, operating system, mode (stand-alone, network, distributive, mainframe-to-terminal, etc.), or peripheral equipment. Measures of portability attempt to express the ease of operating a piece of software on different automated systems. The more portable the application development environment, the more likely that a favorite application is available to the end-user's favorite platform.

(NOTE: For purposes of part 12, a multimedia title is a finished multimedia production for presentation to an end-user.)

Interoperability is successful interchange of both data and meaning. Application processes interoperate when the output of a given process is successfully acquired and used by other processes. Consider an audiographic teleconference. The goal of the conference is to talk about and make changes to a document that includes text, graphics, and other elements. Assume that the participants have software that can display this document, but that each participant has a different brand of software. If any participant can make changes to the document that are then

displayed to all participants, then interoperability exists. However, if a participant must relate desired changes to the conference initiator, who then makes the changes and displays the edited document on the other participants' computers, portability exists but not interoperability.

General-purpose standards to support interoperability are usually complex and comprehensive. Usually such standards rely on other standards and families of related standards to provide interoperability.

NOTE: Throughout Part 12, all tables have abbreviations listed under the column (Standard Type) as follows:

a. National Public Consensus = NPC
b. International Public Consensus = IPC
c. Government Public Consensus = GPC
d. Consortia Public Consensus = CPC
e. Corporate Private Non-Consensus = CPN-C

3.12.1 Multimedia data interchange formats and protocols. Interchange refers to transferring information between processes (applications or services). Interchange can be successful only if both parties to the interchange transaction, sender and receiver, know about the format of the information being interchanged. Interchange can be blind, which means that the information must be self-describing to some extent, or negotiated, which means that sender and receiver carry on a dialogue to determine formats they have in common and can interchange successfully.

Information can be interchanged at several semantic levels. The simplest level we will call a monomedia format or data type. A data type represents one type of information. Multimedia data types of interest include text, vector graphics, raster graphics (still and moving images), and audio. All data types are represented in encoded form. The encoding may be simple (e.g., 7-bit ASCII text) or complex (e.g., Moving Picture Experts Group [MPEG] compression and motion prediction).

Data types may be interchanged directly or embedded in more structured interchange files or data streams. Collections of monomedia objects may be wrapped in a container file, such as Bento (created by Apple and recommended by the IMA). Relationships among the objects in these files, such as synchronization information, may be shown by providing additional information.

Another layer of structuring may be provided by providing a direct mapping onto the file system of an operating system. Such features of file systems as directories, subdirectories, and files may have direct analogues on the transmission media (e.g., tape, floppy disk, or CD-ROM).

Data formats allow interchange of monomedia information. Container file formats allow interchange of information that is more structured and is capable of showing relationships among the data formats. Many data- and container-format specifications contain extra information that permits some meaning to be deduced from the interchange of formats. Currently, most data interchange is accomplished with data formats.

3.12.1.1 Text encoding interchange. Text encodings are methods of defining characters sets as numerical values that are mapped to specific characters. This BSA is a distillation of the Characters and Symbols MLSA.

3.12.1.1.1 Standards. Table 3.12-1 presents multimedia standards for text interchange.

TABLE 3.12-1 Text encoding interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Universal Multiple-Octet Coded Character Set (UCS), Part 1: Architecture and Basic Multilingual Plane (with Technical Corrigendum 1: 1996)	10646-1:1993	Mandated (Approved)
IPC	ISO/IEC	ISO 8-Bit Single-Byte Coded Graphic Character Sets: Parts 1-9	8859-1 to 9:1987-1989	Mandated (Approved)
IPC	ISO/IEC	ISO 8-Bit Single-Byte Coded Graphic Character Sets: Part 10: Latin Alphabet Set No. 6	8859-10:1992	Mandated (Approved)
GPC	NIST	Code for Information Interchange, Its Representations, Subsets, and Extensions (ASCII) (adopts ANSI X3.4-1986/R 1992, X3.32-1990, X3.41-1974)	FIPS PUB 1-2:1984	Informational (Approved)
CPC	Unicode Consortium	Unicode version 1.1	UCS-2	Informational (Approved)
GPC	NIST	Additional Controls for Use with American National Standard Code for Information Interchange (adopts ANSI X3.64-1979/R1990)	FIPS PUB 86:1981	Informational (Approved)
IPC	ISO	ISO 7-Bit Coded Character Set for Information Exchange	646:1991	Informational (Approved)
IPC	ISO/IEC	Character Code Structure and Extension Techniques	2022:1994	Informational (Approved)
NPC/IPC	ANSI/ISO/IEC	ISO 8-Bit Code for Information Interchange - Structure and Rules for Implementation (8-Bit ASCII) (Revision and redesignation of ANSI X3.134.1)	4873:1991	Informational (Approved)
IPC	ISO/IEC	Coded Graphic Character Set for Text Communication - Latin Alphabet Second Edition (replaces 6937 pt.1 & pt. 2)	6937:1994	Informational (Approved)
IPC	ISO/IEC	Control Functions for ISO 7-Bit and 8-Bit Coded Character Sets	6429:1992	Informational (Approved)
CPC	X/Open	Universal Multiple-Octet Coded Character Set Coexistence and Migration	E401 (3/94)	Informational (Approved)
TBD	JIS	JIS--Japan Unix	JIS X0201/0202	Informational (Approved)
CPN-C	AT&T	Extended Unix Code (EUC) (ISO 2022 compliant)	System V Multinational Language System	Informational (Approved)
CPN-C	Microsoft	Shift - JIS for PCs and Macs (ISO 2022 compliant)	Microsoft Japan's language support	Informational (Approved)
CPC	Unicode Consortium	Unicode Standard	Unicode v. 2.0	Informational (Draft)
IPC	ISO/IEC	Universal Multiple-Octet Coded Character Set, Part 1: Architecture and Basic Multilingual Plane, Amend 1: UTF-16, Amend 2: UTF-8, Amend 3: control characters, Amend 4: remove UTF-1	10646-1, Am 1-4:1993	Informational (Draft)
IPC	ISO	Universal Multiple-Octet Coded Character Set, Part 1: Architecture and Basic Multilingual Plane, Amend 5: Korean Hangul; 6: Tibetan additions; 8: Han unification	10646-1: DAM 5-8	Informational (Draft)

3.12.1.1.2 Alternative specifications. None.

3.12.1.1.3 Standards deficiencies. For character sets, each language needs a programming environment to handle conversion, sorting, and string handling to support proper localization and internationalization.

3.12.1.1.4 Portability caveats. Target presentation systems and viewers may not have the required support for specific text encodings.

A backward incompatible change of ISO 10646 is being prepared. It involved a rearrangement of the code positions for some Korean characters. This will probably be in draft amendment 5 which is expected in 1997. This rearrangement is contrary to the previous policy of the committee.

3.12.1.1.5 Related standards. None.

3.12.1.1.6 Recommendations. ISO 8859 is the predominant character encoding standard used in X Windows and includes multilingual character set standards. ISO 2022 specifies methods of extending the 255-glyph [illegible] sets coded by single octets. ISO 10646 allows multiple-byte encodings.

Unicode is a standard for the representation of international character sets. It is ISO 10646 compliant. Unicode uses a unified Han character set to represent Japanese and Chinese characters. A country-specific implementation may be required for each country if this system is used. Unicode should be used for any new systems for which will need large character sets such as those used in foreign languages.

3.12.1.2 Document interchange. (This BSA appears in part 5, Data Interchange, and part 12, Multimedia.) Document interchange standards allow the transfer of formatted documents across a network so they can be reproduced exactly and worked on at their destinations.

3.12.1.2.1 Standards. Table 3.12-2 presents standards for document interchange.

TABLE 3.12-2 Document interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Standard Generalized Markup Language (SGML) (Amendment 1 - 1988) (Adopted by FIPS PUB 152:1989)	8879:1986	Mandated (Approved)
CPC	IETF	HyperText Markup Language (HTML) v.2.0	RFC 1866:1995	Mandated (Approved)
GPC	DOD	Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of text (based on ISO 8879)	MIL-PRF-28001	Informational (Approved)
IPC	ISO/IEC	Distributed Office Applications Model (DOAM), Part 1: General Model	10031-1:1991	Informational (Approved)
IPC	ISO/IEC	Distributed Office Applications Model (DOAM), Part 2: Distinguished Object Reference and Associated Procedures	10031-2:1991	Informational (Approved)
IPC	ISO/IEC	Document Filing and Retrieval (DFR), Part 1: Abstract Service Definition and Procedures (corrigendum 1-1994, corrigendum 2- 1994, corrigendum 3-1994)	10166-1:1991	Informational (Approved)
IPC	ISO/IEC	Document Filing and Retrieval (DFR), Part 2: Protocol Specification (corrigendum 1-1994)	10166-2:1991	Informational (Approved)
IPC	ISO	Text and Office Systems - Referenced Data Transfer - Part 1: Abstract Service Definition	10740-1	Informational (Approved)
IPC	ISO	Text and Office Systems - Referenced Data Transfer - Part 2: Protocol Specification	10740-2	Informational (Approved)
IPC	ITU-T	Document Transfer and Manipulation (DTAM) - Services and Protocols- Introduction and General Principles	T.431 (1992)	Informational (Approved)
IPC	ITU-T	Document Transfer and Manipulation (DTAM) - Service Definition	T.432 (1993)	Informational (Approved)
IPC	ITU-T	Document Transfer and Manipulation (DTAM) - Protocol Specification	T.433 (1993)	Informational (Approved)
IPC	ITU-T	Document Transfer and Manipulation (DTAM) - Operational Structure	T.441 (1989)	Informational (Approved)
NPC	ANSI	Text Information Interchange in Page Image Format (PIF)	X3. 98-1983	Informational (Approved)
IPC	ISO	Standard Generalized Markup Language (SGML) Document Interchange Format Support Facilities (SDIF)	9069:1988	Informational (Approved)
IPC	ISO/IEC	Documentation Style Semantics and Specification Language (DSSSL)	10179:1995	Informational (Approved)
CPN-C	AT&T	TROFF - Markup Language	Unix BSD 4.3	Informational (Approved)
CPN-C	Microsoft	Rich Text Format (RTF)	RTF Tech. Manuals	Informational (Approved)
CPN-C	Adobe	PostScript Type 1 - Outlines	PS Tech. Manuals	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPN-C	Adobe	Portable Document Format (PDF)	PDF	Informational (Approved)
CPC	IETF	HyperText Markup Language (HTML)	HTML v.3.2	Emerging (Draft)
GPC	DOD	Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of text (based on ISO 8879)	MIL-M-28001B of 6/26/1993	Informational (Superseded (CALS))

3.12.1.2.2 Alternative specifications. The following specifications are also available:

a. ANSI/NISO Z39.59-1988 (to represent the logical structure of books and articles)

b. The Association of American Publishers (AAP), the Text Encoding Initiative (TEI), and the DOD Continuous Acquisition and Life Cycle Support (CALS) program have designed alternate nonproprietary architectures with SGML encodings

c. Microsoft's Dynamic Data Exchange (DDE)

d. Microsoft's Dynamic Link Libraries

e. ANSI/NISO Z39.2-1994: Information Interchange Format

f. ANSI/NISO Z39.18-1995: Scientific and Technical Reports - Elements, Organization, and Design

g. ANSI/NISO Z39.50-1992: Information Retrieval Application Service Definition and Protocol Specification for Open Systems Interconnection

h. ANSI/NISO Z39.59-1992: Common Command Language for Online Interactive Information Retrieval

3.12.1.2.3 Standards deficiencies. There is very little standardization of font names when handling fonts represented by tagged-text data types. However, many systems are attempting font substitution, that is, replacing a specified font with one that is similar, such as substituting TrueType Arial for PostScript Helvetica. Not all tagged text systems are able to specify colored text.

3.12.1.2.4 Portability caveats. At present, portability using ODA/ODIF is limited, because it is not in widespread use or widely available, although SGML is widely available.

3.12.1.2.5 Related standards. The following standards are related to document exchange:

a. ISO 8824:1987 and ISO 8825:1987 - ASN.1/BER

b. SGML for documents that are not predefined

c. TeX by Donald Knuth of MIT and LaTeX macros are widely used for typesetting, especially for documents that include mathematics

3.12.1.2.6 Recommendations. In keeping with the ongoing shift from literal page appearance to electronic transfer of document content (as exemplified by the electronic commerce and CALS programs) we recommend the use of SGML for document interchange. 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. On March 25-26, 1993, the Defense Information Systems Agency (DISA) convened a Document Interchange Symposium. The symposium featured a panel of ODA and SGML experts to deliberate on SGML/ODA issues. The panel reached the following conclusions:

a. SGML has been adopted by a wide range of government and private industry initiatives for document interchange.

b. Few commercially viable ODA products are found in the U.S. marketplace.

c. Distinctions between office and publishing documents are diminishing (making the need for unique office document architectures less acute).

d. SGML has been adopted by the publishing community.

In addition to the panel's conclusions, it should be noted that NIST has decided not to develop a FIPS for ODA. The DOD SGML standard (MIL-PRF-28001) is based on ISO 8879. MIL-HDBK-28001 for SGML is being developed.

For documents intended for distribution on the Internet, particularly the World Wide Web, HTML should be used. HTML is a document type definition (DTD) of SGML for Internet documents.

Adobe PDF is being used frequently in DOD for formatting documents where revisions are not required. However, PDF suffers by the fact that it has not yet been endorsed by an open consensus standards body. Efforts need to be taken to move PDF from the de facto, proprietary, realm to be an open standard.

3.12.1.3 Font information interchange. (This BSA appears in part 5, Data Interchange, and part 12, Multimedia.) Font information interchange standards specify the encoding of font resource information for use in document processing environments. Font interchange deals with the exchange of character fonts, such as Times Roman or Helvetica, and related information as opposed to simple exchange of character encodings, which do not include font information.

3.12.1.3.1 Standards. Table 3.12-3 presents standards for font information interchange.

TABLE 3.12-3 Font information interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Font Information Interchange, Part 1: Architecture (Corrigendum 1-1992, Corrigendum 2-1994)	9541-1:1991	Adopted (Approved)
IPC	ISO/IEC	Font Information Interchange, Part 2: Interchange Format (Corrigendum 1-1993)	9541-2:1991	Adopted (Approved)
IPC	ISO/IEC	Font Information Interchange, Part 3: Glyph Shape Representation	9541-3:1994	Adopted (Approved)
IPC	ISO/IEC	Font Information Interchange - Procedure for Registration of Glyph and Glyph Collection Identifiers	10036:1993	Informational (Approved)
GPC	NIST	Guideline for Optical Character Recognition Print Quality (adopts ANSI X3.99-1983)	FIPS PUB 90:1983	Informational (Approved)
CPN-C	Adobe	PostScript Type I - Outlines	PS Tech. Manuals	Informational (Approved)
CPN-C	Microsoft	TrueType - Outlines	TT Tech. Manuals	Informational (Approved)
IPC	ISO/IEC	Font Information Interchange, Part 4: Character Collections	9541-4	Informational (Draft)
IPC	ISO/IEC	Font Information Interchange, Part 5: Font Attributes and Character Model	9541-5	Informational (Draft)
IPC	ISO/IEC	Font Information Interchange, Part 6: Font and Character Attribute Subsets and Application	9541-6	Informational (Draft)
IPC	ISO/IEC	Font Information Interchange, Part 7: Font Interchange Format	9541-7	Informational (Draft)

3.12.1.3.2 Alternative specifications. Alternative specifications include TrueType and PostScript.

3.12.1.3.3 Standards deficiencies. There is and will be very little standardization of font names, because of copyright concerns. None of the existing font interchange standards accurately enable font substitution. However, many systems are attempting font substitution, that is, replacing a specified font with one that is similar, such as substituting TrueType Arial for PostScript Helvetica.

No standard exists for three-dimensional font families, although such text is becoming popular in display text applications, such as advertising and presentations.

3.12.1.3.4 Portability caveats. Target presentation systems and viewers may not have the required fonts to construct the called-for text in a presentation system. Font substitution may result in an unexpected text presentation. Outline font geometry also can be represented as two-dimensional graphics geometry, which eliminates the need to support a specific font on a target platform.

3.12.1.3.5 Related standards. Standards related to font information interchange standards are:

a. ISO 8632: Computer Graphics Metafile (CGM)
b. X Logical Font Description (see part 3)
c. PostScript Level 2 (starting to be used for colored text)

3.12.1.3.6 Recommendations. If CGM is being used, then ISO 8632-1 DAM 3 also is needed for font information exchange along with ISO 9541. The ISO 9541 specifies the architecture and format for various shape descriptions to be used in document processing environments that recognize Abstract Syntax Notation (ASN).1 or SGML parsing algorithms. ISO 9541 uses Adobe System's PostScript Type-I font technology and file formats. The ISO 9541 is recommended for font information exchange.

For some applications, such as view-only kiosks and presentations, convert text to a graphics format to avoid unknown font resource issues. Use fonts that are in common usage for cross-platform work.

3.12.1.4 Printer data interchange. Printer data interchange is performed by using page description languages to describe a page to be printed so the printer processor can convert the representation directly into a page image for any printer.

3.12.1.4.1 Standards. Table 3.12-4 presents standards for display text interchange.

TABLE 3.12-4 Printer data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Standard Page Description Language (SPDL)	10180:1992	Informational (Approved)
IPC	ISO/IEC	Standard for the Exchange of Product Model Data (STEP), Part 46: Integrated Generic Resources: Visual Presentation	10303-46:1994	Informational (Approved)
CPN-C	Adobe	Encapsulated PostScript Format (EPSF)	EPSF Level 1	Informational (Approved)
CPN-C	Adobe	Portable Document Format (PDF)	PDF	Informational (Approved)
IPC	ISO/IEC	Information Technology - Text and office systems - Document Printing Application (DPA) - Part 2: Protocol specification	10175-2:1996	Informational (Approved)
IPC	ISO/IEC	Information Technology - Text and office systems - Document Printing Application (DPA), Part 1: Abstract service definition and procedures	10175-1:1996	Informational (Approved)

3.12.1.4.2 Alternative specifications. The following de facto specifications are available:

a. Adobe: PostScript and Display PostScript
b. Hewlett-Packard: Hewlett-Packard Page Description Language (HPDL)
c. Xerox: Interpress

3.12.1.4.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.12.1.4.4 Portability caveats. ISO 10180, Standard Page Description Language (SPDL), combines the best of Adobe PostScript and Xerox Interpress, along with enhancements and extensions developed by ISO. However, it is not a superset of the PostScript and Interpress page description languages. The inclusion of parts of each vendor's page description, as well as the ISO extensions, render it incompatible with either PostScript or Interpress.

Although it is a proprietary standard, EPSF is widely supported for importation of display text. However, care should be taken to ensure that tools used to deliver titles support importation of EPSF. Many raster image formats are candidates for this purpose.

3.12.1.4.5 Related standards. No standards are related to page description exchange standards.

3.12.1.4.6 Recommendations. If specifying SPDL in a procurement, the specification of a converter box that converts formats such as PostScript, Interpress, or HPDL to SPDL is recommended. SPDL is a standard with no commercial following. The proprietary specifications, such as PostScript and PDF, are dominant. If used, EPSF or PDF should be considered as an

interim solution only until a public standard is available. Adobe PDF is being used frequently in DOD for formatting documents where revisions are not required. However, PDF suffers by the fact that it has not been endorsed by an open consensus standards body.

3.12.1.5 Two-dimensional graphics interchange. Two-dimensional graphics interchange standards deal with computer graphics that are represented by geometric encoding as opposed to images that are represented as bitmaps.

3.12.1.5.1 Standards. Table 3.12-5 presents multimedia standards for two-dimensional graphics interchange.

TABLE 3.12-5 Two-dimensional graphics interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Metafile for Storage/Transfer of Pictorial Description Information (CGM) (as profiled by FIPS PUB 128-1 and MIL-STD-2301)	8632-1,2,3,4:1992 (w/Amd 1&2)	Mandated (Approved)
NPC/IPC	ANSI/ISO/IEC	Programmers' Hierarchical Interactive Graphics System (PHIGS and PHIGS PLUS) (as profiled by FIPS PUB 153-1)	9592-1,2,3,4:1989 with AMD1:1992	Mandated (Approved)
IPC	ISO/IEC	Graphical Kernel System (GKS) functional description API (ANSI X3.124:1985 as profiled by FIPS PUB 120-1:1991)	7942:1985	Mandated (Approved)
CPC	MIT X Consortium	Data Stream Encoding (X Protocol)	X11R5	Informational (Approved)
CPN-C	Apple	PICT and PICT32	Apple SDK	Informational (Approved)
CPN-C	Microsoft	Windows 32-bit Graphics Device Interface (WIN32-GDI)	WIN32 Tech. Manuals	Informational (Approved)
CPN-C	Microsoft	Windows Metafile and Graphics Device Interface (WMF/GDI) (16-bit)	WMF Tech. Manuals	Informational (Approved)
CPN-C	Autodesk	Document Exchange Format (DXF)	DXF Tech. Manuals	Informational (Approved)
CPN-C	Microsoft	Visual Basic	Tech. Manuals	Informational (Approved)
CPN-C	IBM	Graphics Programming Exchange (GPE), PM 2.1	GPE Tech. Manuals	Informational (Approved)
CPN-C	IBM	GPI (API)	PM 2.1	Informational (Approved)
CPN-C	Microsoft	WIN16-GDI (API)	Windows SDK	Informational (Approved)
CPN-C	Apple	Quickdraw32 (API)	Quickdraw	Informational (Approved)

3.12.1.5.2 Alternative specifications. None.

3.12.1.5.3 Standards deficiencies. Some features are added to PHIGS implementations to compensate for perceived deficiencies in the standard.

3.12.1.5.4 Portability caveats. In 2 1/2-dimensional work where front-to-back ordering of graphical objects is important, the order may be lost when converting from an application program to an interchange format.

Most implementations of PHIGS provide extra features that are not part of the PHIGS standard and often are unnecessary for typical graphics development. These features must be avoided if possible, since unique features limit portability.

3.12.1.5.5 Related standards. The following standards are related to two-dimensional graphics interchange:

a. ISO/IEC 9593-1: PHIGS Language Bindings - Part 1: FORTRAN (Corrigendum 1:1993, 2:1994).

b. ISO/IEC 9593-2: PHIGS Language Bindings - Part 3: Ada (Amd 1 1994, Corr. 1 1993)

c. ISO/IEC 9593-4: PHIGS Language Bindings - Part 4: C (Amd 1 1994 Corr. 1 1994)

3.12.1.5.6 Recommendations. ISO 8632 CGM (MIL-PRF-28003A, MIL-STD-2301, FIPS 128-1) and PHIGS/PHIGS+ (FIPS 153, ISO 9592) are recommended. PHIGS standards should be used without nonstandard features. PHIGS supports both two- and three- dimensional graphics. GKS functionality is totally subsumed and extended by PHIGS.

3.12.1.6 Three-dimensional graphics interchange. Three-dimensional graphics are typically used for CAD/CAM and CAE applications. The interchange is used to directly convey from computer to computer the physical design and shape characteristics of an object or model. However, three-dimensional graphics are becoming more popular in many multimedia applications.

3.12.1.6.1 Standards. Table 3.12-6 presents multimedia standards for three-dimensional graphics interchange formats.

TABLE 3.12-6 Three-dimensional graphics interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC/IPC	ANSI/ISO/IEC	Programmers' Hierarchical Interactive Graphics System (PHIGS and PHIGS PLUS) (as profiled by FIPS PUB 153-1)	9592-1,2,3,4:1989 with AMD1:1992	Mandated (Approved)
GPC	NIST	Initial Graphics Exchange Specification (IGES) (adopts ASME/ANSI Y14.26M-1989) (IGES ver. 4)	FIPS PUB 177:1992	Informational (Approved)
GPC	DOD	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols	MIL-PRF-28000	Informational (Approved)
CPC	MIT X Consortium	X Consortium's PHIGS-based 3-D Extension to the X Window System (PEX)	X11R5	Informational (Approved)
CPC	MIT X Consortium	X Consortium's PHIGS-based 3-D Extension to X Window System (PEX)	X11R6	Informational (Approved)
NPC	ANSI/SAE	Initial Graphics Exchange Specification	ANSI/SAE J1881-AUG88	Informational (Approved)
CPN-C	SGI	Virtual Reality Modeling Language-- Version 1.0 Specification (VRML)	VRML v1.0 5/26/1995	Informational (Approved)
CPN-C	Pixar	Renderman - RIB (Language, API)	Tech. Manuals	Informational (Approved)
CPN-C	SGI	Graphics Language (GL) (Language, API)	Tech. Manuals	Informational (Approved)

3.12.1.6.2 Alternative specifications. None.

3.12.1.6.3 Standards deficiencies. IGES does not handle all interfaces between the data exchange specifications and external components, such as the interface between the product data specification and numerically controlled machining tools. IGES does not cover the complete life cycle of manufactured products. It addresses only the specification of products and not the manufacturing process relationships. The DOD/CALS IGES standard is preferred for engineering drawings, electronics, and numerical control. The standard is optional for technical manual illustrations.

Some features are added to PHIGS implementations to compensate for perceived deficiencies in the standard.

3.12.1.6.4 Portability caveats. Most implementations of PHIGS provide extra features that are not part of the PHIGS standard and often are unnecessary for typical graphics development. These features must be avoided if possible, since unique features limit portability.

3.12.1.6.5 Related standards. The following standards are related to three-dimensional graphics interchange:

a. ISO 8805: Graphical Kernel System for Three Dimensions (GKS-3D) functional description

b. RenderMan

c. Silicon Graphics: Graphics Language

d. Dore: Dore Reference Manual

e. ISO/IEC 9593-1: PHIGS Language Bindings - Part 1: FORTRAN (Corrigendum 1: 1993, 2:1994)

f. ISO/IEC 9593-3: PHIGS Language Bindings - Part 2: Ada (Amd 1:1994, Corr. 1:1993)

g. ISO/IEC 9593-4: PHIGS Language Bindings - Part 4: C (Amd 1: 1994, Corr. 1: 1994)

3.12.1.6.6 Recommendations. PHIGS (FIPS 153, ISO 9592) should be used as appropriate. PHIGS includes language bindings for C, FORTRAN, and Ada. PHIGS supports both two- and three- dimensional graphics. GKS-3D functionality is totally subsumed and extended by PHIGS.

3.12.1.7 Animated graphics interchange. Animated graphics include two- and three-dimensional graphics that are presented as motion sequences. The motion is generated internally by a computer system. This differs from motion images, which translate motion captured with a camera for computer display.

3.12.1.7.1 Standards. Table 3.12-7 presents multimedia standards for two- and three-dimensional animated graphics interchange.

TABLE 3.12-7 Animated graphics interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPN-C	Autodesk	Flick Files (FLI & FLC)	FLI, FLC Tech. Manuals	Informational (Approved)
CPN-C	Microsoft	Audio Video Interactive (AVI)	AVI Tech. Manuals	Informational (Approved)
CPN-C	Apple	QuickTime	QuickTime 2.5	Informational (Approved)

3.12.1.7.2 Alternative specifications. None.

3.12.1.7.3 Standards deficiencies. No IPC, NPC, or GPC standards exist for two-dimensional animated graphics. No standards exist for three-dimensional graphics.

3.12.1.7.4 Portability caveats. Exchanging animation across applications and platforms is not well supported.

3.12.1.7.5 Related standards. None.

3.12.1.7.6 Recommendations. If two-dimensional animation is required, the CPN-C standards above should be considered as interim solutions only. Autodesk Flick Files (FLI & FLC) are the only interchange files aimed solely at two-dimensional animated graphics. The two formats differ in resolution. FLI files support 320 x 200 while FLC files are resolution-dependent, although they commonly resolve to 640 x 400.

3.12.1.8 Still image interchange. Still images are images, such as photographs, that are described by bitmaps, as opposed to vector graphics which are described with geometric notation.

3.12.1.8.1 Standards. Table 3.12-8 presents multimedia standards for still image interchange.

TABLE 3.12-8 Still image interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Digital Compression and Coding of Continuous - Tone Still Images, Part 1: Requirements and Guidelines (as profiled by MIL-STD-188-198A - JPEG)	10918-1:1994	Mandated (Approved)
GPC	DOD	National Imagery Transmission Format version 2.0	MIL-STD-2500A	Mandated (Approved)
GPC	DOD	Bi-Level Image Compression for the National Imagery Transmission Format Standards (NITFS)	MIL-STD-188-196 of 6/18/1993	Mandated (Approved)
IPC	ISO/IEC	Digital Compression and Coding of Continuous-Tone Still Images - Part 2: Compliance Testing	10918-2:1993	Informational (Approved)
GPC	NIST	Standard for the Interchange of Large Format Tiled Documents	NISTIR 88-4017	Informational (Approved)
GPC	DOD	Requirements for Raster Graphics Representation in Binary Format (Group 4 Raster Scanned Images)	MIL-PRF-28002	Informational (Approved)
IPC	ISO/IEC	Progressive Bi-Level Image Compression (JBIG) Compression Algorithm for Black-and-White Images	11544 (Corrigendum 1):1995	Informational (Approved)
IPC	ISO/IEC	Image Processing and Interchange (IPI) Functional Specification, Part 3: Image Interchange Facility (IIF)	12087-3:1995	Informational (Approved)
IPC	ANSI/NPESA	Prepress Digital Data Exchange - Tag Image File Format for Image Technology (TIFF/IT)	IT8.8	Informational (Approved)
IPC	ISO/IEC	Image Processing and Interchange (IPI) Functional Specification: Part 1: Common Architecture	12087-1:1995	Informational (Approved)
IPC	ISO/IEC	Image Processing and Interchange (IPI) Functional Specification: Part 2: Programmers Imaging Kernel System API	12087-2:1994	Informational (Approved)
IPC	ISO/IEC	Image Processing and Interchange (IPI) API Language Bindings Part 4: C	12088-4:1995	Informational (Approved)
CPC	Various	Photo CD	Photo CD Tech. Manuals	Informational (Approved)
CPN-C	Adobe	PostScript Level 2	PS Tech. Manuals	Informational (Approved)
CPN-C	Adobe	Portable Document Format (PDF)	PDF	Informational (Approved)
CPN-C	CompuServe	Graphics Interchange Format (GIF)	GIF 7a and 89a	Informational (Approved)
CPN-C	ACR/NEMA	Medical Informatics Standard	Std. Pub. No. 300	Informational (Approved)
CPN-C	Aldus	Tagged Image File Format (TIFF)	TIFF v. 6.0, 1992	Informational (Approved)
CPN-C	Z-Soft	PC Paintbrush Format (PCX)	PCX Tech. Manuals	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPN-C	Microsoft	WIN16 - DIB/WMF	Win 3.1 SDK	Informational (Approved)
CPN-C	Truevision	Targa-32	Targa Tech. Manuals	Informational (Approved)
CPN-C	Microsoft	WIN16 - BMP/WMF	Win 3.1 SDK	Informational (Approved)
IPC	ISO/IEC	Digital Compression and Coding of Continuous-Tone Still Images - Part 3: Extensions	10918-3:1995	Informational (Draft)
IPC	ISO/IEC	Image Processing and Interchange (IPI) Functional Specification, Part 3: Image Interchange Facility (IIF) Amendment 1: Type Definition, Scoping, and Logical Views for Image Interchange Facility	12087-3 DAM 1:1994	Informational (Draft)
IPC	ISO/IEC	Image Processing and Interchange (IPI) API Language Bindings, Part 4: C	CD12087-4:	Informational (Draft)

3.12.1.8.2 Alternative specifications. Photo CD has five variations of CD formats announced, including one for the medical industry. Many proprietary image formats exist.

3.12.1.8.3 Standards deficiencies. Not all standards can handle the interchange of calibrated color information. Notably, RGB formats are usually unreferenced as to the colorimetric definition of pure red.

Exchanging JPEG images across different implementations can lead to slightly inconsistent images when compared one-for-one with the original. Round-off errors in internal arithmetic are not all the same.

No standard algorithm exists for the reduction of color spaces from 24 to 16 to 8 to 4 bits. Different platforms handle color degradation differently.

3.12.1.8.4 Portability caveats. Even if calibrated color is included with the image, not all applications or platforms can handle the specifications. Some low-end pre-press systems are becoming color-literate. Photo CD does handle calibrated color information.

Because approval of ISO 12087 is so recent, implementations may be limited.

Adobe PDF is being used frequently in DOD for formatting documents where revisions by the end-user are not required.

3.12.1.8.5 Related standards. The following standards and types of standards are related to still image interchange:

a. CIE Colorimetric standards

b. Various facsimile standards

c. Microsoft Resource Interchange File Format (RIFF)

d. Apple Bento container format

e. ISO 8632 (CGM)

f. NIST FIPS 158-1, X Windows, for Bitmap Distribution Format

g. X/Open C170, X Window System File Formats and Application Conventions (BDF)

h. X Consortium, Bitmap Distribution Format (BDF), v. 2.1

CGM includes support for bit-mapped images, although it is seldom used for still image interchange.

3.12.1.8.6 Recommendations. JPEG (MIL-STD-188-198A, ISO 10918) should be used for most applications involving compressed still images. Although JPEG includes lossless compression, virtually all JPEG images are created using lossy compression. This means that information is lost when the image is compressed. Source images, prior to compression, should be maintained.

JPEG supports multiple levels of lossy compression. The degree of compression influences the amount of information lost and image quality upon decompression. Compression levels should be tailored to image quality requirements. While lossy JPEG images typically display at high quality on computer monitors, the quality may be somewhat diminished on hardcopy output devices such as high-resolution color printers.

MIL-PRF-28002B should be used in a CALS environment, and when needed, supplemented by NIST IR 88-4017 (tiling). Tiling and compression are desirable for very large still images. This version (MIL-PRF-28002B) supports raster data.

If the compression scheme defined in MIL-STD-2500A is specified in a procurement, a migration strategy to JPEG should be required. MIL-STD-2500A supports ITU-T Group III compression while CALS supports Group IV only. Use the NITFS compression standards or CALS compression standard, as applicable.

ISO 11544 (JBIG) should be considered when lossless image compression of black and white images is required.

ISO/IEC 12087 is the only IPC standard for still-image APIs. This standard should be used if available implementations can meet mission requirements.

Select aspect ratios and resolutions equal to or greater than those available on target platforms, to protect against new display sizes and resolutions. Source images should be maintained for archival and reuse purposes.

3.12.1.9 Motion video interchange. Motion video interchange includes standards for motion video and associated audio. Animation (3.12.1.6) and live video-audio exchange through video teleconferencing (VTC) (3.12.5) are not included.

3.12.1.9.1 Standards. Table 3.12-9 presents multimedia standards for motion video interchange.

TABLE 3.12-9 Motion video interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Coding of Moving Pictures and Associated Audio for Digital Storage Media up to about 1.5 Mbit/sec (MPEG 1), Part 1: Systems, Part 2: Video, Part 3: Audio (with Technical Corrigendum 1:1996)	11172-1,2,3:1993	Mandated (Approved)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG2), Part 1: Systems	13818-1:1996	Mandated (Approved)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG2), Part 2: Video	13818-2:1996	Mandated (Approved)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 3: Audio	13818-3:1995 with Amd 1	Mandated (Approved)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 9: Extension for Real Time Interface for Systems Decoders	13818-9:1996	Informational (Approved)
IPC	ISO/IEC	Coding of Moving Pictures and Associated Audio for Digital Storage Media up to about 1.5 Mbit/sec (MPEG 1), Part 4: Conformance Testing	11172-4: 1995	Informational (Approved)
GPC	DOD	Military Training Programs (Video exchange)	MIL-STD-1379D of 12/5/1990	Informational (Approved)
CPC	IMA	Recommended Practices for Multimedia Portability, v.1.1 (analog video)	IMA-RP, 1990	Informational (Approved)
IPC	ITU-R	Characteristics of Television Systems - Characteristics of Systems for Monochrome and Colour Television	Report 624-4: 1990	Informational (Approved)
IPC	IEC	Phase Alternating Line (PAL) for television (analog video)	1146	Informational (Approved)
IPC	ITU-R	Encoding Parameters of Digital Television for Studios	601-2	Informational (Approved)
CPC	IMA	Recommended Practices for Multimedia Portability, v.1.2 (analog video, includes MIDI)	IMA-RP, 1993	Informational (Approved)
CPN-C	Apple	QuickTime	QuickTime 2.5	Informational (Approved)
CPN-C	Truevision	Targa-16, Targa-24	Targa-16, 24	Informational (Approved)
CPN-C	Microsoft	Video 1, RLE & Indeo, RIFF - AVI Files	Tech. Manuals	Informational (Approved)
CPN-C	Intel	Digital Video Interactive (DVI)	DVI Tech. Manuals	Informational (Approved)
CPN-C	Pioneer	Video Disc (analog video)	Tech. Manuals	Informational (Approved)
CPN-C	Microsoft	Video for Windows 1.0 API	MM SDK Tech. Manuals	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPN-C	Truevision	Targa Development 1.0 (application)	Targa Dev. 1.0 Tech. Manuals	Informational (Approved)
IPC	ISO/IEC	Coding of Moving Pictures and Associated Audio for Digital Storage Media up to about 1.5 Mbit/sec (MPEG 1), Part 5: Technical Report on Software for ISO/IEC 11172:1993	11172-5	Informational (Draft)
IPC	ISO/IEC	Generic Moding of Moving Pictures and Associated Audio Information (MPEG2) Part 4: Compliance Testing	13818-4	Emerging (Draft)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 5: Software Simulation	13818-5	Informational (Draft)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 6: Extensions for DSM-CC	13818-6	Informational (Draft)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 7: Audio Extensions	13818-7:1993	Informational (Draft)

3.12.1.9.2 Alternative specifications. None.

3.12.1.9.3 Standards deficiencies. Animation, synchronization, and degradation control are not well supported in any of the current digital-video environment.

3.12.1.9.4 Portability caveats. The ability of many platforms to display motion video is limited by platform performance. Full-screen, full-motion video usually requires special decompression hardware. Therefore, motion video, especially video that uses software decompression, should use the minimum image size and frame rate required.

NTSC is the U.S. standard for analog television resolution. PAL is a common European standard. SECAM is used in France, Eastern Europe, parts of Africa, and the Middle East.

Although MPEG 1 is rapidly emerging as the standard for computer-based motion video, especially from CD-ROM, decoding MPEG 1 at reasonable image sizes and frame rates requires special hardware assistance. Therefore, MPEG 1 should not be considered portable to legacy systems that do not include MPEG 1 decompression hardware. It is expected that many future computer systems will include MPEG 1 hardware.

MPEG 1 provides for a wide range of video resolutions and data rates but is optimized for single and double-speed CD-ROM data rates (1.2 and 2.4 Mbits/s). With 30 frames per second video at a display resolution of 352 x 240 pixels, the quality of compressed and decompressed video at this data rate is often described as similar to VHS recording. MPEG 1 is frequently used in applications with limited bandwidth, such as CD-ROM playback or Integrated Services Digital Network (ISDN) videoconferencing.

MPEG 2 is designed for the encoding, compression, and storage of studio-quality motion video and multiple CD-quality audio channels at bit rates of 4 to 6 Mbits/s. MPEG 2 has also been extended to cover HDTV.

Programming models are generally in a state of flux, especially at the operating system level. As a result, any code development will probably not port, especially if performance advantages are taken in the imaging, audio, and video areas. QuickTime and Video for Windows are currently available for both Apple System 7 and Microsoft Windows.

3.12.1.9.5 Related standards. The following standards are related to motion video:

a. ISO 10918 (JPEG)

JPEG is used for motion video in non-linear editing systems with proprietary decompression hardware. It is preferred for such systems because each frame is compressed in isolation, allowing direct access to and editing of individual frames. However, ISO 10918 does not include motion specifications.

3.12.1.9.6 Recommendations. MPEG 1 (ISO 11172) is the emerging motion video standard for computer systems and should be used for distribution to systems that include MPEG 1 decompression hardware. For distribution to legacy systems that do not include MPEG 1 hardware, software solutions, such as Microsoft Audio Video Interactive (AVI), should be considered as interim solutions.

MIL-STD-1379D should be used for interactive training delivered on level-3 laserdisc systems using the MS DOS operating system.

MPEG 2 (ISO 13818) is optimal for a variety of data rates ranging from 3 to 10 Mbits/s and higher. It is expected to be used in the cable industry's planned 500-channel systems and for the emerging Video CD technology.

Maintain original video for archival and re-use purposes.

3.12.1.10 Digital audio interchange. Digital audio, also called sampled audio, consists of information that is recorded as digital samples that are played back directly by digital-to-analog conversion.

3.12.1.10.1 Standards. Table 3.12-10 presents multimedia standards for digital audio interchange.

TABLE 3.12-10 Digital audio interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Coding of Moving Pictures and Associated Audio for Digital Storage Media up to about 1.5 Mbit/sec (MPEG 1), Part 1: Systems, Part 2: Video, Part 3: Audio (with Technical Corrigendum 1:1996)	11172-1,2,3:1993	Mandated (Approved)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 3: Audio	13818-3:1995 with Amd 1	Mandated (Approved)
IPC	ITU-T	Pulse Code Modulation (PCM) of voice frequencies (narrowband)	G.711:1989	Informational (Approved)
IPC	ITU-T	7 KHz Audio Encoding within 64 kbit/s (broadband)	G.722 (1989)	Informational (Approved)
IPC	ITU-T	Extensions of G.721 to 24 and 40 kbit/s for Digital Circuit Multiplication Equipment Application	G.723 (1989)	Informational (Approved)
IPC	ITU-T	40, 32, 24, and 16 kbit/s Adaptive Digital Pulse Code Modulation (ADPCM)	G.726 (1990)	Informational (Approved)
IPC	ITU-T	Coding of Speech at 16 kbit/s using Low-Delay Code Excited Linear Prediction (LD-CELP).	G.728:1992	Informational (Approved)
CPC	IMA	Recommended Practices for Multimedia Portability, v.1.2 (analog video, includes MIDI)	IMA-RP, 1993	Informational (Approved)
CPC	IMA	Recommended Practices for Enhancing Digital Audio Compatibility in Multimedia Systems	IMA RP, 1992	Informational (Approved)
CPN-C	OMF	Audio Interchange File Format, Audio Interchange File Format Compressed (AIFF/AIFC)	AIFF (EA IFF 85)	Informational (Approved)
CPN-C	Microsoft	Resource Interchange File Format - Wave Form Audio (RIFF WAVE) v.1.0	RIFF Tech. Manuals	Informational (Approved)
CPN-C	Creative Labs	SoundBlaster Creative Voice File Format (VOC)	VOC Tech. Manuals	Informational (Approved)
CPN-C	Apple	Pulse Code Modulation (PCM) 11.025 kHz, 8-bit, linear	AIFF Version 1 (also IMA RP)	Informational (Approved)
CPN-C	Apple	Pulse Code Modulation (PCM) 22.05 kHz, 8-bit, linear	AIFF Version 1, (also IMA RP)	Informational (Approved)
CPC	Various	Pulse Code Modulation (PCM) 44.1 kHz, 16-bit, linear CD-DA (music CDs)	Red Book, 1980 (also IMA RP)	Informational (Approved)
CPN-C	Intel	Adaptive Differential Pulse Code Modulation (ADPCM) 8-, 11.025-, 22.05-, 44.10-kHz, 4-bit	DCI Documents (also IMA RP)	Informational (Approved)
CPC	Various	Adaptive Differential Pulse Code Modulation (ADPCM) 17-kHz, 4-bit CD-XA (Extended Architecture)	XA level B	Informational (Approved)
CPC	Various	Adaptive Differential Pulse Code Modulation (ADPCM) 8.5-kHz, 4-bit CD-XA (Extended Architecture)	XA level C	Informational (Approved)

3.12.1.10.2 Alternative specifications. Many popular sound cards support other formats, such as 2- and 4-bit PCM.

3.12.1.10.3 Standards deficiencies. No uniform timing information is carried with most audio interchange formats. Thus synchronization of multiple audio streams is inherently difficult. Also, sound clips may have to be retimed to SMPTE time codes when producing broadcast video output.

3.12.1.10.4 Portability caveats. Apple sampling rates deviate slightly from the values given in the table because of internal clock rates. Therefore, mixing of audio played back from two different platform types is difficult. This is true even among the same kinds of platforms because CPU clocks and sampling clocks on sound boards can vary widely.

The IMA's Recommended Practices for Enhancing Digital Audio Compatibility in Multimedia Systems is a set of audio formats that are guaranteed to be supported on any IMA audio-compliant platform. These formats are required to provide baseline digital audio cross-platform support to satisfy a range of audio quality and data bandwidth requirements. Although the recommended practice has gained industry support, many manufacturers use proprietary ADPCM compression algorithms.

SoundBlaster VOC format is used mainly in Microsoft MS-DOS applications. This is the dominant de facto standard for such applications.

3.12.1.10.5 Related standards. The following standards are related to digital audio interchange standards.

a. Microsoft AVI
b. Apple QuickTime 1.5
c. Apple Bento container format

3.12.1.10.6 Recommendations. MPEG 1 audio is not a single compression algorithm but a family of three audio encoding and compression schemes called MPEG-Audio Layer-2, and Layer-3, all three of which are hierarchically compatible. The audio compression schemes are lossy, but they can achieve perceptually lossless quality.

MPEG 2 audio is intended to encode up to five full bandwidth channels and additional low-frequency enhancement channel, and up to seven commentary or multilingual channels.

Procurements concerned with digital audio should proceed with care. Many important standards for digital audio are proprietary standards.

3.12.1.11 Encoded audio interchange. Encoded audio consists of audio that is described by a language that is interpreted on playback. Encoded audio is typically used for synthesized music.

3.12.1.11.1 Standards. Table 3.12-11 presents multimedia standards for encoded audio interchange.

TABLE 3.12-11 Encoded audio interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	IMA	Musical Instrument Digital Interface (MIDI)	MIDI 1.0	Informational (Approved)
CPC	IMA	MIDI Time Code and Cueing (supplement to MIDI 1.0)	MIDI supplement	Informational (Approved)
CPC	IMA	Recommended Practices for Multimedia Portability, v.1.2 (analog video, includes MIDI)	IMA-RP, 1993	Informational (Approved)
CPC	VESA	Audio Interface (VBE/AI) Standard 1.0 API	VESA 1994	Informational (Approved)
CPN-C	Creative Labs	SoundBlaster SBK (API)	SoundBlaster Tech. Manuals	Informational (Approved)
CPN-C	Microsoft	Multimedia Control Interface (MCI) API	MCI API 1.0	Informational (Approved)
IPC	ISO/IEC	Standard Music Description Language (SMDL) (An SGML and HyTime application)	10743:1995	Informational (Draft)

3.12.1.11.2 Alternative specifications. None

3.12.1.11.3 Standards deficiencies. No IPC, NPC, or GPC standards exist for encoded audio. Synchronization and degradation control are not well supported in any of the current environments.

3.12.1.11.4 Portability caveats. Programming models are generally in a state of flux, especially at the operating system level. As a result, any code development will probably not port, especially if performance advantages are taken in the imaging, audio, and video areas.

3.12.1.11.5 Related standards. None.

3.12.1.11.6 Recommendations. Although MIDI is a CPC standard, it is widely supported by industry. Given the near universal support for MIDI, it is unlikely that an alternative will make inroads unless the underlying technology changes. If synthesized music or sound effects are needed, MIDI is recommended as an interim solution until an IPC, NPC, or GPC standard is available.

Maintain original audio for archival and re-use purposes.

3.12.2 Multimedia programming systems. A programming system is defined to be an application or platform that is intended to encompass all the necessary support to produce or playback a broad range of multimedia titles.

3.12.2.1 Programming platforms. Programming platforms are computer systems designed to include necessary facilities for developing and displaying multimedia titles.

3.12.2.1.1 Standards. Table 3.12-12 presents standards for programming platforms.

TABLE 3.12-12 Programming platforms standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	MPC Working Group	Multimedia Personal Computer (MPC) III	MPC3, 1995	Informational (Approved)
CPC	MPC Working Group	Multimedia Personal Computer (MPC) II	MPC2, 1993	Informational (Approved)
CPC	MPC Working Group	Multimedia Personal Computer (MPC)	MPC, 1991	Informational (Approved)
CPN-C	Apple	QuickTime	QuickTime 2.5	Informational (Approved)
CPN-C	Philips	Compact Disc Interactive (CD-I)	Green Book, 1987	Informational (Approved)

3.12.2.1.2 Alternative specifications. Available alternative solutions include various proprietary computer platforms, such as Silicon Graphics development computers.

3.12.2.1.3 Standards deficiencies. No IPC, GPC, or NPC standards exist for the specification of multimedia programming platforms.

The original MPC specification is insufficient for most modern multimedia applications.

All systems are struggling with synchronization accuracy and control of digital data streams, both from the specification and implementation points of view.

Some platform specifications are minimal and too incomplete to guarantee interoperability or portability. Little certification work is underway to guarantee compliance to any of these.

3.12.2.1.4 Portability caveats. Byte alignment of native data types can be a problem when moving between platforms.

3.12.2.1.5 Related standards. None.

3.12.2.1.6 Recommendations. Platforms should be tailored to mission needs. CD-I, which is aimed at the consumer market, is not recommended.

3.12.2.2 Authoring languages. Authoring languages are languages that are specifically designed for the development of multimedia applications and tools. They may be interpreted or compiled on target platforms.

3.12.2.2.1 Standards. Table 3.12-13 presents standards for authoring languages.

TABLE 3.12-13 Authoring languages standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Hypermedia/Time-Based Structuring Language (HyTime)	10744:1992	Informational (Approved)
CPN-C	MacroMedia	MMLingo	MMLingo Tech. Manuals	Informational (Approved)
CPN-C	Sybase/Gain	Gain Extension Language (GEL)	GEL v.2.1	Informational (Approved)

3.12.2.2.2 Alternative specifications. Other authoring and scripting languages are available. Many full-featured commercial authoring systems are available, some of which support multiple platforms.

3.12.2.2.3 Standards deficiencies. Deficiencies in the existing specifications are unknown.

3.12.2.2.4 Portability caveats. Portability problems with the existing specifications are unknown.

3.12.2.2.5 Related standards. None.

3.12.2.2.6 Recommendations. HyTime (ISO 10744) is the only IPC standard available for multimedia authoring languages. It should be used if suitable for specific title development.

3.12.2.3 Interchange media. Interchange media are designed to deliver finished multimedia titles to a broad range of platforms.

3.12.2.3.1 Standards. Table 3.12-14 presents standards for supporting interchange between platforms.

TABLE 3.12-14 Interchange media standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Data Interchange on Read-Only 120mm Optical Data Disks (CD-ROM) (see ECMA 130-1988)	10149:1995	Adopted (Approved)
IPC	ISO/IEC	Volume and File structure of CD-ROM for Information Interchange (same as ECMA 119)	9660:1988	Adopted (Approved)
GPC	DOD (DISA)	Department of Defense Handbook, DOD-Produced CD-ROM Products, 1st Revision	MIL-HDBK-9660A (1996)	Informational (Approved)
IPC	ECMA	Data Interchange on Read-Only 120 mm Optical Data Disks (CD-ROM)	130 (1988)	Informational (Approved)
CPC	IMA	Recommended Practice for Data Exchange (adopts Bento and an OMFI subset)	IMA-RP, 950701.1	Informational (Approved)
CPC	Various	UNIPACK (format interface)	P18.01-DO.141 (5/93)	Informational (Approved)
IPC	ISO/IEC	Coding of Multimedia and Hypermedia Information - Part 1: MHEG objects representation - base notation (ASN.1), Part 4: Registration procedure for MHEG format identifier	13522-1,4:1995	Informational (Approved)
CPC	Various	CD-Rom standard	Yellow Book, 1984	Informational (Approved)
CPN-C	Microsoft	CD-XA (Extended Architecture) (media interface for interchange)	CD-XA, 1986	Informational (Approved)
CPN-C	Apple	CD-WO (Write Once) (media interface for interchange)	Orange Book, 1993	Informational (Approved)
CPN-C	Apple	Bento (Format and API)	1.0d5, 1992	Informational (Approved)
CPN-C	Avid	Open Media Framework Interchange (OMFI) format and API	OMFI, V. 1.0, 1993	Informational (Approved)
CPC	Various	Digital Video Disk (DVD)	DVD	Informational (Approved)
CPC	Various	High Density Compact Disc, System Description v 0.5 (MM-CD)	Gold Book, 1995	Informational (Draft)
CPC	Various	Super Disk (SD)	SD	Informational (Draft)
CPC	X/Open	CD-ROM Support Component (XCDR)	P120:5/91	Informational (Superseded)

3.12.2.3.2 Alternative specifications. No other specifications are available.

3.12.2.3.3 Standards deficiencies. ISO 9660 does not support long filenames such as those used on UNIX systems.

3.12.2.3.4 Portability caveats. The IMA Recommended Practice for Data Exchange has only recently been published. Therefore, it is not yet broadly supported. It is designed to be a platform- and content-neutral recommendation for the exchange of multimedia data for content and title developers.

3.12.2.3.5 Related standards. The following standards are related to CD-ROM:

a. CD-R is a standard and technology that allows a user to write to and read from a Compact Disc.

b. CD-ROM is a compact disc format used to hold text, graphics, and stereo sound.

c. CD-ROM/XA is a CD-ROM enhancement that allows audio to be interleaved with data. It also functions as a bridge between CD-ROM and CD-I, since CD-ROM/XA discs will play on a CD-I player. CD-ROM/XA uses a standard CD-ROM player, but requires a CD-ROM/XA controller card in the computer. Although it is not a video specification limited video can be included on disc. To use it, you must have a drive that reads the audio portions of the disc and an audio card in your computer that translates the digital data into sound. Not all drives can recognize the extensions.

d. CD-Video (CD-V) is a format for putting five minutes of video on a three-inch disc.

e. CD-WO is a CD-ROM version of the WORM technology. CD-WO discs conform to ISO 9660 standards and can be played in CD-ROM drives.

3.12.2.3.6 Recommendations. ISO 9660 and 10149 should be used for all CD-ROM applications. ISO 9660 describes the logical structure of information on a CD. ISO 10149 describes the physical structure of the CD. In addition, DISA's Department of Defense CD-ROM Requirements and Guidelines, which gives DOD labeling and security requirements along with other information, should be followed.

MHEG (ISO 13522) will define an interchange format for real-time multimedia information interchange. Its goals are platform independent interchange of interactive multimedia content, robust time-space composition and synchronization, real-time interchange, and incorporation of arbitrary monomedia formats.

Use of high-capacity compact discs (MM-CD and SD) should be avoided until a single standard has been agreed upon. Even after agreement, use should be considered carefully because portability will not be available for legacy systems that do not support these discs. An agreement to produce a single standard was announced at the time of this writing.

3.12.3 Multimedia presentation. Presentation standards deal directly with representational issues of information and output devices that convert digital information to human information. Graphical user interfaces are covered in detail in part 3 of the ITSG and are not included here.

3.12.3.1 Text presentation. Text presentation deals with displaying formatted text and documents to appear to the viewer in the way the author intended. It includes both the layout and typeface of the text.

3.12.3.1.1 Standards. Table 3.12-15 presents standards for text presentation.

TABLE 3.12-15 Text presentation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Standard Page Description Language (SPDL)	10180:1992	Informational (Approved)
IPC	ISO/IEC	Documentation Style Semantics and Specification Language (DSSSL)	10179:1995	Informational (Approved)
CPN-C	Adobe	Portable Document Format (PDF)	PDF	Informational (Approved)
CPN-C	Adobe	PostScript Type I - Outlines	PS Tech. Manuals	Informational (Approved)
CPN-C	Microsoft	TrueType - Outlines	TT Tech. Manuals	Informational (Approved)

3.12.3.1.2 Alternative specifications. Viewers are available for some commercial applications, such as Microsoft Word and FrameMaker.

3.12.3.1.3 Standards deficiencies. No approved public standards exist for text presentation.

3.12.3.1.4 Portability caveats. TrueType is limited to Microsoft Windows.

3.12.3.1.5 Related standards. HTML is related to text presentation.

3.12.3.1.6 Recommendations. SPDL deals with text presentation. These standards add formatting information to SGML for the presentation of electronic documents. Adobe PDF supports interchange of documents including graphics among Apple, IBM PC, and UNIX systems. A document is simply printed to Acrobat, which produces an interchange file. The Acrobat reader is available at no charge. Adobe Acrobat should be considered as an interim solution. PDF is used frequently but suffers by the fact that it has not been endorsed by an open consensus standards body. Efforts need to be taken to move PDF from the de facto, proprietary, realm to be an open standard.

HTML is a DTD of SGML. It does not as rigidly define the appearance of HTML-tagged documents as does SPDL or PDF.

3.12.3.2 Graphics presentation. Graphics presentation standards deal with interfaces to graphics display devices and environments for the presentation of graphics and related multimedia objects. Note that in this instance, graphics presentation includes raster and vector graphics.

3.12.3.2.1 Standards. Table 3.12-16 presents standards for graphics presentation.

TABLE 3.12-16 Graphics presentation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	VESA	VESA BIOS 2.0 (SVGA and audio command interface)	VESA 1994	Informational (Approved)
CPN-C	IBM	CGA/EGA Graphics (command interface)	CGA/EGA 1991	Informational (Approved)
CPN-C	IBM	VGA Graphics (command interface)	VGA 1992	Informational (Approved)
CPN-C	Apple	PICT and PICT32	Apple SDK	Informational (Approved)
CPN-C	IBM	XGA Graphics (command interface)	IBM Tech. Report	Informational (Approved)
IPC	ISO	Computer Graphics and Image Processing - Presentation Environment for Multimedia Objects (PREMO)	None	Informational (Draft)

3.12.3.2.2 Alternative specifications. None.

3.12.3.2.3 Standards deficiencies. No approved IPC, GPC, or NPC standards exist for graphics presentation. Strict adherence to correct presentation and output standards will require color calibration equipment.

3.12.3.2.4 Portability caveats. Graphics portability is generally achieved by data interchange, not by uniform cross-platform display standards. Source material may be visually impaired through use of low quality displays. Vector and raster graphics that require high resolutions and large color spaces will be less portable.

3.12.3.2.5 Related standards. None.

3.12.3.2.6 Recommendations. There is no recommendation at this time.

3.12.3.3 Color definition. (This BSA appears in part 5, Data Interchange, part 12, Multimedia, and part 13, Human Factors.) Color definition deals with establishing a reference base for identifying colors to aid in the matching and exchange of color. Color definition standards apply to defining color in general, and not only to color definition for information technology systems.

3.12.3.3.1 Standard. Table 3.12-17 presents standards for color definition.

TABLE 3.12-17 Color definition standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ASTM	Standard Test Method for Computing the Colors of Objects by Using the CIE System	E308 (1990)	Informational (Approved)
NPC	EIA	1976 CIE-UCS Chromaticity Diagram with Color Boundaries	TEB26 (1988)	Informational (Approved)
IPC	ISO	CIE Standard Colorimetric Illuminants	CIE 10526 (1991)	Informational (Approved)
IPC	ISO	CIE Standard Colorimetric Observers	CIE 10527 (1991)	Informational (Approved)
IPC	CIE	Recommendations on Uniform Color Spaces, Color-Difference Equations, and Psychrometric Color Terms	CIE Pub. 15, Suppl. 2 (1986)	Informational (Approved)
NPC	NPESA	Graphic Technology - Input Data for Characterization of 4-Color Process Printing	IT8.7/3 (1993)	Informational (Approved)
NPC	NPESA	Graphic Arts Prepress Definition of Default RGB Data for Use in the Graphic Arts Industry	IT8.7/4	Informational (Approved)
N/A	SMPTE/EIA/VESA/ISO	Unreferenced 24-bit RGB	Technical Reports	Informational (Approved)
IPC	ISO/IEC	Text and Office Systems Colour Architecture (TOSCA)	JTC1/SC18/WG5	Informational (Draft)
CPC	ICC	Definition of Named Color	TBD	Informational (Formative)
NPC	ANSI IT8 and CGATS	Specifications for Web Offset Publications (SWOP)	TBD	Informational (Formative)

The CIE (International Commission on Illumination) is the principal international standards writing body for agreements for color, vision, and illumination. Under ANSI, four bodies work on color-related standards. ANSI X3 works on office document automation and information systems. ANSI IT8/CGATS is concerned with graphic arts. ASTM deals with color metrology and standard practices, and SMPTE handles standards for color television and color monitors.

ANSI's Committee for Graphic Arts Technology Standards (CGATS) has eight subcommittees working on topics such as materials handling, process control, and color data definition. NPESA is the National Printing Equipment and Supply Association.

3.12.3.3.2 Alternative specification. The following alternative specifications are also available:

a. Pantone Matching System

b. RGB (Red, Green, Blue) - the method directly used by color video display terminals

c. CMYK (Cyan, Magenta, Yellow, Black) - used in four color printing

d. HSV (Hue, Saturation, V.)

e. HSL (Hue, Saturation, Luminescence)

f. HVC

g. SWOP (Specifications for Web Offset Publications)

h. HSB (Hue, Saturation, Brightness)

i. TIFF (Tag Image File Format)

3.12.3.3.3 Standard deficiencies. Comparison of color defined by the existing standards assumes identical viewing conditions. There are no standards directly addressing comparisons across viewing environments, although models are being worked on. Strict adherence to correct presentation and output standards will require color calibration equipment.

3.12.3.3.4 Portability caveats. Translation of color from one color definition system to another can be difficult and is only an approximation at best. There are three different color definitions from the CIE. They are the CIEXYZ tristimulus values, and the CIELAB and CIELUV color spaces. These standards have existed for a long time and are seen as the common basis for any future unifying definitions.

There are also the problems of color matching. For example, of 1012 Pantone colors for coated paper, 70 cannot be reproduced in the CMYK definition. CIEXYZ is useful in comparing colors under identical viewing conditions. CIEXYZ has a rigorous definition and by itself does not necessarily constitute a complete color specification. CIEXYZ is a standardized set of primaries which are not physically realizable but can match all possible colors with entirely positive tristimulus values. A new form of color definition is emerging, known as high-fidelity color. The idea behind high-fidelity color is the use of five to seven different colors in the printing process to widen the range of colors that can be printed. Two such models that have appeared are the Kumper set which increases the number of printed colors in the blue region by 80%, and the VSF model which provides better performance in deep red and green colors. These processes are very non-standard and should be avoided at present.

Common systems typically do not support colorimetric calibration.

3.12.3.3.5 Related standards. The following types of standards are related to standards for the definition of color:

a. color matching standards
b. color data exchange standards
c. color use standards
d. style guide standards

3.12.3.3.6 Recommendations. The approved standards in this section are recommended where they are applicable. Maintain original copies of source material so that revisions can be produced for next generation systems that will allow the inclusion of calibration information.

3.12.3.4 Audio presentation. Audio presentation standards deal with interfaces for audio playback.

3.12.3.4.1 Standards. Table 3.12-18 presents standards for audio presentation.

TABLE 3.12-18 Audio presentation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	VESA	VESA BIOS 2.0 (SVGA and audio command interface)	VESA 1994	Informational (Approved)
CPC	Various	Pulse Code Modulation (PCM) 44.1 kHz, 16-bit, linear CD-DA (music CDs)	Red Book, 1980 (also IMA RP)	Informational (Approved)
CPN-C	Apple	Pulse Code Modulation (PCM) 22.05 kHz, 8-bit, linear	AIFF Version 1, (also IMA RP)	Informational (Approved)
CPN-C	Creative Labs	SoundBlaster SBK (API)	SoundBlaster Tech. Manuals	Informational (Approved)

3.12.3.4.2 Alternative specifications. None.

3.12.3.4.3 Standards deficiencies. No IPC, GPC, or NPC standards exist for audio presentation. Strict adherence to correct display and output standards will require audio calibration equipment.

3.12.3.4.4 Portability caveats. Source material may be aurally impaired through use of low-quality amplifiers and speakers. Calibration information that allows a user to correctly set audio levels at the beginning of a title can substantially enhance a presentation.

3.12.3.4.5 Related standards. None.

3.12.3.4.6 Recommendations. Maintain original copies of source materials for re-use when IPC, GPC, and NPC standards become available.

3.12.3.5 Monitors. Monitor standards specify the electrical and display characteristics of computer and television monitors.

3.12.3.5.1 Standards. Table 3.12-19 presents standards for monitors.

TABLE 3.12-19 Monitors standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ITU-R	Characteristics of Television Systems - Characteristics of Systems for Monochrome and Colour Television	Report 624-4: 1990	Informational (Approved)
IPC	IEC	Phase Alternating Line (PAL) for television (analog video)	1146	Informational (Approved)
CPC	VESA	Monitor Timing Standard for 800 x 600 72Hz and 1024 x 768 70Hz refresh rate	VESA 1993	Informational (Approved)
CPC	VESA	Monitor Timing Manufacturing Guideline for 1024 x 768 with 60 Hz, 800x600 with 60Hz, 800x600 with 56Hz refresh rate	VESA 1993	Informational (Approved)
CPC	NTSC	15.73425kHz Scan Specification (TV Monitor)	NTSC-YIQ Standard (19[illegible]0)	Informational (Approved)
NPC	SMPTE	Studio Monitor Specification (Phosphor Interface)	SMPTE C, D60, D65	Informational (Approved)
NPC	SMPTE	Basic parameter values for the HDTV standard for the studio and for international programme exchange	Rec. 709	Informational (Approved)
NPC	SMPTE	Television - Signal Parameters -1125/60 High-Definition Production System (TV monitor)	SMPTE Standard 240M, 1988	Informational (Approved)
NPC	SMPTE	Television - Digital Representation and Bit-Parallel Interface - 1125/60 High-Definition Production System (TV monitor)	SMPTE Standard 260M, 1992	Informational (Approved)

3.12.3.5.2 Alternative specifications. None.

3.12.3.5.3 Standards deficiencies. Strict adherence to correct display and output standards will require audio and color calibration equipment.

3.12.3.5.4 Portability caveats. Source material may be visually impaired through use of low quality monitors. Calibration information that allows a user to correctly set monitor levels at the beginning of a title can substantially enhance a presentation.

3.12.3.5.5 Related standards. None.

3.12.3.5.6 Recommendations. Use the established standards given above for computer and television monitors. Avoid development for high-definition television, which is now a formative technology.

3.12.3.6 Embedded time codes. Embedded time codes provide timing information within data streams. They are necessary for proper synchronization in the presentation of multimedia.

3.12.3.6.1 Standards. Table 3.12-20 presents standards for embedded time codes.

TABLE 3.12-20 Embedded time codes standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	SMPTE	Television, Audio, and Film - Storage and Transmission of Data - Binary Groups of Time and Control Codes	262M	Informational (Approved)

3.12.3.6.2 Alternative specifications. Proprietary timing and synchronization control codes are used in some environments.

3.12.3.6.3 Standards deficiencies. None.

3.12.3.6.4 Portability caveats. None.

3.12.3.6.5 Waivered standards. None.

3.12.3.6.6 Recommendations. Use SMPTE 262M.

3.12.4 Video and audiographic teleconferencing. Video teleconferencing is the live transmission of audio and video over a network among two or more users. Audiographic teleconferencing (AGT) lets conference participants manipulate documents and other data collectively with accompanying real-time audio. Many VTC and AGT standards deal with audio/video network services. Only those standards directly related to multimedia data formats are presented below. Transmission protocols, transfer protocols, and security standards are not included.

3.12.4.1 Video and audiographic teleconferencing.

3.12.4.1.1 Standard. Table 3.12-21 presents standards for video and audiographic teleconferencing.

TABLE 3.12-21 Video and audiographic teleconferencing standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Industry Profile for Video Teleconferencing	VTC001, Revision 1, April 25, 1995	Mandated (Approved)
IPC	ITU-T	Terminal for Low Bit Rate Multimedia Communications, March 19, 1996	H.324	Mandated (Approved)
GPC	NIST	Video Teleconferencing Services at 56 to 1, 920 KB/s (adopts CCITT H.221, H.230, H.242, H.261, and H.320 (all 1990))	FIPS PUB 178:1992	Informational (Approved)
IPC	ITU-T	Pulse Code Modulation (PCM) of voice frequencies (narrowband)	G.711:1989	Informational (Approved)
IPC	ITU-T	Transmission performance characteristics of pulse code modulation	G.712 (1992)	Informational (Approved)
IPC	ITU-T	7 KHz Audio Encoding within 64 kbit/s (broadband)	G.722 (1989)	Informational (Approved)
IPC	ITU-T	Extensions of G.721 to 24 and 40 kbit/s for Digital Circuit Multiplication Equipment Application	G.723 (1989)	Informational (Approved)
IPC	ITU-T	System Aspects of the Use of 7 kHz Audio Codec Within 64 kbit/s	G.725 (1989)	Informational (Approved)
IPC	ITU-T	40, 32, 24, and 16 kbit/s Adaptive Digital Pulse Code Modulation (ADPCM)	G.726 (1990)	Informational (Approved)
IPC	ITU-T	Extensions of Recommendation G.726 on 40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation for use with uniform-quantized input and output	G.726A (1994)	Informational (Approved)
IPC	ITU-T	5, 4, 3, and 2 bits Sample Embedded ADPCM	G.727 (1990)	Informational (Approved)
IPC	ITU-T	Extensions of Recommendation G.727 on 5-, 4-, 3- and 2-bits/sample embedded Adaptive Differential Pulse Code Modulation for use with uniform-quantized input and output	G.727A (1994)	Informational (Approved)
IPC	ITU-T	Coding of Speech at 16 kbits/s using Low-Delay Code Excited Linear Prediction (LD-CELP).	G.728:1992	Informational (Approved)
IPC	ITU-T	Codecs for videoconferencing using primary digital group transmission	H.120	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ITU-T	Video Codec for Audiovisual Services at p x 64 kbit/s - Line Transmission on Non-Telephone Signals (known as PX64)	H.261 (1993)	Informational (Approved)
IPC	ITU-T	Coded Representation of Picture and Audio Information - Progressive Bi-Level Image Compression - Terminal Equipment and Protocols for Telematic Services	T.82 (1993)	Informational (Approved)
IPC	ITU-T	Information Technology - digital compression and coding of continuous-tone still images: compliance testing	T.83	Informational (Approved)
IPC	ITU-T	Binary File Transfer Format for the Telematic Services: Terminal Equipment and Protocols for Telematic Services	T.434 (1992)	Informational (Approved)
IPC	ITU-T	Transmission protocols for multimedia data	T.120	Informational (Approved)
IPC	ITU-T	VTC over ATM	H.321	Emerging (Approved)
IPC	ITU-T	VTC over Ethernet	H.323	Emerging (Approved)
GPC	NIST	Video Teleconferencing Services at 56 to 1920 kb/s (Adopts ITU H.320, H.221, H.242, H.230, H.261, H.231, H.243, H.253, H.234, H.244)	FIPS PUB 178-1	Informational (Draft)
IPC	ITU-T	Dual Rate Speech Coder for Multimedia Communications Transmitting at 5.3 and 6.3 kbits/s	G.723	Informational (Draft)
IPC	ITU-T	Information Technology - Generic Coding of Moving Pictures and Associated Audio Information, Part 2: Video (adopts ISO/IEC 13818-2)	H.262	Informational (Draft)
IPC	ITU-T	Video coding for low bitrate communications	H.263	Informational (Draft)
IPC	ISO/IEC	Generic Moding of Moving Pictures and Associated Audio Information (MPEG2) Part 4: Compliance Testing	13818-4	Emerging (Draft)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 5: Software Simulation	13818-5	Informational (Draft)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 6: Extensions for DSM-CC	13818-6	Informational (Draft)
IPC	ISO/IEC	Generic Coding of Moving Pictures and Associated Audio Information (MPEG 2), Part 7: Audio Extensions	13818-7:1993	Informational (Draft)
GPC	DOD	Interoperability and Performance Standard for VTC (superseded by COS VTC001-Rev.1)	MIL-STD-188-331 and 331-A	Informational (Superseded)

3.12.4.1.2 Alternative specification. ISO and the ATM Forum are working on standards for high-bandwidth teleconferencing, especially over ATM networks.

3.12.4.1.3 Standard deficiencies. None of the ITU teleconferencing standards work well over Ethernet and TCP/IP networks because of bandwidth limitations.

3.12.4.1.4 Portability caveats. Portability problems with the existing standards are unknown.

3.12.4.1.5 Related standards. MPEG1 (ISO/IEC 11172) and MPEG2 (ISO/IEC 13818) are related to video and audiographic teleconferencing. Various ITU H, G, and T series standards are related to architecture, equipment, transmission protocols, transfer protocols, and security.

3.12.4.1.6 Recommendations. MIL-STD-188-331 and MIL-STD-188-331A have been superceded by the Industry Profile for Video Teleconferencing, VTC001-Rev. 1, which is mandated for DOD by the OASD. Because of differences in network bandwidths and transmission limitations, video and audio standards should be chosen to fit individual VTC system capabilities. For example, ITU G.711 should be used for narrow-band speech, while G.722 should be used for wide-band speech. FIPS PUB 178-1 will replace the VTC001 profile, but is still in draft at this writing.

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 13 of 14 parts)

HUMAN FACTORS SERVICES

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

TABLE OF CONTENTS

LIST OF TABLES

3.13 Human Factors. Human factors (ergonomics) is the science of determining proper relations between computer systems and the user. Ease of use, comfort, health, and safety are primary concerns (e.g., how a keyboard should be laid out). An ergonomically-designed product implies that the device blends smoothly with the user's body or actions. For computing systems, these standards provide guidelines and requirements for the design of computer hardware, software user interfaces, and computing environments.

3.13.1 Human factors for computer hardware. Human factors requirements for computer hardware concern the user's physical interface through input devices and displays and how well it serves the needs of the user. Health and safety concerns are also addressed.

3.13.1.1 Human factors for video display terminals. (This BSA appears in both part 3, User Interface, and part 13, Human Factors.) This base service area addresses the human factors requirements for all types of video displays, and includes safety concerns.

3.13.1.1.1 Standards. Table 3.13-1 presents human factors standards for video display terminals.

TABLE 3.13-1 Human factors for video display terminals standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) Part 1: Introduction	9241-1:1992	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) Part 2: Task Requirements	9241-2: 1992	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) Part 3: Visual Display Requirements	9241-3:1992	Informational (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
GPC	DOD	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	MIL-STD-1472D Notice 2, 30 June 1992	Informational (Approved)
IPC	ECMA	Ergonomics - Requirements for Non-CRT (Cathode Ray Tube) Visual Display Units	136 (1989)	Informational (Approved)
IPC	ISO	Ergonomic Principles in the Design of Work Systems	6385:1981	Informational (Approved)
NPC	ANSI/AIIM	Electronic Imaging Output Displays	TR19-1993	Informational (Approved)
CPC	NSC	Guide to Working Safely with Computers - Manual (relates to VDTs)	13068-0000	Informational (Approved)
IPC	ECMA	Procedure for Measurement of Emissions of Electric and Magnetic Fields from VDUs from 5 Hz to 400 kHz	172 (1992)	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 8: Requirements for display of colors	9241-8	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 7: Display requirements with reflections	9241-7	Informational (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)

DOD Instruction (DODI) 8120 mandates use of the DOD HCI Style Guide.

AIIM is the Association for Image and Information Management.
ECMA is the European Computer Manufacturers' Association.
HFS is the Human Factors Society.
NSC is the National Safety Council.

ISO 9241-1 presents an overview of the content and usage of the multipart ISO 9241 standard. A revised version of ISO 9241-1 is currently at the Committee Draft (CD) level and will soon be released for Draft International Standard (DIS) ballot. ISO 9241-2 presents an overview of factors that should be considered when designing tasks to be performed in a specific computing environment.

3.13.1.1.2 Alternative specifications. There are no alternative specifications available.

3.13.1.1.3 Standards deficiencies. The performance-based test described in ISO 9241-3 adequately discriminates between a display that meets the physical requirements of the standard and one that does not. However, timing scores may be badly affected by the effects of testing practice. Changes to the test method and metrics are under consideration. ISO 9241-3 does not adequately address flat panel displays. ISO 13406 is intended to remedy this situation.

3.13.1.1.4 Portability caveats. No portability problems are known with the above specifications.

3.13.1.1.5 Related standards. The following standards are related to human factors standards for video display terminals:

a. ISO CD 10075-2, Ergonomic principles related to mental work load, Part 2: Design Principles, gives guidance on the design of work systems in general, with the intention of providing optimal working conditions with respect to health and safety, well-being, performance, and effectiveness.

b. MIL-STD-1908 (1992) Definition of Human Factors Terms.

c. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

d. MIL-STD-1800A (1990) Human Engineering Performance Requirements for Systems (Air Force published, but rarely used, duplicates MIL-STD-1472).

e. MIL-HDBK-759B(2) (1993) Human Factors Engineering Design for Army Materiel. (Draft 759C is complete.)

f. MIL-HDBK-761A(1989) Human Engineering Guidelines for Management Information Systems.

g. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

h. DOD-HDBK-743A (1991) Anthropometry of U.S. Military Personnel.

i. ITU-T E.134 Human Factors Aspects of Public Terminals: Generic Operating Procedures.

j. An ISO work item for a standard on "Human-Centered design" has been approved, but no working draft has yet been released for comment.

3.13.1.1.6 Recommendations. Procurements that require hardware components to be addressed by ergonomic standards can require conformance with standards for computer displays. Display characteristics include brightness and contrast, character legibility, image stability, glare, and the use of color.

Note, however, that ISO human factors/ergonomics standards are either normative or informative. An informative standard contains no mandatory requirements. A normative standard contains one or more requirements that must be met in order to achieve conformance with the standard.

ISO 9241-1 presents an overview of the content and usage of the multipart ISO 9241 standard. A revised version of ISO 9241-1 is currently at the Committee Draft (CD) level and will soon be released for Draft International Standard (DIS) ballot. ISO 9241-2 presents an overview of factors that should be considered when designing tasks to be performed in a specific computing environment.

Parts 1 and 2 of the ISO 9241 standard are informative. Part 3 of the ISO 9241 standard is normative; parts 2-9 are expected to be normative on completion. Conformance requirements for each normative part are embedded within that part. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product.

Procurements must recognize the difference between informative and normative parts of the standard in question. Where possible, both the informative and normative parts should be required for the best implementation of modern human factors/ergonomic thinking. In general, conformance tests for informative parts will not be available.

The ISO and ISO/IEC standards cited in the gray area of the table are being balloted and revised at a rapid rate. Interested parties should monitor the progress of these standards at six month intervals to ensure they have the latest information. Offerers of products meeting existing or emerging standards should be required to provide a migration plan to ensure compliance of the products with the final standards documents.

The DOD HCI Style Guide is recommended, in particular section 3, which deals with hardware.

3.13.1.2 Human factors for keyboards. (This BSA appears in both part 3, User Interface, and part 13, Human Factors.) This BSA covers keyboard layout, including specific directions for layout of regions of the keyboard, and keyboard design. Ease of use and correct ergonomic design also are a part of this BSA.

3.13.1.2.1 Standards. Table 3.13-2 presents human factors standards for keyboards.

TABLE 3.13-2 Human factors for keyboards standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 1: General principles governing keyboard layout	9995-1:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 2: Alphanumeric section	9995-2:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 3: Common secondary layout of the alphanumeric section	9995-3:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 4: Numeric section	9995-4:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 5: Editing section	9995-5:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 6: Function section	9995-6:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 7: Symbols used to represent functions	9995-7:1994	Informational (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 8: Allocation of Letters to the Keys of a Numeric Keyboard	9995-8:1994	Informational (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
NPC	ANSI	Coded Character Sets for Keyboard Arrangement in ANSI X4.23-1982 and X4.22-1983	X3.114-1984 (R1991)	Informational (Approved)
NPC	ANSI	Keyboard Arrangement	X3.154-1988	Informational (Approved)
NPC	ANSI	Alternate Keyboard Arrangement	X3.207-1991	Informational (Approved)
GPC	DOD	Military Standard Keyboard Arrangements	MIL-STD-1280, Notice 1, 1969	Informational (Approved)
GPC	DOD	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	MIL-STD-1472D Notice 2, 30 June 1992	Informational (Approved)
IPC	IEC	Man-Machine Interface (MMI) - Actuating Principles	447:1993	Informational (Approved)
CPC	NSC	Cumulative Trauma Disorders: a Manual for Musculoskeletal Diseases of the Upper Limbs	12221-0000	Informational (Approved)
IPC	ISO	Ergonomic Principles in the Design of Work Systems	6385:1981	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ACGIH	Ergonomic Interventions to Prevent Musculoskeletal Injuries in Industry	9000:1987	Informational (Approved)
CPC	NSC	Evaluating Your Workplace: Hands & Arms - Ergonomic Changes Manual	12587-0004	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

DODI 8120 mandates use of the DOD HCI Style Guide.

The ANSI X3.154 standard specifies the customary "QWERTY" keyboard arrangement. The ANSI X3.207 standard specifies the "DVORAK" keyboard arrangement. ACGIH is the American Conference of Governmental Industrial Hygienists.

3.13.1.2.2 Alternative specifications. There are no alternative specifications available.

3.13.1.2.3 Standards deficiencies. MIL-STD-1472D is in need of a comprehensive revision to update technical material so that it is reasonably consistent with the state of the art and to ensure that the two commands not currently using the standard can do so.

3.13.1.2.4 Portability caveats. No portability problems are known with the above specifications.

3.13.1.2.5 Related standards. The following standards are related to human factors standards for keyboards:

a. ISO 9241-1:1992, Ergonomic requirements for office work with visual display terminals (VDTs), part 1: Introduction, presents an overview of the content and usage of the multipart ISO 9241 standard. A revised version of ISO 9241-1 is currently at the CD level and will soon be released for DIS ballot.

b. ISO 9241-2:1992, Ergonomic requirements for office work with VDTs, part 2: Task Requirements, presents an overview of factors that should be considered when designing tasks to be performed in a specific computing environment.

c. ISO CD 10075-2, Ergonomic principles related to mental work load -- Part 2: Design Principles, gives guidance on the design of work systems in general, with the intention of providing optimal working conditions with respect to health and safety, well-being, performance, and effectiveness.

d. MIL-STD-1908 (1992), Definition of Human Factors Terms.

e. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

f. MIL-STD-1800A (1990) Human Engineering Performance Requirements for Systems.

g. MIL-HDBK-759B(2) (1993) Human Factors Engineering Design for Army Materiel. (Draft 759C is complete.)

h. MIL-HDBK-761A(1989) Human Engineering Guidelines for Management Information Systems.

i. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

j. DOD-HDBK-743A (1991) Anthropometry of U.S. Military Personnel.

k. ITU-T E.134 Human Factors Aspects of Public Terminals: Generic Operating Procedures.

l. An ISO work item for a standard on "Human-Centered design" has been approved, but no working draft has yet been released for comment.

3.13.1.2.6 Recommendations. Procurements that require hardware components to be addressed by ergonomic standards can require conformance with standards for keyboards. Keyboard characteristics include keyboard height, slope, profile, surface properties, adjustability, bounce and character repeat, key positioning, key displacement and force, keytop shape, and keytop legends.

Parts 1 and 2 of the ISO 9241 standard (see related standards) are informative. Parts 2-9 are expected to be normative on completion. Conformance requirements for each normative part are embedded within that part. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product.

Parts 1-8 of the ISO/IEC 9995 standard are normative. Conformance requirements for each normative part are embedded within that part. Conformance with the overall ISO 9995 standard is based on conformance with all normative parts that apply to a particular product.

The DOD HCI Style Guide is recommended, particularly for section 3, which covers hardware.

3.13.1.3 Human factors for non-keyboard input devices. (This BSA appears in both part 3, User Interface, and part 13, Human Factors.) This section presents human factors standards for input devices other than keyboards. These devices include trackballs, pens, and tablets among others.

3.13.1.3.1 Standards. Table 3.13-3 presents human factors standards for non-keyboard input devices.

TABLE 3.13-3 Human factors for non-keyboard input devices standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
IPC	ISO/IEC	Keyboard Layout for Text and Office Systems Part 7: Symbols used to represent functions	9995-7:1994	Informational (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
IPC	IEC	Man-Machine Interface (MMI) - Actuating Principles	447:1993	Informational (Approved)
IPC	ISO	Ergonomic Principles in the Design of Work Systems	6385:1981	Informational (Approved)
CPC	NSC	Cumulative Trauma Disorders: a Manual for Musculoskeletal Diseases of the Upper Limbs	12221-0000	Informational (Approved)
CPC	NSC	Evaluating Your Workplace: Hands & Arms - Ergonomic Changes Manual	12587-0004	Informational (Approved)
CPC	NSC	Cumulative Trauma	15229-0000	Informational (Approved)
NPC	ACGIH	Ergonomic Interventions to Prevent Musculoskeletal Injuries in Industry	9000:1987	Informational (Approved)
[illegible]	ISO/IEC	Text and Office Systems, Dialog Interaction Part 1: Cursor Control	10741-1:1992	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 9: Requirements for non-keyboard input devices	9241-9	Informational (Draft)
NPC	ANSI/HFS	Human Factors Engineering of Visual Display Terminal Workstations (Rev. 1)	100-1988 (Revision 1)	Informational (Draft (WD))

DODI 8120 mandates use of the DOD HCI Style Guide.

3.13.1.3.2 Alternative specifications. There are no alternative specifications available. Research in this area includes a foot operated control for the cursor when the hands are occupied (nicknamed a "mole" in obvious derivation from "mouse").

3.13.1.3.3 Standards deficiencies. Deficiencies in the cited standards are not known.

3.13.1.3.4 Portability caveats. No portability problems are known with the above specifications.

3.13.1.3.5 Related standards. The following standards are related to human factors standards for non-keyboard input devices:

a. ISO 9241-1:1992, Ergonomic requirements for office work with VDTs, part 1: Introduction, presents an overview of the content and usage of the multipart ISO 9241 standard. A revised version of ISO 9241-1 is currently at the CD level and will soon be released for DIS ballot.

b. ISO 9241-2:1992, Ergonomic requirements for office work with VDTs, part 2: Task Requirements, presents an overview of factors that should be considered when designing tasks to be performed in a specific computing environment.

c. ISO CD 10075-2, Ergonomic principles related to mental work load -- Part 2: Design Principles, gives guidance on the design of work systems in general, with the intention of providing optimal working conditions with respect to health and safety, well-being, performance, and effectiveness.

d. MIL-STD-1908 (1992), Definition of Human Factors Terms.

e. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

f. MIL-STD-1800A (1990) Human Engineering Performance Requirements for Systems.

g. MIL-HDBK-759B(2) (1993) Human Factors Engineering Design for Army Materiel. (Draft 759C is complete.)

h. MIL-HDBK-761A (1989) Human Engineering Guidelines for Management Information Systems.

i. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

j. DOD-HDBK-743A (1991) Anthropometry of U.S. Military Personnel.

k. ITU-T E.134 Human Factors Aspects of Public Terminals: Generic Operating Procedures.

l. An ISO work item for a standard on "Human-Centered design" has been approved, but no working draft has yet been released for comment.

3.13.1.3.6 Recommendations. Procurements that require hardware components to be addressed by ergonomic standards can require conformance with standards for non-keyboard input devices. Ergonomic issues for non-keyboard input devices include keyclick, tracking speed, and on-screen ghosting of the pointer.

Parts 1 and 2 of ISO 9241 are informative. Parts 2-9 are expected to be normative on completion. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product. Parts 1-8 of ISO/IEC 9995 are normative. Conformance with the overall ISO 9995 standard is based on conformance with all normative parts that apply to a particular product. Part 1 of the ISO/IEC 10741 standard is expected to be normative on completion.

Procurements must recognize the difference between informative and normative parts of the standard in question. Where possible, both the informative and normative parts should be required for the best implementation of modern human factors/ergonomic thinking. In general, conformance tests for informative parts will not be available.

The DOD HCI Style Guide is recommended particularly for section 3, which covers hardware.

3.13.2 Human factors for software user interfaces. This Mid level service area deals with human factors requirements for the software portion of the user interface.

3.13.2.1 Graphical user interface style guides. A GUI's style guide, which is part of the presentation management layer in the NIST's User Interface Reference Model, specifies a standard "look" for the GUI of an application to the user.

3.13.2.1.1 Standards. Table 3.13-4 presents graphical user interface style guides.

TABLE 3.13-4 Graphical user interface style guides standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
CPC	OSF	Motif Style Guide	Motif SG Rev. 1.2:1992	Mandated (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
IPC	NATO	Principles of Presentation of Information in Aircrew Stations	STANAG 3705	Informational (Approved)
GPC	DOD	User/Computer Interface	MIL-STD-1801 29 May 1987	Informational (Approved)
GPC	DOD	Human Engineering Performance Requirements for Systems	MIL-STD-1800A 10 Oct. 1990	Informational (Approved)
GPC	DOD	DOD Handbook, Human Engineering Guidelines for Management Information Systems	MIL-HDBK-761A 30 Sep. 1989	Informational (Approved)
GPC	DOD	Guidelines for Designing User Interface Software	ESD-TR-86-278	Informational (Approved)
GPC	DOD	Air Force Intelligence Data Handling System (IDHS) Style Guide	IDHS Style Guide 1990	Informational (Approved)
GPC	DOD	Human Factors Guidelines for the Army Tactical Command and Control System (ATCCS) Soldier-Machine Interface	ATCCS Guidelines v.1.0 and v.2.0, 1990 and 1992	Informational (Approved)
GPC	DOD	The User Interface Specifications for Navy Command and Control Systems	Navy CCS, Version 1.1, 1992	Informational (Approved)
GPC	DOD	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	MIL-STD-1472D Notice 2, 30 June 1992	Informational (Approved)
GPC	DOD	Human Engineering Guidelines for Management Information Systems	DOD-HDBK-71A (DOD 1989c)	Informational (Approved)
GPC	DOD	Human Engineering Requirements for Military Systems, Equipment, and Facilities	MIL-STD-46855B 26 May 1994	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
GPC	DOD	Department of Defence Intelligence Information Systems Style Guide	DODIIS Style Guide, 10/91	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 10: Dialogue principles	9241-10:1996	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 11: Guidance on Usability	9241-11	Information (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 12: Presentation of Information	9241-12	Information (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 13: User Guidance	9241-13	Information (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 14: Menu Dialogs	9241-14	Information (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 15: Command Language Dialogs	9241-15	Information (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 16: Direct manipulation dialogs	9241-16	Information (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 17: Form-filling dialogs	9241-17	Information (Draft)
IPC	ISO/IEC	Graphical Symbols Used on Screen Interactive Icons	11581	Information (Draft (CD))
HPC	IEEE	Recommended Practice for Graphical User Interface Dialogs	P1201.2	Information (Draft (Project being canceled, lack of progress))
OPC	DOD	Joint Surveillance Control (JSC) Human Computer Interface Standard, Version 1.0	JSC HCI Std, 1.0	Information (Draft)

DODI 8120 mandates the DOD HCI Style Guide.

The Human-Computer Interface (HCI) Style Guide provides a common framework for HCI design and implementation with emphasis on standard look and feel for GUI based applications. Motif 1.2 is the current version of the OSF specification for GUI behavior and appearance and programming and data interfaces. It includes a style guide for GUI interfaces.

3.13.2.1.2 Alternative specifications. Several applicable consortia or de facto style guides are available for software user interfaces. These style guides promote consistency in user interface design across applications. However, conformance with one or more the style guides listed below does not guarantee conformance with ergonomic standards (e.g., ISO 9241). These style guides include:

a. The Windows Interface: An Application Design Guide (Microsoft)

b. Object-Oriented Interface design: IBM Common User Access Guidelines (IBM)

c. Macintosh Human Interface Guidelines (Apple Computer)

d. SAA Presentation Manager Style Guide/ Common User Access (CUA) (IBM)

e. Standard User Interface Style Guide for Compartmented Mode Workstations (Defense Intelligence Agency (DIA))

f. Compartmented Mode Workstation Labeling: Source Code and User Interface Guidelines (DIA)

g. Air Force Standard Systems Center GUI Style Guide, SSCR 700-10, Vol I

h. User Interface Specifications for the Global Command and Control System (GCCS), Version 1.0, draft, October 1994

i. Theater Battle Management Style Guide (U.S. Navy)

j. Army Theater Battle Management HCI Specification

k. Navy JMCIS.

3.13.2.1.3 Standards deficiencies. Currently, conformance to parts 12-17 of the ISO 9241 standard is on a part-by-part basis. There is concern that the overall standard may thus fail to address potential ergonomic problems arising from interaction between the user interface elements covered by the individual parts.

There is concern that ISO/IEC 11581 may contain overly rigid specifications for the set of icon shapes that can be used to represent different user interface parts.

3.13.2.1.4 Portability caveats. NIST FIPS 158-1 (User Interface Component of the Applications Portability Profile) mandates the use of the X Window protocol, X library, and X toolkit intrinsics. IEEE P1201.2, when completed, is intended to increase the level of user interface consistency (and thus user interface portability) across X Windows-based environments. There are potential conflicts here.

DOD HCI Style Guide is based on (and intended to supersede) the Army, Navy, Air Force, and DODIIS style guides cited in the table above. The goal of this effort is to minimize unnecessary user interface diversity across DOD systems. There are potential problems with systems designed to accommodate different style guides.

MIL-STD-1800 is an Air Force-only standard that duplicates MIL-STD-1472D and is largely ignored in Air Force acquisitions. It has been recommended that MIL-STD-1800 be canceled and any value added material be added to MIL-STD-1472D.

3.13.2.1.5 Related standards. The following standards are related to user interface style guides:

a. ISO 9241-1:1992, Ergonomic requirements for office work with VDTs, part 1: Introduction, presents an overview of the content and usage of the multipart ISO

9241 standard. A revised version of ISO 9241-1 is currently at the CD level and will soon be released for DIS ballot.

b. ISO 9241-2:1992, Ergonomic requirements for office work with VDTs, part 2: Task Requirements, present an overview of factors that should be considered when designing tasks to be performed in a specific computing environment.

c. ISO CD 10075-2, Ergonomic principles related to mental work load -- Part 2: Design Principles, gives guidance on the design of work systems in general, with the intention of providing optimal working conditions with respect to health and safety, well-being, performance, and effectiveness.

d. MIL-STD-1908 (1992), Definition of Human Factors Terms.

e. NIST FIPS 158-1, User Interface Component of the Applications Portability Profile.

f. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

g. MIL-HDBK-759B(2) (1993) Human Factors Engineering Design for Army Materiel. (Draft 759C is complete.)

h. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

i. DOD-HDBK-743A (1991) Anthropometry of U.S. Military Personnel.

j. ITU-T E.134 Human Factors Aspects of Public Terminals: Generic Operating Procedures.

k. An ISO work item for a standard on "Human-Centered design" has been approved, but no working draft has yet been released for comment.

3.13.2.1.6 Recommendations. A style guide is necessary for development of all GUIs. There are no formal standards efforts in this area. A style guide is part of the Presentation Layer in NIST FIPS 158-1. Procurements that require software user interfaces to be addressed by ergonomic standards can require conformance with standards for menu structures, command languages, direct manipulation dialogs, forms-based dialogs, windowing, icons, screen formatting, information coding, and user guidance.

It is recommended that the practices of the DOD HCI Style Guide, TAFIM, Volume 8 be followed. It provides a common framework for HCI design and implementation with emphasis on standard look and feel for GUI based applications. As many aspects of standard GUI style are application specific, application area style guides should also be used when available. Motif 1.2 is the current version of the OSF specification for GUI behavior and appearance and programming and data interfaces. It includes a style guide for GUI interfaces and is also recommended.

Parts 1 and 2 of the ISO 9241 standard are informative; parts 10 and 11 are expected to be informative on completion. Parts 12-17 are expected to be normative on completion. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product. The ISO/IEC 11581 standard is expected to be normative on completion.

3.13.2.2 Visualization. (This BSA appears in part 3, User Interface, and part 13, Human Factors.) Visualization is the method of displaying data in a graphical manner to aid in recognition of patterns and trends in data and to give the viewer a depiction of a physical system that has been modeled by data points (e.g., finite element analysis (FEA) and computational fluid dynamics (CFD)). Another technique is the visualization user interface (VUI), a GUI that interprets text and numbers as pictures to show their relative scales and other relationships. A VUI remodels data so that text and numbers are hidden behind a picture expressing their complex relationships. Engineering visualization is a term freely applied to almost any intersection where the engineering process meets image creation technologies.

3.13.2.2.1 Standards. Table 3.13-5 presents visualization standards.

TABLE 3.13-5 Visualization standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ANSI/SAE	Aerodynamic Flow Visualization Techniques and Procedures	HS J1566 - 1986	Informational (Approved)

3.13.2.2.2 Alternative specifications. There are no alternative specifications available, but extensive academic research on this topic is taking place, particularly in the University of Maryland's Human-computer Interaction Laboratory and the Software Psychology Society. Topics include using treemaps for visualizing hierarchical information, using statistical distortion to promote the detection of outlying data, and use of color coding as a visualization aid.

3.13.2.2.3 Standards deficiencies. Deficiencies in the existing standard are unknown.

3.13.2.2.4 Portability caveats. Portability problems with the existing standard are unknown.

3.13.2.2.5 Related standards. The following standards are related to visualization standards:

a. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems

b. MIL-STD-1800A (1990) Human Engineering Performance Requirements for Systems

c. MIL-STD-1908 (1992) Definitions of Human Factors Terms

d. MIL-HDBK-761A (1989) Human Engineering Guidelines for Management Information Systems

e. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

3.13.2.2.6 Recommendations. There are no recommendations for visualization itself, but it does require the use of powerful graphics generation if a dynamic system will be shown, rather than a

series of static views. Other requirements can include a high degree of mathematical precision and single-pixel accuracy in rendering.

3.13.2.3 Color use. (This BSA appears in part 3, User Interface, and part 13, Human Factors.) The use of color is a vital part of communication with the user of computer applications. Computer representation of color is done through the use of the Red, Green, Blue (RGB) color separation method which must be used to approximate color definitions used in graphic technologies.

3.13.2.3.1 Standards. Table 3.13-6 presents standards for color use.

TABLE 3.13-6 Color use standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
IPC	CIE	Recommendations on Uniform Color Spaces, Color-Difference Equations, and Psychrometric Color Terms	CIE Pub. 15, Suppl. 2 (1986)	Informational (Approved)
IPC	NATO	Aircraft Electronic Colour Display Systems	STANAG 3940 (1991)	Informational (Approved)
IPC	ISO	[illegible]	[illegible]	[illegible] (Draft)

DODI 8120 mandates use of the DOD HCI Style Guide. The DOD HCI Style Guide addresses use of color and the meaning of color in section 4.3.

3.13.2.3.2 Alternative specifications. Alternative specifications include any user interface style guide that addresses the use and meaning of color.

3.13.2.3.3 Standards deficiencies. Comparison of color defined by the existing standards assumes identical viewing conditions. There are no standards directly addressing comparisons across viewing environments, although models are being worked on.

3.13.2.3.4 Portability caveats. Translation of color from one color definition system to another can be difficult and is only an approximation at best. There are three different color definitions from the CIE. They are CIEXYZ, CIELAB, and CIELUV. These standards have existed for a long time and are seen as the common basis for any future unifying definitions.

One problem with the use of color is color blindness. To accommodate the color blind, if color is used to convey important information, then a second method should also be used (such as brightness of the color).

3.13.2.3.5 Related standards. The following standards are related to human factors standards for the use of color:

a. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems

b. MIL-STD-1800A (1990) Human Engineering Performance Requirements for Systems

c. MIL-STD-1908 (1992) Definitions of Human Factors Terms

d. MIL-HDBK-761A (1989) Human Engineering Guidelines for Management Info. Systems

e. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

3.6 Recommendations. The approved standards in this section are recommended where they are applicable. The DOD HCI Style Guide is recommended, particularly section 4.3 which addresses the use and meaning of color.

3.13.2.4 Color definition. (This BSA appears in part 5, Data Interchange, part 12, Multimedia, and part 13, Human Factors.) Color definition deals with establishing a reference base for identifying colors to aid in the matching and exchange of color. Color definition standards apply to defining color in general, and not only to color definition for informatic technology systems.

3.13.2.4.1 Standards. Table 3.13-7 presents standards for color definition.

TABLE 3.13-7 Color definition standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC	ASTM	Standard Test Method for Computing the Colors of Objects by Using the CIE System	E308 (1990)	Informational (Approved)
NPC	EIA	1976 CIE-UCS Chromaticity Diagram with Color Boundaries	TEB26 (1988)	Informational (Approved)
IPC	ISO	CIE Standard Colorimetric Illuminants	CIE 1 6 (1991)	Informational (Approved)
IPC	ISO	CIE Standard Colorimetric Observers	CIE 10527 (1991)	Informational (Approved)
IPC	CIE	Recommendations on Uniform Color Spaces, Color-Difference Equations, and Psychrometric Color Terms	CIE Pul 15, Suppl. 2 (1986)	Informational (Approved)
NPC	NPESA	Graphic Technology - Input Data for Characterization of 4-Color Process Printing	IT8.7 (1993)	Informational (Approved)
NPC	NPESA	Graphic Arts Prepress Definition of Default RGB Data for Use in the Graphic Arts Industry	T8.7/4	Informational (Approved)
N/A	SMPTE/EIA/VESA/ISO	Unreferenced 24-bit RGB	Technical Reports	Informational (Approved)
IPC	[illegible]	[illegible]	[illegible]	[illegible]
IPC	ICC	[illegible]	TBD	[illegible]
NPC	ANSI IT8 and CGATS	[illegible]	TBD	[illegible]

The CIE (International Commission on Illumination) is the principal int nal standards writing body for agreements for color, vision, and illumination. Under A four bodies work on color-related standards. ANSI X3 works on office document automation information systems. ANSI IT8/CGATS is concerned with graphic arts. ASTM deals with colo metrology and standard practices, and SMPTE handles standards for color television and color monitors.

ANSI's Committee for Graphic Arts Technology Standards (CGATS) has eight subcommittees working on topics such as materials handling, process control, and color data definition. NPESA is the National Printing Equipment and Supply Association.

3.13.2.4.2 Alternative specifications. The following alternative specifications are also available:

a. Pantone Matching S tem

b. RGB (Red, Green, Blue) - the method directly used by color video display terminals

c. CMYK (Cyan, Magenta, Yellow, Black) - used in four color printing

d. HSV (Hue, Saturation, V.)

e. HSL (Hue, Saturation, Luminescence)

f. HVC

g. SWOP (Specifications for Web Offset Publications)

h. HSB (Hue, Saturation, Brightness)

i. TIFF (Tag Image File Format)

3.13.2.4.3 Standards deficiencies. Comparison of color defined by the existing standards assumes identical viewing conditions. There are no standards directly addressing comparisons across viewing environments, although models are being worked on. Strict adherence to correct presentation and output standards will require color calibration equipment.

3.13.2.4.4 Portability caveats. Translation of color from one color definition system to another can be difficult and is only an approximation at best. There are three different color definitions from the CIE. They are the CIEXYZ tristimulus values, and the CIELAB and CIELUV color spaces. These standards have existed for a long time and are seen as the common basis for any future unifying definitions. There are also the problems of color matching. For example, of 1012 Pantone colors for coated paper, 70 cannot be reproduced in the CMYK definition. CIEXYZ is useful in comparing colors under identical viewing conditions. CIEXYZ has a rigorous definition and by itself does not necessarily constitute a complete color specification. CIEXYZ is a standardized set of primaries which are not physically realizable but can match all possible colors with entirely positive tristimulus values. A new form of color definition is emerging, known as high-fidelity color. The idea behind high-fidelity color is the use of five to seven different colors in the printing process to widen the range of colors that can be printed. Two such models that have appeared are the Kupper set which increases the number of printed colors in the blue region by 80%, and the VSF model which provides better performance in deep red and green colors. These processes are very non-standard and should be avoided at present.

Common systems typically do not support colorimetric calibration.

3.13.2.4.5 Related standards. The following types of standards are related to standards for the definition of color:

a. color matching standards
b. color data exchange standards

c. color use standards
d. style guide standards

3.13.2.4.6 Recommendations. The approved standards in this section are recommended where they are applicable. Maintain original copies of source material so that revisions can be produced for next generation systems that will allow the inclusion of calibration information.

3.13.2.5 Color data interchange. (This BSA appears in part 5, Data Interchange, and part 13, Human Factors.) This BSA deals with the specific problems of interchanging data about color in computer graphics.

3.13.2.5.1 Standards. Table 3.13-8 presents standards for color data interchange.

TABLE 3.13-8 Color data interchange standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Graphic Technology - Prepress Digital Data Exchange - Colour Picture Data on Magnetic Tape (ANSI IT8.1-1988)	10755:1992	Informational (Approved)
IPC	ISO	Graphic Technology - Prepress Digital Data Exchange - Colour Line Art Data on Magnetic Tape	10756:1994	Informational (Approved)
IPC	ISO	Graphic Technology - Prepress Digital Data Exchange - Online Transfer from Electronic Prepress Systems to Colour Hardcopy Devices	10758:1994	Informational (Approved)
NPC	NPESA	Graphic Technology - Input Data for Characterization of 4-Color Process Printing	IT8.7/3 (1993)	Informational (Approved)
NPC	NPESA	Graphic Arts Prepress Definition of Default RGB Data for Use in the Graphic Arts Industry	IT8.7/4	Informational (Approved)
IPC	ISO/IEC	Generic Architecture for Colour Data Interchange (GACDI)	JTC1/SC24/WG5	Informational (Draft)

The Generic Architecture for Colour Data Interchange (GACDI) standard is a color architecture standard that will provide a consistent color framework across document-related standards. This standard will enable users to interchange color information in an open systems environment through the use of color data and transform representations.

3.13.2.5.2 Alternative specifications. No alternative specifications are available.

3.13.2.5.3 Standards deficiencies. There are no standards directly addressing comparison across viewing environments, although models are being worked on.

3.13.2.5.4 Portability caveats. Portability problems with the existing standards are unknown.

3.13.2.5.5 Related standards. Data interchange standards are related to standards for color data exchange.

3.13.2.5.6 Recommendations. The approved standards in this section are recommended where they are applicable.

3.13.2.6 Color matching. (This BSA appears in part 5, Data Interchange, and part 13, Human Factors.) This BSA deals with the problem of matching displayed and printed colors in computer systems.

3.13.2.6.1 Standards. Table 3.13-9 presents standards for color matching.

TABLE 3.13-9 Color matching standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Graphic Technology - Prepress Digital Data Exchange - Online Transfer from Electronic Prepress Systems to Colour Hardcopy Devices	10758:1994	Informational (Approved)
NPC	ASTM	Standard Test Method for Computing the Colors of Objects by Using the CIE System	E308 (1990)	Informational (Approved)
IPC	CIE	Recommendations on Uniform Color Spaces, Color-Difference Equations, and Psychrometric Color Terms	CIE Pub. 15, Suppl. 2 (1986)	Informational (Approved)
NPC	NPESA	Graphic Technology - Input Data for Characterization of 4-Color Process Printing	IT8.7/3 (1993)	Informational (Approved)
NPC	NPESA	Graphic Arts Prepress Definition of Default RGB Data for Use in the Graphic Arts Industry	IT8.7/4	Informational (Approved)
CPC	ICC	ICC Profile Format	ICC Profile Format ver. 3, 1994	Informational (Approved)
IPC	ISO/IEC	Data and Office Systems Colour Architecture (TOSCA)	JTC1/SC18/WG9	[illegible] (Draft)

The ICC was formed in March, 1994, by Apple, Adobe, Silicon Graphics, Taligent, Agfa, Kodak, Microsoft, and Sun for the purpose of defining profiles for color handling. The ICC Profile format has no preferred color space, and provides for more than four input colors.

ColorSync Profile Consortium has adopted the CGATS.5 specification as its definition of colorimetry and color measurement.

The Open System Color Association (OSCA) has taken on the role of providing industry with a centralized, stable, reliable, and common source of certified color-calibration data. OSCA consists of Agfa, DuPont, Fujifilm, Kodak, Radius, 3M, and 24 other non-founding member companies. OSCA's work is in harmony with the ICC Profile format.

3.13.2.6.2 Alternative specifications. The following alternative specifications are also available:

a. Pantone Matching System (PMS)

b. RGB (Red, Green, Blue) - the method directly used by color video display terminals

c. CMYK (Cyan, Magenta, Yellow, Black) - used in four color printing

d. Apple ColorSync 2.0 (supports ICC and CMYK)

e. Kodak Precision Color Management System (CMS)

f. Electronics for Imaging (EFI) Inc., EFIColor

g. Hewlett-Packard ColorSmart

h. Microsoft Independent Color Matching (ICM) in future versions of WindowsNT and Windows 95. (accepts ICC Profile Format).

i. Pantone Open Color Environment (POCE) (overshadowed by CMS and ColorSync)

j. Pantone ColorDrive (to standardize color palettes)

k. Trumatch SwatchPrinter

l. Tektronix TekColor

m. Agfa-Gevaert FotoFlow

3.13.2.6.3 Standards deficiencies. Comparison of color defined by the existing standards assumes identical viewing conditions. There are no standards directly addressing comparisons across viewing environments, although models are being worked on. The issue of where and how to correct color remains unresolved.

3.13.2.6.4 Portability caveats. Translation of color from one color definition system to another can be difficult and is only an approximation at best. There are three different color definitions from the CIE. They are CIEXYZ, CIELAB, and CIELUV. These standards have existed for a long time and are seen as the common basis for any future unifying definitions.

Because of their display orientation, all standards that are defining computer generated graphics color, use RGB models. Most programmers assume that the RGB values they are using are linear with display intensity and that may be approximately true depending on the response of the graphics system. The actual colors produced vary according to the graphics system used.

3.13.2.6.5 Related standards. Color definition standards are related to human factors standards for color matching.

3.13.2.6.6 Recommendations. The approved standards in this section are recommended where they are applicable.

3.13.2.7 Customization to local norms. (This BSA appears in part 3, User Interface, part 13, Human Factors, and part 14, Internationalization.) Customization to local norms involves modification of the key mapping to accommodate the local language and display of data in the commonly-used format (e.g., numbers, dates, time).

3.13.2.7.1 Standards. Table 3.13-10 presents standards for customization to local norms.

TABLE 3.13-10 Customization to local norms standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
CPC	X/Open	Internationalisation Guide, version 2	G304 (7/93)	Informational (Approved)
CPC	X/Open	Locale Registry Procedures	G303 (1993)	Informational (Approved)
CPC	OSF	Motif 1.2 (consistent with X/Open's NLS specifications & also double-byte character sets)	Motif 1.2	Informational (Approved)
CPC	MIT X Consortium	X Window System (X font manager- includes double-byte character sets)	X11R5	Informational (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
GPC	DOD	Military Standard Keyboard Arrangements	MIL-STD-1280, Notice 1, 1969	Informational (Approved)
GPC	DOD	User/Computer Interface	MIL-STD-1801 29 May 1987	Informational (Approved)
GPC	DOD	Human Engineering Performance Requirements for Systems	MIL-STD-1800A 10 Oct. 1990	Informational (Approved)
GPC	DOD	DOD Handbook, Human Engineering Guidelines for Management Information Systems	MIL-HDBK-761A 30 Sep. 1989	Informational (Approved)
GPC	DOD	Guidelines for Designing User Interface Software	ESD-TR-86-278	Informational (Approved)
GPC	DOD	Department of Defense Intelligence Information Systems Style Guide	DODIIS Style Guide, 10/91	Informational (Approved)
GPC	DOD	Air Force Intelligence Data Handling System (IDHS) Style Guide	IDHS Style Guide 1990	Informational (Approved)
GPC	DOD	Human Factors Guidelines for the Army Tactical Command and Control System (ATCCS) Soldier-Machine Interface	ATCCS Guidelines v.1.0 and v.2.0, 1990 and 1992	Informational (Approved)
GPC	DOD	The User Interface Specifications for Navy Command and Control Systems	Navy CCS, Version 1.1, 1992	Informational (Approved)
GPC	DOD	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	MIL-STD-1472D Notice 2, 30 June 1992	Informational (Approved)
GPC	DOD	Human Engineering Guidelines for Management Information Systems	DOD-HDBK-71A (DOD 1989c)	Informational (Approved)
CPC	X/Open	Distributed Internationalisation Services	S213 (11/92)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Internationalisation of Internetworking Specifications	S302 (4/93)	Informational (Approved)
CPC	X/Open	File System Safe UCS Transformation Format (FSS-UTF)	P316 (1993)	Informational (Approved)
CPC	X/Open	System Interface and Headers, Issue 3	C212 (3/92)	Informational (Approved)
CPC	X/Open	Supplementary Definitions, Issue 3	C213 (3/92)	Informational (Approved)
CPC	X/Open	Universal Multiple-Octet Coded Character Set Coexistence and Migration	E401 (3/94)	Informational (Approved)
NPC	ANSI/SAE	Human Interface Design Methodology for Integrated Display Symbology	ARP 4155 (1990)	Informational (Approved)
GPC	DOD	Human Engineering Requirements for Military Systems, Equipment, and Facilities	MIL-STD-46855B 26 May 1994	Informational (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Informational (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Informational (Approved)
CPC	X/Open	Locale Registry Procedures, Version 2	G502 (5/95)	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
CPC	X/Open	Internationalization Guide, Version 3	G008 (11/95)	Informational (TBD)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 11: Guidance on usability specifications and measures	9241-11	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 12: Presentation of information	9241-12	Informational (Draft)
NPC	IEEE	Recommended Practice for Graphical User Interface Developer	P1201.2	Informational (Draft (Project being canceled, lack of progress))
GPC	DOD	Joint Satellite Control GBCS Human Computer Interface Standard, Version 1.0	JSC HCI Std., 1.0	Informational (Draft)

DODI 8120 mandates use of the DOD HCI Style Guide

Motif 1.2 is the current version of the OSF specification for GUI behavior and appearance and programming and data interfaces. X11R5 is the current release of Version 11 of the X Windows standard.

3.13.2.7.2 Alternative specifications. Several applicable consortia or de facto style guides are available for internationalization. However, conformance with one or more the style guides listed below does not guarantee conformance with ergonomic standards:

a. The Windows Interface: An Application Design Guide (Microsoft)

b. Object-Oriented Interface design: IBM Common User Access Guidelines (IBM)
c. Macintosh Human Interface Guidelines (Apple Computer).

3.13.2.7.3 Standards deficiencies. Currently, conformance to parts 12-17 of the ISO 9241 standard is on a part-by-part basis. There is concern that the overall standard may thus fail to address potential ergonomic problems arising from interactions between the user interface elements covered by the individual parts.

3.13.2.7.4 Portability caveats. Although Motif supports the X/Open Native Language System, it also supports a number of its own internationalization extensions which makes it incompatible with some legacy specifications (e.g., OpenLook).

NIST FIPS 158-1 (User Interface Component of the Applications Portability Profile) mandates the use of the X Window protocol, X library, and X toolkit intrinsics. IEEE P1201.2, when completed, is intended to increase the level of user interface consistency (and thus user interface portability) across X Windows-based environments. There are potential conflicts here.

The DOD HCI Style Guide is based on (and intended to supersede) the Army, Navy, Air Force, and DODIIS style guides cited in the table above. The goal of this effort is to minimize unnecessary user interface diversity across DOD systems. There are potential problems with systems designed to accommodate different style guides.

3.13.2.7.5 Related standards. The following standards are related to cultural convention services:

a. X/Open Internationalisation Locale: L001 (1994): ja_JP - Japanese for Japan.

b. X/Open Internationalisation Locale: L002 (1994): da_DK - Danish for Denmark.

c. X/Open Internationalisation Locale: L003 (1994): de_AT - German for Austria.

d. X/Open Internationalisation Locale: L004 (1994): en_DK - English for Denmark.

e. X/Open Internationalisation Locale: L005 (1994): fo_FO - Faroese for the Faroes.

f. X/Open Internationalisation Locale: L006 (1994) is_IS - Icelandic for Iceland.

g. X/Open Internationalisation Locale: L007 (1994) kl_GL - Greenlandic for Greenland.

h. X/Open Internationalisation Locale: L008 (1994) lt_LT - Lithuanian for Lithuania.

i. X/Open Internationalisation Locale: L009 (1994): lv_LV - Latvian for Latvia.

j. X/Open Internationalisation Locale: L010 (1994): de_CH - German for Switzerland.

k. X/Open Internationalisation Locale: L011 (1994): de_DE - German for Germany.

l. X/Open Internationalisation Locale: L012 (1994): en_GB - English for Great Britain.

m. X/Open Internationalisation Locale: L013 (1994): en_IE - English for Ireland.

n. X/Open Internationalisation Locale: L014 (1994): en_US - English for the U.S.A.

o. X/Open Internationalisation Locale: L015 (1994): hu_HU - Hungarian for Hungary.

p. X/Open Internationalisation Locale: L016 (1994): it_IT - Italian for Italy.

q. X/Open Internationalisation Locale: L017 (1994): nl_NL - Dutch for the Netherlands.

r. X/Open Internationalisation Locale: L018 (1994): pl_PL - Polish for Poland.

s. X/Open Internationalisation Locale: L019 (1994): pt_PT - Portuguese for Portugal.

t. X/Open Internationalisation Locale: L020 (1994): ro_RO - Romanian for Romania.

u. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

v. MIL-STD-1908 (1992) Definitions of Human Factors Terms.

w. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

3.13.2.7.6 Recommendations. Procurements that require software user interfaces to be addressed by ergonomic standards can require conformance with standards for menu structures, command languages, direct manipulation dialogs, forms-based dialogs, windowing, icons, screen formatting, information coding, and user guidance.

Parts 1 and 2 of the ISO 9241 standard are informative; parts 10 and 11 are expected to be informative on completion. Part 3 of the ISO 9241 standard is normative; parts 2-9 and 12-17 are expected to be normative on completion. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product.

Procurements must recognize the difference between informative and normative parts of the standard in question. Where possible, both the informative and normative parts should be required for the best implementation of modern human factors/ergonomic thinking. In general, conformance tests for informative parts will not be available.

The DOD HCI Style Guide is recommended for customization to local norms.

3.13.3 Human factors for computer environments. This Mid-Level Service Area addresses the environment as it affects both the user and the computer.

3.13.3.1 Human factors for the physical environment. (This BSA appears in both part 3, User Interface, and part 13, Human Factors.) Procurements that require computing environments to be addressed by ergonomic standards can require conformance with standards for illuminance, glare, acoustic noise, the thermal environment, electromagnetic emissions, computer workspace design and furniture design.

The effects of low-level non-ionized radiation, particularly from CRTs, on humans have been a controversial topic. Over the years there have been articles advising pregnant women who have a prior history of miscarriage to stay away from working in computer areas. During the cold war, the Soviets were suspected of secretly bombarding foreigners with non-ionized radiation to study long term effects. People who live near high voltage power lines and have developed cancer are suspected victims of electromagnetic radiation. While there are no hard theories to describe the relationship between health problems and this kind of radiation, let alone a standard established. Some VDT vendors have made claims regarding the emissions of their products and there are aftermarket shields available that may provide some protection against this form of radiation.

Laser printers are said to emit ozone during the printing process. In an enclosed area, high levels of ozone can be unhealthy or even toxic. This issue is still unclear. It remains to be seen how much ozone is emitted and what concentrations are hazardous.

3.13.3.1.1 Standards. Table 3.13-11 presents human factors standards for the physical environment.

TABLE 3.13-11 Human factors for the physical environment standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
CPC	OSF	Motif Style Guide	Motif SG Rev. 1.2:1992	Mandated (Approved)
CPN-C	Microsoft	The Windows Interface: An Application Design Guide, Microsoft Press, 1992	API Design Guide	Mandated (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
GPC	DOD	Noise Limits for Military Material	MIL-STD-1474C of 8 March 1991	Informational (Approved)
GPC	DOD	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	MIL-STD-1472D Notice 2, 30 June 1992	Informational (Approved)
GPC	DOD	Physical Ear Noise Attenuation Testing	MIL-STD-912 of 11 December 1990	Informational (Approved)
IPC	ISO	Ergonomic Principles Related to Mental Work Load - General Terms and Definitions	10075:1991	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Principles of Visual Ergonomics - Lighting of Indoor Work Systems	8995:1989	Informational (Approved)
IPC	ISO	Expression of Users' Requirements Part 1: Thermal Requirements	6242-1:1992	Informational (Approved)
IPC	ISO	Expression of Users' Requirements Part 2: Air Purity Requirements	6242-2:1992	Informational (Approved)
IPC	ISO	Expression of Users' Requirements Part 3: Acoustical Requirements	6242-3:1992	Informational (Approved)
NPC	EIA	Considerations Used in Establishing the X-Radiation Ratings of Monochrome and Color Direct-View Television Picture and Data Display Tubes	TEP 194, Amd 1 1987, Amd 2 1988	Informational (Approved)
CPC	NSC	Ergonomics in Computerized Offices	12223-0000	Informational (Approved)
CPC	NSC	Guide to Working Safely with Computers - Manual (relates to VDTs)	13068-0000	Informational (Approved)
CPC	NSC	Guide to Working Safely with Computers	13608-0000	Informational (Approved)
CPC	NSC	Working Safely with Your Computer	15223-0000	Informational (Approved)
IPC	ECMA	Ergonomics - Recommendations for VDU (Visual Display Units) Work Places	TR/22 (1984)	Informational (Approved)
IPC	ECMA	Application of Human Engineering to Advanced Aircrew Systems	3994 (1984)	Informational (Approved)
IPC	ECMA	Measurement of Airborne Noise Emitted by Computer and Business Equipment	74 (1992)	Informational (Approved)
IPC	ECMA	Measurement of High Frequency Noise Emitted by Computer and Business Equipment	108 (1989)	Informational (Approved)
IPC	ECMA	Declared Noise Emission Values of Computer and Business Equipment	109 (1992)	Informational (Approved)
IPC	ECMA	Determination of Sound Power Levels of Computer and Business Equipment Using Sound Intensity Measurements; Scanning Method in Controlled Rooms	160 (1992)	Informational (Approved)
IPC	ISO	Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) Part 5: Workplace requirements	9241-5	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 6: Environmental requirements	9241-6	Informational (Draft)
IPC	ISO	Ergonomic Requirements for Office Work with VDTs Part 7: Display requirements with reflections	9241-7	Informational (Draft)
NPC	ANSI/HFS	Human Factors Engineering of Visual Display Terminal Workstations (Rev. 1)	100-1988 (Revision 1)	Informational (Draft (WD))

DODI 8120 mandates use of the DOD HCI Style Guide.

3.13.3.1.2 Alternative specifications. MPR II 1990:8 (Test Methods for Visual Display Units, Section 2.0.1) is a Swedish document containing recommended values for electronic emissions from visual display units. While not an ISO standard, it serves as a de facto electromagnetic emissions standard for displays in most other countries. Many vendors of monitors claim

compliance with this or a similar specification. After-market radiation and glare shields are also available.

3.13.3.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.
3.13.3.1.4 Portability caveats. MIL-STD-1474C's criteria are more stringent than those of the Occupational Safety and Health Administration and also covers additional topics such as nondetectability. This standard may be incorporated into the next revision of MIL-STD-1472, eliminating the need to retain MIL-STD-1474C.

3.13.3.1.5 Related standards. The following standards are related to human factors standards for computer environments:

a. ISO 9241-1:1992, Ergonomic Requirements for Office Work with VDTs, part 1: Introduction, presents an overview of the content and usage of the multipart ISO 9241 standard. A revised version of ISO 9241-1 is at the CD level and will soon be released for DIS ballot.

b. ANSI/ASHRAE 55, Thermal Environmental Conditions for Human Occupancy, 1992.

c. ANSI S12.10-1985, Method for Measurement and Designation of Noise Emitted by Computer and Business Equipment.

d. ANSI S1.13-1971, Methods for the Measurement of Sound Pressure Levels.

e. ANSI X5.1-1985, Tests for General Office Chairs.

f. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

g. MIL-STD-1800A (1990) Human Engineering Performance Requirements for Systems.

h. MIL-HDBK-759B(2) (1993) Human Factors Engineering Design for Army Materiel. (Draft 759C is complete.)

i. MIL-HDBK-761A (1989) Human Engineering Guidelines for Management Information Systems.

j. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

k. DOD-HDBK-743A (1991) Anthropometry of U.S. Military Personnel.

l. MIL-STD-740-1 (1986) Airborne Sound Measurements and Acceptance Criteria of Shipboard Equipment.

m. MIL-STD-740-2 (1986) Structureborne Vibratory Acceleration Measurements Acceptance Criteria of Shipboard Equipment.

n. MIL-STD-1294A (1985) Acoustical Noise Limits in Helicopters.

o. An ISO work item for a standard on "Human-Centered design" has been approved, but no working draft has yet been released for comment.

3.13.3.1.6 Recommendations. The approved standards in this section are recommended where they are applicable. Parts 2-9 and 12-17 are expected to be normative on completion. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product.

The DOD HCI Style Guide is recommended particularly for section 3, which covers hardware.

INFORMATION TECHNOLOGY STANDARDS GUIDANCE

(ITSG)

(Part 14 of 14 parts)

INTERNATIONALIZATION SERVICES

Version 3.1 - April 7, 1997

AREA IPSC

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

TABLE OF CONTENTS

LIST OF TABLES

3.14 Internationalization. Internationalization is the adaptation of a computer system's interface to present data according to local conventions and to use character sets that support the local language.

NOTE: Throughout Part 14, all tables shall have abbreviations listed under the column (Standard Type) as follows:

a. National Public Consensus = NPC
b. International Public Consensus = IPC
c. Government Public Consensus = GPC
d. Consortia Public Consensus = CPC
e. Corporate Private Non-Consensus = CPN-C

3.14.1 Character set and data representation. A character set is a subset of all letters in different alphabets, numbers, punctuation marks, mathematical symbols, and other characters used by computers. These services include the capability to input, store, manipulate, retrieve, communicate, and present data independent of the coding scheme used.

3.14.1.1 Coded character sets. (This BSA appears in both part 5, Data Interchange, and part 14, Internationalization.) A character set is a subset of all letters in different alphabets, numbers, punctuation marks, mathematical symbols, and other characters used by computers. These services include the capability to input, store, manipulate, retrieve, communicate, and present data independent of the coding scheme used.

3.14.1.1.1 Standards. Table 3.14-1 presents standards for coded character sets.

TABLE 3.14-1 Coded character sets standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Coded Graphic Character Set for Text Communication - Latin Alphabet Second Edition (replaces 6937 pt.1 & pt. 2)	6937:1994	Adopted (Approved)
IPC	ISO/IEC	Coded Graphic Character Set for Use in the Preparation of Documents used in Electrotechnology and for Information Exchange	1286:1995	Informational (Approved)
IPC	ISO/IEC	Coded Graphic Character Set for Text Communication	6937	Informational (Draft)
IPC	ISO	Mathematical coded character set for bibliographic information interchange	6862	Informational (Draft)
IPC	ISO	Hebrew alphabet coded character set for bibliographic information interchange	8957	Informational (Draft)
IPC	ISO	Armenian alphabet coded character set for bibliographic information interchange	10585	Informational (Draft)
IPC	ISO	Georgian alphabet coded character set for bibliographic information interchange	10586	Informational (Draft)
IPC	ISO/IEC	Coded Character Sets for Text Communication, Parts 0, 3, 7, 8	6937-0,3,7,8:1994	Informational (Draft)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)

3.14.1.1.2 Alternative specifications. Alternative character coding schemes include Encoded Binary Decimal (EBCDC) and the Macintosh character set.

3.14.1.1.3 Standards deficiencies. The greatest deficiency any of these standards have is narrow applicability to a single application or language or no standard means of translation from set to set.

3.14.1.1.4 Portability caveats. Character sets are generally portable, but there are sometimes questions about conversion between sets.

3.14.1.1.5 Related standards. The following standards are related to coded character set standards:

a. NIST FIPS 19-2: Catalog of Widely Used Code Sets

b. Optical Character Recognition (OCR) Character Code Sets:

(1) SO 1073-1:1976: Alphanumeric character sets for optical recognition- Part 1: Character set OCR-A -- Shapes and dimensions of the printed image

(2) SO 1073-2:1976: Alphanumeric character sets for optical recognition- Part 2: Character set OCR-B -- Shapes and dimensions of the printed image

(3) SO 1831:1980: Printing specifications for optical character recognition

(4) SO 2033:1983: Information processing -- Coding of machine readable characters (MICR and OCR)

c. Magnetic Ink Character Recognition (MICR) Character Sets

(1) SO 2033:1983: Information processing -- Coding of machine readable characters (MICR and OCR)

(2) SO 1004:1995: Information Processing - Magnetic ink character recognition - Print specifications

3.14.1.1.6 Recommendations. ISO 6937 is recommended for ordinary English-only alphabetic applications.

3.14.1.2 Seven-bit coded character sets. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Character sets which contain only as many characters as can be uniquely identified using a seven-bit number (i.e., 128 characters numbered 0 to 127).

3.14.1.2.1 Standards. Table 3.14-2 presents standards for seven-bit coded character sets.

TABLE 3.14-2 Seven-bit coded character sets standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Code for Information Interchange, Its Representations, Subsets, and Extensions (ASCII) (adopts ANSI X3.4-1986/R 1992, X3.32-1990, X3.41-1974)	FIPS PUB 1-2:1984	Adopted (Approved)
IPC	ISO	ISO 7-Bit Coded Character Set for Information Exchange	646:1991	Adopted (Approved)
IPC	ISO	Information Processing - Representation of the 7-Bit Coded Character Set on Punched Tape	1113:1979	Informational (Approved)
NPC	ANSI	Code Extension Techniques for Use with the 7-Bit Coded Character Set of American National Standard Code for Information Interchange	X3. 41-1974	Informational (Approved)
IPC	ISO	Information Processing - Arabic 7-Bit Coded Character Set for Information Interchange	9036:1987	Informational (Approved)
IPC	NATO	Parameters and Practices for the Use of the NATO 7-Bit Code	STANAG 5036	Informational (Approved)
IPC	NATO	Interoperable Characters for Teleprinters Using NATO 7-Bit Code	STANAG 5045	Informational (Approved)

ISO 646 describes a set of 128 control, alphabetic, digit, and symbol characters. It includes the use of the control characters and describes the option of national replacement characters. It is the standard that formed the basis for creating additional standards that extend the character set to include many languages. A variant, ISO 646:1991 IRV, left open an additional 128 codes to be used to represent symbols for other languages.

3.14.1.2.2 Alternative specifications. Alternative character coding schemes include Encoded Binary Decimal (EBCDC) and the Macintosh character set.

3.14.1.2.3 Standards deficiencies. The greatest deficiency any of these standards have is narrow applicability to a single application or language or no standard means of translation from set to set.

3.14.1.2.4 Portability caveats. Character sets are generally portable, but there are sometimes questions about conversion between sets. FIPS 19-2, a catalog of widely used code sets that lists and briefly describes code stes in wide use in the United States and might be used in Federal data systems, may be helpful to consult.

3.14.1.2.5 Related standards. The following standards are related to seven-bit coded character sets:

a. NIST FIPS 19-2: Catalog of Widely Used Code Sets

b. Optical Character Recognition Character Code Sets

c. ISO 3275:1974-- Implementation of the 7-bit coded character set and its 7-bit and 8-bit extensions on 3,81 mm magnetic cassette for data interchange

d. ISO 6586:1980 -- Implementation of the ISO 7-bit and 8-bit coded character sets on punched cards

e. ISO 1113:1979 -- Representation of the 7-bit coded character set on punched tape

3.14.1.2.6 Recommendations. FIPS 1-2, which adopts the ASCII character set, is recommended for common applications. ISO 646 is also recommended.

3.14.1.3 Eight-bit coded character sets. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Character sets which contain only as many characters as can be uniquely identified using an eight-bit number (typically, 256 characters numbered 0 to 255).

3.14.1.3.1 Standards. Table 3.14-3 presents standards for eight-bit coded character sets.

TABLE 3.14-3 Eight-bit coded character sets standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
NPC/IPC	ANSI/ISO/IEC	ISO 8-Bit Code for Information Interchange - Structure and Rules for Implementation (8-Bit ASCII) (Revision and redesignation of ANSI X3.134.1)	4873:1991	Adopted (Approved)
IPC	ISO/IEC	Standardized Coded Graphic Character Sets for Use in 8-Bit Codes	10367:1991	Informational (Approved)
IPC	ECMA	8-Bit Coded Character Set	6 (1991)	Informational (Approved)
IPC	ECMA	8-Bit Coded Character Set Structure and Rules	43 (1991)	Informational (Approved)

3.14.1.3.2 Alternative specifications. Alternative character coding schemes include EBCDC and the Macintosh character set.

3.14.1.3.3 Standards deficiencies. The greatest deficiency any of these standards have is narrow applicability to a single application or language or no standard means of translation from set to set.

3.14.1.3.4 Portability caveats. Character sets are generally portable, but there are sometimes questions about conversion between sets.

3.14.1.3.5 Related standards. The following standards are related to eight-bit coded character sets:

a. NIST FIPS 19-2: Catalog of Widely Used Code Sets

b. OCR Character Code Sets

c. ISO 3275:1974-- Implementation of the 7-bit coded character set and its 7-bit and 8-bit extensions on 3,81 mm magnetic cassette for data interchange

d. ISO 6586:1980 -- Implementation of the ISO 7-bit and 8-bit coded character sets on punched cards

3.14.1.3.6 Recommendations. ISO 4873 is recommended.

3.14.1.4 Eight-bit single byte character sets. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Character sets which contain only as many characters as can be uniquely identified using an eight-bit number in a single byte (typically, but not always, 256 characters numbered 0 to 255).

3.14.1.4.1 Standards. Table 3.14-4 presents standards for eight-bit single byte character sets.

TABLE 3.14-4 Eight-bit single byte character sets standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	ISO 8-Bit Single-Byte Coded Graphic Character Sets: Parts 1-9	8859-1 to 9:1987-1989	Mandated (Approved)
IPC	ISO/IEC	ISO 8-Bit Single-Byte Coded Graphic Character Sets: Part 10: Latin Alphabet Set No. 6	8859-10:1992	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets, Latin Alphabets No. 1 to No. 4	94 (1986)	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets - Latin/Cyrillic Alphabet	113 (1988)	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets - Latin/Arabic Alphabet	114 (1986)	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets - Latin/Greek Alphabet	118 (1986)	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets - Latin/Hebrew Alphabet	121 (1987)	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets, Latin Alphabet No. 5	128 (1988)	Informational (Approved)
IPC	ECMA	8-Bit Single-Byte Coded Graphic Character Sets - Latin Alphabet No. 6	144 (1992)	Informational (Approved)

ISO 8859 defines a set of 191 graphic characters with a single 8-bit byte. It uses the characters 0x20 through 0x7F to represent those used in the US-ASCII (ISO 646) set.

3.14.1.4.2 Alternative specifications. Alternative character coding schemes include EBCDC and the Macintosh character set.

3.14.1.4.3 Standards deficiencies. The greatest deficiency any of these standards have is narrow applicability to a single application or language or no standard means of translation from set to set.

3.14.1.4.4 Portability caveats. Character sets are generally portable, but there are sometimes questions about conversion between sets.

3.14.1.4.5 Related standards. The following standards are related to eight-bit single byte character sets:

a. NIST FIPS 19-2: Catalog of Widely Used Code Sets
b. Optical Character Recognition Character Code Sets

3.14.1.4.6 Recommendations. ISO 8859, parts 1-9, is recommended.

3.14.1.5 Control functions. (This BSA appears in part 5, Data Interchange and part 14, Internationalization.) This service area is for definition and coding of control functions for inclusion in character sets.

3.14.1.5.1 Standards. Table 3.14-5 presents standards for control functions.

TABLE 3.14-5 Control functions standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Control Functions for ISO 7-Bit and 8-Bit Coded Character Sets	6429:1992	Adopted (Approved)
GPC	NIST	Additional Controls for Use with American National Standard Code for Information Interchange (adopts ANSI X3.64-1979/R1990)	FIPS PUB 86:1981	Informational (Approved)
IPC	ISO	Information Processing - Graphical Representations for the Control Characters of the 7 Bit Coded Character Set	2047:1975	Informational (Approved)
IPC	ISO	Bibliographic control characters	6630:1986	Informational (Approved)
IPC	ECMA	Control Functions for Coded Character Sets	48 (1991)	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

ISO 6429 defines 7-bit, 7-bit extended, 8-bit, and 8-bit extended character set control functions.

3.14.1.5.2 Alternative specifications. There are no alternative specifications.

3.14.1.5.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.14.1.5.4 Portability caveats. Portability problems with the existing standards are unknown.

3.14.1.5.5 Related standards. There are no related standards.

3.14.1.5.6 Recommendations. ISO 6429 is recommended.

3.14.1.6 Character set conversion. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Character set conversion deals with the problem of translating from one character set to another.

3.14.1.6.1 Standards. Table 3.14-6 presents standards for character set conversion.

TABLE 3.14-6 Character set conversion standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Conversion Between the Two Coded Character Sets of ISO 646 and ISO 6937-2 and the CCITT International Telegraph Alphabet No. 2 (ITA2)	6936:1988	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

ISO 6936 specifies conversion between the 58 character ITA2 set and the 128 character ISO 646 set.

3.14.1.6.2 Alternative specifications. There are alternative specifications that are sometimes necessary:

a. Mac to ASCII
b. EBCDC to ASCII

3.14.1.6.3 Standards deficiencies. The greatest deficiency any of these standards have is narrow applicability to a single application or language or no standard means of translation from set to set.

3.14.1.6.4 Portability caveats. Character sets are generally portable, but there are sometimes questions about conversion between sets.

3.14.1.6.5 Related standards. The following standards are related to character sets conversion:

a. Transliteration standards.

3.14.1.6.6 Recommendations. There are no recommendations. Character set conversion standards depend on which sets are involved.

3.14.1.7 Code extension techniques. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) There is also a need to define standard techniques for expanding the number of characters represented by a character set. Switching between character sets in mid-string is done by escape sequences.

3.14.1.7.1 Standards. Table 3.14-7 presents standards for code extension techniques.

TABLE 3.14-7 Code extension techniques standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Character Code Structure and Extension Techniques	2022:1994	Adopted (Approved)
IPC	ISO	Information Processing - Implementation of the 7-Bit Coded Character Set and Its 7-Bit and 8-Bit Extensions on 3,81 mm Magnetic Tape Cassette for Data Interchange	3275:1974	Informational (Approved)
IPC	ISO	Extension of the Latin Alphabet Coded Character Set for Bibliographic Information Interchange	5426:1983	Informational (Approved)
IPC	ISO	Extension of the Cyrillic Alphabet Coded Character Set for Bibliographic Information Interchange	5427:1984	Informational (Approved)
IPC	ISO	Greek Alphabet Coded Character Set for Bibliographic Information Interchange	5428:1984	Informational (Approved)
IPC	ISO	Documentation - African Coded Character Set for Bibliographic Information Interchange	6438:1983	Informational (Approved)
IPC	ECMA	Code Extension Techniques	35 (1994)	Informational (Approved)
IPC	ISO	Extension of the Cyrillic alphabet coded character set for non-Slavonic languages for bibliographic information interchange	10754	Informational (Draft)
IPC	ISO/IEC	ISP for Code Extension Based on ISO/IEC 2022 Part 1: FCS11-2022 Option 1	13970-1:1995	Informational (Draft)
IPC	ISO	Extension of the Latin Alphabet Coded Character Set for Bibliographic Information Interchange, part 2: Latin characters used in minor European languages and obsolete typography	5426-2	Informational (Draft)
IPC	ISO	Extension of the Arabic alphabet coded character set for bibliographic information interchange	11822	Informational (Draft)
IPC	ISO/IEC	ISO 7-Bit and 8-Bit Coded Character Sets - Code Extension Techniques	2022:1986	Informational (Superseded)

3.14.1.7.2 Alternative specifications. Alternative specifications would include other, larger, forms of character sets (8-bit instead of 7-bit, or multiple-octet sets instead of 8-bit).

3.14.1.7.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.14.1.7.4 Portability caveats. Few systems support the ISO 2022 encoding architecture because escape sequences present difficulties to processing.

3.14.1.7.5 Related standards. There are no related standards.

3.14.1.7.6 Recommendations. ISO 2022 is recommended.

3.14.1.8 Universal character sets. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Universal character sets are an approach to defining the broadest possible character set. This involves using more than an 8-bit code. Use of a 16-bit code allows for a character set of 32,768 characters, which is sufficient to cover several complete alphabets, including accented letters. The object of UCS is to represent the written form of world languages unambiguously to facilitate information interchange

3.14.1.8.1 Standards. Table 3.14-8 presents standards for universal character sets.

TABLE 3.14-8 Universal character sets standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Universal Multiple-Octet Coded Character Set (UCS), Part 1. Architecture and Basic Multilingual Plane (with Technical Corrigendum 1: 1996)	10646-1:1993	Mandated (Approved)
CPC	X/Open	Universal Multiple-Octet Coded Character Set Coexistence and Migration	E401 (3/94)	Informational (Approved)
CPC	Unicode Consortium	Unicode version 1.1	UCS-2	Informational (Approved)
IPC	ISO/IEC	Universal Multiple-Octet Coded Character Set, Part 1: Architecture and Basic Multilingual Plane, Amend 1: UTF-16, Amend 2: UTF-8, Amend 3: [illegible], Amend 4: [illegible]	10646-1, Am 1-4:1995	Informational (Draft)
IPC	ISO	Universal Multiple-Octet Coded Character Set, Part 1: Architecture and Basic Multilingual Plane, Amend 5: Korean Hangul, 6: [illegible]	[illegible]	Informational (Draft)

ISO 10646 is an extension of ISO 8859. A separate part of 8859 is defined for a variety of character sets. The 10646 is multiple-octet character set that can be encoded using 8-, 16-, or 32-bit character sizes. All existing character sets in 8859 are included as pages in the 10646 encoding, along with virtually all known characters on the planet. The 10646 is effectively the dictionary of coded character sets.

Unicode is an implementation of ISO 10646 that defines a set of 16-bit characters and is not exactly a superset of 8859.

3.14.1.8.2 Alternative specifications. There are no alternatives for a universal character set.

3.14.1.8.3 Standards deficiencies. Only a small number of modern languages are unrepresentable by these satndards, but are expected to be supported soon.

3.14.1.8.4 Portability caveats. The portability problems with universal character sets involve their multi-byte nature. Translation to and from single-byte sets is full of chances for errors.

3.14.1.8.5 Related standards. There are no related standards.

3.14.1.8.6 Recommendations. If multiple-octet representations (16- or 32-bit) of characters are required, ISO 10646 is recommended.

3.14.1.9 Currency and funds representation. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Covers characters for and the representation of currency and monetary values.

3.14.1.9.1 Standards. Table 3.14-9 presents standards for currency and funds representation.

TABLE 3.14-9 Currency and funds representation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Codes for the Representation of Currencies and Funds	4217:1990	Informational (Approved)

3.14.1.9.2 Alternative specifications. There are no alternative specifications.

3.14.1.9.3 Standards deficiencies. Deficiencies in the standard are unknown.

3.14.1.9.4 Portability caveats. Portability problems in the standard are unknown.

3.14.1.9.5 Related standards. Numerical value representation standards and internationalization locale specifications are related.

3.14.1.9.6 Recommendations. ISO 4217 is recommended.

3.14.1.10 Country name representation. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) These standards provide for a short character combination that can be used to represent the names of countries.

3.14.1.10.1 Standards. Table 3.14-11 presents standards for country name representation.

TABLE 3.14-10 Country name representation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	NIST	Countries, Dependencies, Areas of Special Sovereignty and their Principal Administrative Divisions	FIPS PUB 10-4 April 1995	Informational (Approved)
GPC	NIST	American National Standard codes for Representation of Names of Counties, Dependencies, Areas of Special Sovereignty and their Principal Administrative Divisions	FIPS PUB 104-1	Informational (Approved)
IPC	ISO	Codes for Representation of Names of Countries	3166:1993	Informational (Approved)

ISO 3166 defines a 2-letter, a 3-letter, and a numeric code for each country. The 2-letter names are well-known and accepted as internet domain names. The 3-letter codes are often used in international sports.

3.14.1.10.2 Alternative specifications. Alternative specifications would include the international codes to designate the country of registration of automobiles.

3.14.1.10.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.14.1.10.4 Portability caveats. Portability problems with the existing standards are unknown.

3.14.1.10.5 Related standards. There are no related standards.

3.14.1.10.6 Recommendations. There is no recommendation.

3.14.1.11 Representation of human sexes. This BSA concerns the uniform representation of human sexes for the interchange of information.

3.14.1.11.1 Standards. Table 3.14-12 presents standards for representation of human sexes.

TABLE 3.14-11 Representation of human sexes standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Representation of Human Sexes	5218:1977	Informational (Approved)

3.14.1.11.2 Alternative specifications. There are no alternative specifications.

3.14.1.11.3 Standards deficiencies. ISO 5218 does not meet the requirements of specific medical or scientific applications.

3.14.1.11.4 Portability caveats. ISO 5218 does not prescribe file sequences, storage, media, programming languages, or other features of information processing to be used in its implementation.

3.14.1.11.5 Related standards. No related standards have been identified.

3.14.1.11.6 Recommendations. ISO 5218 is recommended for use.

3.14.1.12 Representation of names of languages. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) This BSA presents standards for code to represent the names of languages.

3.14.1.12.1 Standards. Table 3.14-13 presents standards for representation of names of languages.

TABLE 3.14-12 Representation of names of languages standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Code for the Representation of Names of Languages	639:1988	Informational (Approved)
NPC	ANSI/NISO	Codes for Representation of Languages for Information Interchange	Z39.53	Informational (Approved)

3.14.1.12.2 Alternative specifications. Alternative specifications may include abbreviations in common use in entomology.

3.14.1.12.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.14.1.12.4 Portability caveats. Portability problems in the existing standards are unknown.

3.14.1.12.5 Related standards. The following standards are related to representation of names of languages:

a. ISO 9:1995: Transliteration of Cyrillic Characters into Latin Characters - Slavic and Non-Slavic Languages

b. ISO 233-2:1993: Information and documentation - Transliteration of Arabic Characters into Latin Characters - Part 2: Arabic Language - Simplified Transliteration

c. ISO 3602:1989: Documentation - Romanization of Japanese (kana script)

d. ISO DIS 14962: ASCII encoded English

3.14.1.12.6 Recommendations. ISO 639 is recommended.

3.14.1.13 Date and time representation. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Date and time representation and storage require consideration and standardization. Problems include representation of twelve or twenty-four hour time, the order in which the day and month are presented, and dropping of the century digits from the year.

3.14.1.13.1 Standard. Table 3.14-13 presents standards for date and time representation.

TABLE 3.14-13 Date and time representation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Defense Data Dictionary System (DDDS), Version 3.2, May 1996	DDDS Ver. 3.2	Mandated (Approved)
GPC	NIST	Representation of Calendar Date and Ordinal Date for Information Interchange (adopts ANSI X3.30-1985/R1991)	FIPS PUB 4-1:1988 Change Notice 3/25/96	Informational (Approved)
GPC	NIST	Representation of Local Time of the Day for Information Exchange (adopts ANSI X3.43-1986)	FIPS PUB 58-1:1988	Informational (Approved)
GPC	NIST	Representations of Universal Time, Local Time Differentials, and US Time Zone References for Information Interchange (Adopts ANSI X3.51-1979)	FIPS PUB 59:1979	Informational (Approved)
IPC	ISO	Representation of Dates and Times	8601:1988	Informational (Approved)
NPC	ANSI	Representation of Calendar Date and Ordinal Date for Information Interchange	X3. 30-1985 (R1991)	Informational (Approved)
NPC	ANSI	Representation of Local Time of Day for Information Interchange	X3. 43-1986 (R1992)	Informational (Approved)
NPC	ANSI	Representations of Universal Time, Local Time Differentials, and US Time Zone References	X3. 51-1994	Informational (Approved)
NPC	ANSI/EIA	Source and Date Code Marking	476-A:1987	Informational (Approved)

3.14.1.13.2 Alternative specification. There are no other available specifications.

3.14.1.13.3 Standard deficiencies. In the early days of computer technology, information storage space was at a premium. Engineers saved space by using only the last two digits of the year rather than using full four-digit year representation since they did not anticipate that existing systems would still be in operation in the year 2000. This is a problem to be kept in mind during data design for information systems and their databases. The internal representation of the year and dates is expected to cause enormous difficulties as the year 2000 arrives.

3.14.1.13.4 Portability caveats. The difference between a little-endian (i.e., 11 May 1995), a big-endian (i.e., 1995 May 11), and mixed mode (i.e., May 11, 1995) date representation can be a portability problem for systems. The stated DoD data element for date format is "YYYYMMDD" where YYYY is the year, MM is the month, and DD is the day. NIST highly recommends that four-digit year elements be used and that two-digit year elements NOT be used for data interchange. On March 25, 1996 NIST published a change notice to FIPS 4-1 that highly recommends four-digit year elements, and states that two-year elements specified in ANSI

X3.30:1985 (R1991) should not be used for the purpose of any data interchange among U.S. Government agencies.

3.14.1.13.5 Related standards. The following standard is related to date and time representation:

a. NIST FIPS 34, Guide for the Use of International System of Units in FIPS PUBS

3.14.1.13.6 Recommendations. For purposes of data interchange, DoD requires that year, month, and day be represented as 'YYYYMMDD'.

3.14.2 Cultural convention services. These services provide the capability to store and access rules and conventions for cultural entities maintained in a cultural convention repository.

3.14.2.1 Numerical value representation. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Numerical value representation deals with the presentation of numerical values as character strings in machine- and human- readable form.

3.14.2.1.1 Standards. Table 3.14-14 presents standards for numerical value representation.

TABLE 3.14-14 Numerical value representation standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO	Representation of Numerical Values in Character Strings for Information Interchange	6093:1985	Informational (Approved)

ISO 6093 specifies three presentations of numerical values as [illegible] machine-readable form for data interchange.

3.14.2.1.2 Alternative specifications. There are no alternative specifications.

3.14.2.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.14.2.1.4 Portability caveats. Portability problems in the existing standards are unknown.

3.14.2.1.5 Related standards. The following standards are related to numerical value representation:

a. Representation of currency

b. Representation of date/time

c. Localization

d. ANSI X3.50 1986/R1992: Representation for U.S. Customary, SI, and other Units to be used in Systems with limited character sets

e. ISO 2955:1993 - Representation of SI and other Units in Systems with limited Character Sets

3.14.2.1.6 Recommendations. ISO 6093 is recommended.

3.14.2.2 Customization to local norms. (This BSA appears in part 3, User Interface, part 13, Human Factors, and part 14, Internationalization.) Customization to local norms involves modification of the key mapping to accommodate the local language and display of data in the commonly-used format (e.g., numbers, dates, time).

3.14.2.2.1 Standards. Table 3.14-15 presents standards for customization to local norms.

TABLE 3.14-15 Customization to local norms standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
GPC	DOD	Human-Computer Interface (HCI) Style Guide	TAFIM Volume 8, Version 3.0: 1996	Mandated (Approved)
CPC	X/Open	Internationalisation Guide, version 2	G304 (7/93)	Informational (Approved)
CPC	X/Open	Locale Registry Procedures	G303 (1993)	Informational (Approved)
CPC	OSF	Motif 1.2 (consistent with X/Open's NLS specifications & also double-byte character sets)	Motif 1.2	Informational (Approved)
CPC	MIT X Consortium	X Window System (X font manager- includes double-byte character sets)	X11R5	Informational (Approved)
NPC	ANSI/HFS	American National Standard for Human Factors Engineering of Visual Display Terminal Workstations	100-1988	Informational (Approved)
GPC	DOD	Military Standard Keyboard Arrangements	MIL-STD-1280, Notice 1, 1969	Informational (Approved)
GPC	DOD	User/Computer Interface	MIL-STD-1801 29 May 1987	Informational (Approved)
GPC	DOD	Human Engineering Performance Requirements for Systems	MIL-STD-1800A 10 Oct. 1990	Informational (Approved)
GPC	DOD	DOD Handbook, Human Engineering Guidelines for Management Information Systems	MIL-HDBK-761A 30 Sep. 1989	Informational (Approved)
GPC	DOD	Guidelines for Designing User Interface Software	ESD-TR-86-278	Informational (Approved)
GPC	DOD	Department of Defense Intelligence Information Systems Style Guide	DODIIS Style Guide, 10/91	Informational (Approved)
GPC	DOD	Air Force Intelligence Data Handling System (IDHS) Style Guide	IDHS Style Guide 1990	Informational (Approved)
GPC	DOD	Human Factors Guidelines for the Army Tactical Command and Control System (ATCCS) Soldier-Machine Interface	ATCCS Guidelines v.1.0 and v.2.0, 1990 and 1992	Informational (Approved)
GPC	DOD	The User Interface Specifications for Navy Command and Control Systems	Navy CCS, Version 1.1, 1992	Informational (Approved)
GPC	DOD	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	MIL-STD-1472D Notice 2, 30 June 1992	Informational (Approved)
GPC	DOD	Human Engineering Guidelines for Management Information Systems	DOD-HDBK-71A (DOD 1989c)	Informational (Approved)
CPC	X/Open	Distributed Internationalisation Services	S213 (11/92)	Informational (Approved)

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
CPC	X/Open	Internationalization of Internetworking Specifications	S302 (4/93)	Informational (Approved)
CPC	X/Open	File System Safe UCS Transformation Format (FSS-UTF)	P316 (1993)	Informational (Approved)
CPC	X/Open	System Interface and Headers, Issue 3	C212 (3/92)	Informational (Approved)
CPC	X/Open	Supplementary Definitions, Issue 3	C213 (3/92)	Informational (Approved)
CPC	X/Open	Universal Multiple-Octet Coded Character Set Coexistence and Migration	E401 (3/94)	Informational (Approved)
NPC	ANSI/SAE	Human Interface Design Methodology for Integrated Display Symbology	ARP 4155 (1990)	Informational (Approved)
GPC	DOD	Human Engineering Requirements for Military Systems, Equipment, and Facilities	MIL-STD-46855B 26 May 1994	Informational (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interface Definitions, Issue 4, Version 2 (part of XPG4)	C434 (9/94)	Informational (Approved)
CPC	X/Open	Single Unix Specification (Spec. 1170), System Interfaces and Headers, Issue 4, Version 2, (Part of XPG4)	C435 (9/94)	Informational (Approved)
CPC	X/Open	Locale Registry Procedures, Version 2	G502 (5/95)	Informational (Approved)
CPC	OSF	Motif	Motif 2.0	Informational (Approved)
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

DODI 8120 mandates use of the DOD HCI Style Guide.

Motif 1.2 is the current version of the OSF specification for GUI behavior and appearance and programming and data interfaces. X11R5 is the current release of Version 11 of the X Windows standard.

3.14.2.2.2 Alternative specifications. Several applicable consortia or de facto style guides are available for internationalization. However, conformance with one or more the style guides listed below does not guarantee conformance with ergonomic standards:

a. The Windows Interface: An Application Design Guide (Microsoft)

b. Object-Oriented Interface design: IBM Common User Access Guidelines (IBM)
c. Macintosh Human Interface Guideiines (Apple Computer).

3.14.2.2.3 Standards deficiencies. Currently, conformance to parts 12-17 of the ISO 9241 standard is on a part-by-part basis. There is concern that the overal standard may thus fail to address potential ergonomic problems arising from interactions between the user interface elements covered by the individual parts.

3.14.2.2.4 Portability caveats. Although Morif supports the X/Open Native Language System, it also aupports a number of its own internationalization extensions which makes it compatible with some legacy applications (e.g., OpenLook).

NIST FIPS 158-1 (User Interface Componenet of the Applications Portability Profile) mandates the use of the X Window protocol, X library, and X toolkit intrinsics. IEEE P1201.2, when completed, is intended to increase the level of user interface consistency (and thus user interface portability) across X Windows-based environments. There are potential conflicts here.

The DOD HCI Style Guide is based on (and intended to supersede) the Army, Navy, Air Force, and DODIIS Style Guides cited in the table above. The goal of this effort is to minimize unnecessary user interface diversity across DOD systems. There are potential problems with systems designed to accommodate different style guides.

3.14.2.2.5 Related standards. The following standards are related to cultural convention services:

a. X/Open Internationalisation Locale: L001 (1994): ja_JP - Japanese for Japan.

b. X/Open Internationalisation Locale: L002 (1994): da_DK - Danish for Denmark.

c. X/Open Internationalisation Locale: L003 (1994): de_AT - German for Austria.

d. X/Open Internationalisation Locale: L004 (1994): en_DK - English for Denmark.

e. X/Open Internationalisation Locale: L005 (1994): fo_FO - Faroese for the Faroes.

f. X/Open Internationalisation Locale: L006 (1994) is_IS - Icelandic for Iceland.

g. X/Open Internationalisation Locale: L007 (1994) kl_GL - Greenlandic for Greenland.

h. X/Open Internationalisation Locale: L008 (1994) lt_LT - Lithuanian for Lithuania.

i. X/Open Internationalisation Locale: L009 (1994): lv_LV - Latvian for Latvia.

j. X/Open Internationalisation Locale: L010 (1994): de_CH - German for Switzerland.

k. X/Open Internationalisation Locale: L011 (1994): de_DE - German for Germany.

l. X/Open Internationalisation Locale: L012 (1994): en_GB - English for Great Britain.

m. X/Open Internationalisation Locale: L013 (1994): en_IE - English for Ireland.

n. X/Open Internationalisation Locale: L014 (1994): en_US - English for the U.S.A.

o. X/Open Internationalisation Locale: L015 (1994): hu_HU - Hungarian for Hungary.

p. X/Open Internationalisation Locale: L016 (1994): it_IT - Italian for Italy.

q. X/Open Internationalisation Locale: L017 (1994): nl_NL - Dutch for the Netherlands.

r. X/Open Internationalisation Locale: L018 (1994): pl_PL - Polish for Poland.

s. X/Open Internationalisation Locale: L019 (1994): pt_PT - Portuguese for Portugal.

t. X/Open Internationalisation Locale: L020 (1994): ro_RO - Romanian for Romania.

u. MIL-STD-1794 (1986) Human Factors Engineering Program for ICBM Systems.

v. MIL-STD-1908 (1992) Definitions of Human Factors Terms.

w. DOD-HDBK-763 (1987) Human Engineering Procedures Guide.

3.14.2.2.6 Recommendations. Procurements that require software user interfaces to be addressed by ergonomic standards can require conformance with standards for menu structures, command languages, direct manipulation dialogs, forms-based dialogs, windowing, icons, screen formatting, information coding, and user guidance.

Parts 1 and 2 of the ISO 9241 standard are informative; parts 10 and 11 are expected to be informative on completion. Part 3 of the ISO 9241 standard is normative; parts 2-9 and 12-17 are expected to be normative on completion. Conformance with the overall ISO 9241 standard is based on conformance with all normative parts that apply to a particular product.

Procurements must recognize the difference between informative and normative parts of the standard in question. Where possible, both the informative and normative parts should be required for the best implementation of modern human factors/ergonomic thinking. In general, conformance tests for informative parts will not be available.

The DOD HCI Style Guide is recommended for customization to local norms.

3.14.3 Natural language support services. These services provide the capability to support several languages simultaneously.

3.14.3.1 Keyboard device layout. (This BSA appears in both part 3, User Interface, and part 14, Internationalization.) Keyboard device layout standards specify the arrangement of keys on a keyboard.

3.14.3.1.1 Standards. Table 3.14-16 presents standards for keyboard device layout.

TABLE 3.14-16 Keyboard device layout standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Keyboard Layouts for Text and Office Systems	9995-1..8:1994	Mandated (Approved)
GPC	DOD	Military Standard Keyboard Arrangements	MIL-STD-1280, Notice 1, 1969	Informational (Approved)
NPC	ANSI	Allocation of Letters to the Keys of Numeric Keypads	T1.703 (1995)	Informational (Approved)
NPC	ANSI	Coded Character Sets for Keyboard Arrangement in ANSI X4.23-1982 and X4.22-1983	X3.114-1984 (R1991)	Informational (Approved)
NPC	ANSI	Keyboard Arrangement	X3.154-1988	Informational (Approved)
NPC	ANSI	Alternate Keyboard Arrangement	X3.207-1991	Informational (Approved)
CPC	XAOpen	Key Values (in Window Management, Issue 3)	XPG3 Vol. 6 C216	Informational (Approved)
IPC	ISO	Keyboard Layouts for Numeric Applications	3791:1976	Informational (Approved)
IPC	ISO/IEC	Numeric Keyboard for Home Electronic Systems (HES)	946:1988	Informational (Approved)
IPC	ISO/IEC	Character Repertoire, Keyboard Layouts for Languages Using Latin Alphabet	11581 (1994)	Informational (Canceled)
IPC	ISO	Ergonomic requirements for Office work with Visual Display Terminals (VDTs) part 4: Keyboard requirements	9241-4	Informational (Draft)
IPC	ISO	Keyboard for Information Interchange Processing Equipment Using the 150 7-Bit Coded Character Set - Alphanumeric Area	2530:1993	Informational (Superseded)
IPC	ISO	Keyboard Layouts for Text/Office Systems	9241:1992	Informational (Superseded)
IPC	ISO	Keyboard Layouts for Text/Office Systems	9241:1993	Informational (Superseded)
IPC	ISO	Keyboard Layouts for Text/Office Systems	9995:1987	Informational (Superseded)
NPC	ANSI	Keyboard Arrangement	X4.22-1983	Informational (Superseded)

3.14.3.1.2 Alternative specifications. The only other available specifications are proprietary.

3.14.3.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.14.3.1.4 Portability caveats. Portability problems related to the existing specifications are unknown.

3.14.3.1.5 Related standards. No standards are related to keyboard device layout standards.

3.14.3.1.6 Recommendations. Conformance to all ISO and ISO/IEC keyboard specifications conforming to DIS or IS levels is recommended. This is especially important for equipment that will interoperate with that of U.S. allies (e.g., NATO).

3.14.4 Related standards and programs. This MLSA includes services supporting internationalization indirectly.

3.14.4.1 Character set registration. (This BSA appears in part 5, Data Interchange, and part 14, Internationalization.) Character set registration provides a mechanism for identifying and defining graphic character sets

3.14.4.1.1 Standards. Table 3.14-17 presents standards for character set registration.

TABLE 3.14-17 Character set registration standards

Standard Type	Sponsor	Standard	Standard Reference	Status DoD (Lifecycle)
IPC	ISO/IEC	Registration of Repertoires of Graphic Characters from ISO/IEC 10367	7350:1991	Informational (Approved)
IPC	ISO	Procedure for registration of escape sequences	2375:1985	Informational (Approved)

ISO 7350 spceifies procedures for preparing, registering, publishing, and maintaining the register of graphic character sets and procedures for assigning identifiers to the sets.

3.14.4.1.2 Alternative specifications. There are no alternative specifications.

3.14.4.1.3 Standards deficiencies. Deficiencies in the existing standards are unknown.

3.14.4.1.4 Portability caveats. Portability problems in the existing standards are unknown.

3.14.4.1.5 Related standards. The following standards are related to character set registration:

a. Character set standards
b. Localization standards
c. Symbols for use with data such as currency, date, time, numerical values

3.14.4.1.6 Recommendations. There are no recommendations.