Enterprise

Department of the Army Technical Architecture

Version 4.5

12 November 1996

<u>DISTRIBUTION STATEMENT A</u> Approved for public release; distribution is unlimited.

Army Technical Architecture Version 4.5

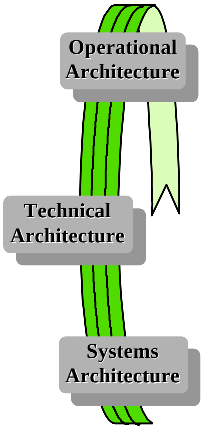
Executive Summary

INTRODUCTION

One of the underlying tenets of information-age warfare is that "*shared situation awareness, coupled with the ability to conduct continuous operations, will allow information age armies to observe, decide, and act faster, more correctly and more precisely than their enemies*"(1) This presupposes that information is reliable, timely, available, usable, and shared. The underlying information infrastructure must, therefore, facilitate rather than inhibit (e.g., stove-pipe) the flow of information between sustaining base agencies and strategic/tactical force elements and provide the flexibility to accommodate different missions and organizational structures.

In the absence of a common and enforced Technical Architecture (TA), most information and embedded systems have been developed with their own (sometimes unique and frequently closed) infrastructures resulting in various message sets, various information processing and information transport architectures. Interoperability has been problematic and expensive, accomplished through the development and maintenance of unique interfaces. As a result, the Services lack an integrated information architecture and continue to rely on "black-box" solutions.

A Technical Architecture is a set of "building codes". By itself it builds nothing. However, used in conjunction with the other Enterprise Architectures -- the Operational and Systems Architectures -- the adoption and enforcement of the TA will foster interoperability between systems, as well dramatically reduce cost, development time, and fielding time for improved systems.



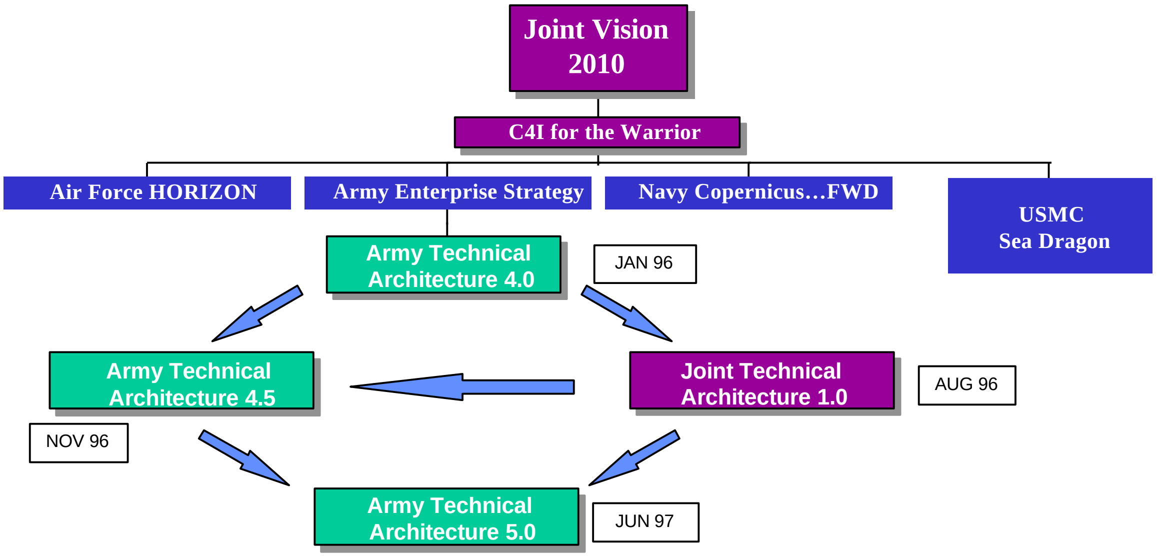
- ➢ *Operational Architecture (OA)* is the total aggregation of missions, functions, tasks, information requirements, and business rules
- ➢ *Technical Architecture* is the "building codes" upon which systems are based
- ➢ *Systems Architecture* is the physical implementation of the OA, the layout and relationship of systems and communications

SCOPE

The Army Technical Architecture (ATA) applies to all systems that produce, use, or exchange information electronically. The ATA will be used by anyone involved in the management, development or acquisition of new or improved systems. Within the Army, the Vice Chief of Staff, Army and the Army Acquisition Executive have jointly made each Milestone Decision Authority (MDA), Major Army Command (MACOM), Program Executive Officer (PEO), Program or Product Manager (PM), Advanced Technology Demonstration (ATD) Manager, Advanced Concept and Technology Demonstration (ACTD) Manager, and Advanced Concept and Technology (ACT) II Manager responsible for compliance with this ATA. System developers will comply with the ATA in order to ensure that products meet interoperability, performance, and sustainment criteria. Combat developers will use the ATA in developing requirements and functional descriptions. Battle Labs will use the ATA to ensure that the fielding of their "good ideas" is not unduly delayed by the cost and time required for wholesale reengineering to meet interoperability standards. Compliance with ATA standards will be included as an evaluated requirement in all acquisitions.

BACKGROUND

The first Army Technical Architecture, Version 3.1, was published on 31 March 1995. This version was mandated for use by the Army Acquisition Community with a requirement to provide a plan for migrating all systems to conform to the mandated standards. Results from a review of many of these plans, plus numerous comments from the field, provided the basis for ATA Version 4.0. This version incorporated improvements as well as expanded the scope to address Weapons Systems, Sustaining Base Systems, and Information Security. Since information exchanged between weapons systems often travels via C3I systems, the standards in Version 3.1 of the TA remained the core and baseline of this expanded ATA. In order to be more discriminating in the applicability of standards and to extend the ATA without complicating the base document, Version 4.0 added appendices for each of four focus areas or “domains” - Sustaining Base & Office Automation, C3I, Weapons, and Modeling & Simulation. ATA Version 4.5 builds upon the expanded groundwork of ATA Version 4.0, updates evolving mandated and emerging standards, and aligns existing C4I-oriented mandates with the Joint Technical Architecture (JTA). Due to its broader scope, the ATA Version 4.5 will continue to be the central source of Technical Architecture guidance for Army systems.



WHAT'S NEW IN VERSION 4.5

This version updates existing ATA standards, fixes several errors, and makes selected emerging standards that have sufficiently matured mandatory. It also brings the ATA into substantial alignment with Version 1.0 of the JTA, issued 22 August 1996. Changes include:

- Architecture Definitions and document background updated to reflect influence of Joint Vision 2010 and the Joint Technical Architecture.
- Designates the ATA as the Army's mechanism to implement Army and DOD technical standard initiatives.
- Updated Common Operating Environment (COE) references to the latest Defense Information Infrastructure (DII) COE version.
- Added Joint Task Force LAN connection standard.
- Moved LAN Emulation over ATM (LANE) standard from emerging to mandate.
- Added emerging standards for Mobile Cellular telephony and Personal Communications Services (PCS).
- Update Military Symbology mandate to MIL-STD-2525A.
- Updated domain HCI Style Guides.
- Updated several information security standards.
- In C3I Domain Appendix, moved from GCCS COE to DII COE.
- In Weapons System Domain Appendix, added MIL-STD-1477B as Military Symbology extension for missile defense domain.
- In Modeling and Simulation Domain Appendix added High Level Architecture (HLA) mandate.

A more comprehensive catalogue of changes made to ATA Version 4.5 with respect to the ATA Version 4.0 is contained in Appendix H of the ATA. It is available online at a World Wide Web address (URL) of "http://www.hqda.army.mil/webs/techarch".

Our ultimate objective is to provide the Warfighter
with a seamless flow of timely, accurate, accessible, and secure information
that gives our forces a decisive edge.

(1) *War in the Information Age*, General Gordon R. Sullivan and Colonel James M. Dubik, June 1994.

Office, Director of Information
Systems for Command, Control
Communications, & Computers
SAIS-ADM

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Implementation of the Army Technical Architecture Version 4.5

References:
a. Memorandum, DACS-ZB/SARD, 30 Jan 1996, Subject: Implementation of the Army Technical Architecture.

b. Memorandum, DACS-ADO, 17 Oct 96, Subject: Army Technical Architecture (ATA) Migration Planning Guidance and Procedures.

Version 4.5 of the Army Technical Architecture (ATA) has completed the configuration management process and is approved for implementation. It is another step along the path toward a seamless, efficiently integrated Army and Joint Information Technology Architecture. The ATA remains the Army's central source of technical guidance for interoperability, integrating standards from the recently approved Joint Technical Architecture (JTA) as well as other architecture and open systems initiatives.

This version updates existing ATA standards, fixes several errors, and mandates selected emerging standards that have sufficiently matured. This release also brings the ATA into substantial alignment with version 1.0 of the JTA, issued 22 August 1996. A summary of changes is contained in the ATA Version 4.5 Executive Summary.

ATA Version 4.5 is mandatory for use in all acquisitions of Information Technology. It supersedes ATA version 4.0 which will continue to be used in Migration Plans and procurements that are already underway. In accordance with Migration Plan processing procedures in reference b, existing migration plans either approved or in progress that were baselined on ATA Version 4.0 need not be changed at this time. They will be updated to reference the current version of the ATA during their next required revision.

ATA Version 4.5 as well as other ATA documentation is available for view and download on the World Wide Web (WWW) at URL "http://www.hqda.army.mil/webs/techarch/". POC for the ATA is Ms. Jean Gilleo, (703) 697-4189, Email: Gilleej@hqda.army.mil.

OTTO J. GUENTHER
LTG, GS
DIRECTOR

DISTRIBUTION:

Office of the Deputy Undersecretary of the Army (Operations Research),
ATTN: SAUS-OR, 102 Army Pentagon, Room 2E660, Washington, DC 20310-0102

Office of the Assistant Secretary of the Army (Research, Development, and Acquisition),
ATTN: SARD-ZB, 103 Army Pentagon, Room 2E672, Washington, DC 20310-0103

Army Science Board, ATTN: SARD-ASB, 103 Army Pentagon, Room 3E359,
Washington, DC 20310-0103

Office of the General Counsel, ATTN: SAGC, 104 Army Pentagon, Room 2E725,
Washington, DC 20310-0104

Office of the Administrative Assistant, ATTN: SAAA, 105 Army Pentagon, Room
3E733, Washington, DC 20310-0105

Director of Information Systems for Command, Control, Communications and
Computers, ATTN: SAIS-ZA, 107 Army Pentagon, Washington, DC 20310-0107

Louisiana Maneuvers Task Force, ATTN: DACS-LAM, 200 Army Pentagon, Room
2B486, Washington, DC 20310-0200

Director of the Army Staff, ATTN: DACS-DPA, 202 Army Pentagon, Room 3E665,
Washington, DC 20310-0202

Deputy Chief of Staff for Personnel, ATTN: DAPE-ZA, 300 Army Pentagon, Room
2E736, Washington, DC 20310-0300

Deputy Chief of Staff for Operations and Plans, ATTN: DAMO-ZA, 400 Army
Pentagon, Room 3E634, Washington, DC 20310-0400

Director of Requirements (Horizontal Technology Integration), Office of the Deputy
Chief of Staff for Operations and Plans, 460 Army Pentagon, Room 3A522,
Washington, DC 20310-0460

Deputy Chief of Staff for Logistics, ATTN: DALO-ZA, 500 Army Pentagon, Room
3E560, Washington, DC 20310-0500

Deputy Chief of Staff for Intelligence, ATTN: DAMI-ZA, 1000 Army Pentagon, Room
2E464, Washington, DC 20310-1000

Inspector General, ATTN: SAIG-ZA, 1700 Army Pentagon, Room 1E736, Washington,
DC 20310-1700

Office of the Judge Advocate General, ATTN: DAJA-ZA, 2200 Army Pentagon, Room
2E444, Washington, DC 20310-2200

Chief, Army Reserve, ATTN: DAAR-ZA, 2400 Army Pentagon, Room 3E390,
Washington, DC 20310-2400

Director, Army National Guard, ATTN: NGB-ARZ, 2500 Army Pentagon, Room 2E408,
Washington, DC 20310-2500

Chief of Engineers, ATTN: DAEN-ZA, 20 Massachusetts Ave NW, Washington , DC
20314-1000

Office of the Surgeon General, ATTN: DASG-ZA, Room 672, 5109 Leesburg Pike,
Falls Church, VA 22041-3258

Director, CECOM RDEC, ATTN: AMSEL-RD, Fort Monmouth, NJ 07703-5201

Director, MICOM RDEC, ATTN: AMSMI-RD, Redstone Arsenal, AL 35898-5250

Director, Strategic Logistics Agency, ATTN: LOSA, 5001 Eisenhower Ave,
Alexandria, VA 22333

Director, US Army Materiel Systems Analysis Activity, ATTN: AMXSY-CR, Aberdeen
Proving Ground, MD 21005

COMMANDER-IN-CHIEF

US Army, Europe and Seventh Army, ATTN: AEAIM, Unit 29351, APO AE 09014

COMMANDER

US Army Communications-Electronics Command and Fort Monmouth,
ATTN: AMSEL-CG, Fort Monmouth, NJ 07703-5000

US Army Corps of Engineers, ATTN: CECG, 20 Massachusetts Ave NW,
Washington, DC 20314-1000

US Army Forces Command, ATTN: DCS, Fort McPherson, GA 30330

US Army Health Services Command, ATTN: HSIM, Fort Sam Houston, TX
78234-6000

US Army Information Systems Command, ATTN: ASCG, Fort Huachuca, AZ
85613-5000

US Army Information Systems Engineering Command, ATTN: ASQB-OCG, Fort
Huachuca, AZ 85613-5000

US Army Intelligence and Security Command, ATTN: IACG, Fort Belvoir, VA
22060-7040

US Army Materiel Command, ATTN: AMCDCG, 5001 Eisenhower Ave, Alexandria,
VA 22333-0001

US Army Medical Command, ATTN: MCCG, Fort Sam Houston, TX 78234-6000

US Army Medical Research and Materiel Command and Fort Detrick,
ATTN: MCMR-ZA, Fort Detrick, MD 21702-5012

US Army MilitaryTraffic Management Command, ATTN: MTCG,
5611 Columbia Pike, Falls Church, VA 22041-5050

US Army Operational Test and Evaluation command, ATTN: CSTE-ZA, Park Center
IV, 4501 Ford Ave., Alexandria, VA 22302-1458

US Army, Pacific ATTN: APCG, Fort Shafter, HI 96858-5100

US Army Signal Center and Fort Gordon, ATTN: ATZH-CG, Fort Gordon, GA
30905-5000

US Army Simulations, Training and Instrumentation Command, ATTN: AMSTI-CG,
12350 Research Parkway, Orlando, FL 32826-3276

US Army Space and Strategic Defense Command, 1941 Jefferson Davis Highway,
Suite 900, Arlington, VA 22215-0280

US Army Special Operations Command, ATTN: AOCG, Fort Bragg, NC 28307-5200

US Army Test and Evaluation command, ATTN: AMCG, Aberdeen Proving Ground,
MD 21005-5055

US Army Training and Doctrine Command, ATTN: ATDC, Fort Monroe, VA
23651-5000

US Forces Korea, APO AP 96205-0010

US Military District of Washington, 103 3rd Street, Fort Lesley J. McNair,
Washington, DC 20319-5058

PROGRAM EXECUTIVE OFFICER

Armored Systems Modernization, US Army TACOM, ATTN: SFAE-ASM, Warren, MI
48397-5000

Aviation, ATTN: SFAE-AV, 4300 Goodfellow Blvd., St. Louis, MO 63120-1798

Command, Control, and Communications Systems, ATTN: SFAE-C3S, Fort Monmouth,
NJ 07703-5000

Field Artillery Systems, ATTN: SFAE-FAS, Picatinny Arsenal, NJ 07806-5000

Intelligence and Electronic Warfare, ATTN: SFAE-IEW, Fort Monmouth, NJ
07703-5000

Missile Defense, ATTN: SFAE-MD-HSV, PO Box 1500, Huntsville, AL 35807-3801

Reserve Component Automation System, 8510 Cinder Bed Road, Suite 1000,
Newington, VA 22122-8510

Standard Army Management Information Systems, ATTN: SFAE-PS, 9350 Hall Road,
Suite 142, Fort Belvoir, VA 22060-5526

Tactical Missiles, ATTN: SFAE-MSL, Redstone Arsenal, AL 35898-8000

Tactical Wheeled Vehicles, ATTN: SFAE-TWV, Warren, MI 48397-5000
Ground Combat Support Systems. ATTN: SFAE-GCSS-W, Warren, MI 48397-5000

PROGRAM MANAGER
Chemical Demilitarization, ATTN: SFAE-CD-Z, Bldg. E4585, Aberdeen Proving
   Ground, MD 21010-5401
Joint Program Management Office for Biological Defense, ATTN: SFAE-BD,
   5201 Leesburg Pike, Skyline 3, Room 1200, Falls Church, VA 22041-3203

Department of the Army
Technical Architecture

Version 4.5
12 November 1996

INTERNET AVAILABILITY

This document is available electronically on the World Wide Web (WWW) at Uniform Resource Locator (URL) "http://www.hqda.army.mil/webs/techarch/". The electronic version contains “HotLinks” to many of the referenced standards.

COMMENTS ON THE ARMY TECHNICAL ARCHITECTURE

To speed processing and consideration, comments and suggested changes should be submitted electronically via Email. Comments submitted as attached word processing documents should be in either Microsoft Word 6.0 or WordPerfect 5.2 format.

Send Email comments to “techarch@HQDA.Army.mil”.

This is where all comments are received and logged. A reference number will be assigned and we will send you an acknowledgment of your comment. Receiving comments by Email allows us to rapidly address your comment and make the necessary changes in the next revision.

Your comment should include the following information: name, organization, phone number, recommended change including section number, and reason. Comments should be as specific as possible, referencing a specific standard or section and providing recommended changes with a brief justification for each change.

More information and an example can be found on the WWW at URL "http://www.hqda.army.mil/webs/techarch/faq.htm".

TRADEMARKS AND REFERENCES

Trademarked names appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the publisher states that it is using the names only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Appendix B contains a list of references that provide the full citation for each reference found in the document.

This page was intentionally left blank.

TABLE OF CONTENTS

SECTION **PAGE**

This page was intentionally left blank.

SECTION 1
TECHNICAL ARCHITECTURE OVERVIEW

1.1 INTRODUCTION

1.1.1 Purpose

The Army's Technical Architecture (ATA) has three mutually supporting objectives. First and foremost, to provide the foundation for a seamless flow of information and interoperability among all tactical, strategic, and sustaining base systems that produce, use, or exchange information electronically. Second, to provide guidelines and standards for system development and acquisition that will dramatically reduce cost, development time, and fielding time for improved systems. Third, to influence the direction of the information industry's technology development and research & development investment so that it can be more readily leveraged in Army systems.

This section provides an overview of the ATA. It describes the purpose, scope, and background of the ATA, what is new in this version and what is covered by each section.

1.1.2 Architectures Defined

An architecture is defined in the Institute of Electrical and Electronic Engineers (IEEE) 610.12 as the structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time. DOD has implemented this by defining an interrelated set of architectures: Operational, Systems, and Technical. The diagram below, Figure 1-1, shows the relationship among the three architectures. The definitions are provided here to ensure a common understanding of the different types of architectures and how the ATA fits into the overall scheme.

1.1.2.1 Technical Architecture

A Technical Architecture (TA) is the minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The technical architecture identifies the services, interfaces, standards, and their relationships. It provides the technical guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed.

1.1.2.2 Operational Architecture

An Operational Architecture (OA) is a description (often graphical) of the operational elements, assigned tasks, and information flows required to support the warfighter. It defines the type of information, the frequency of the exchange, and what tasks are supported by these information exchanges.

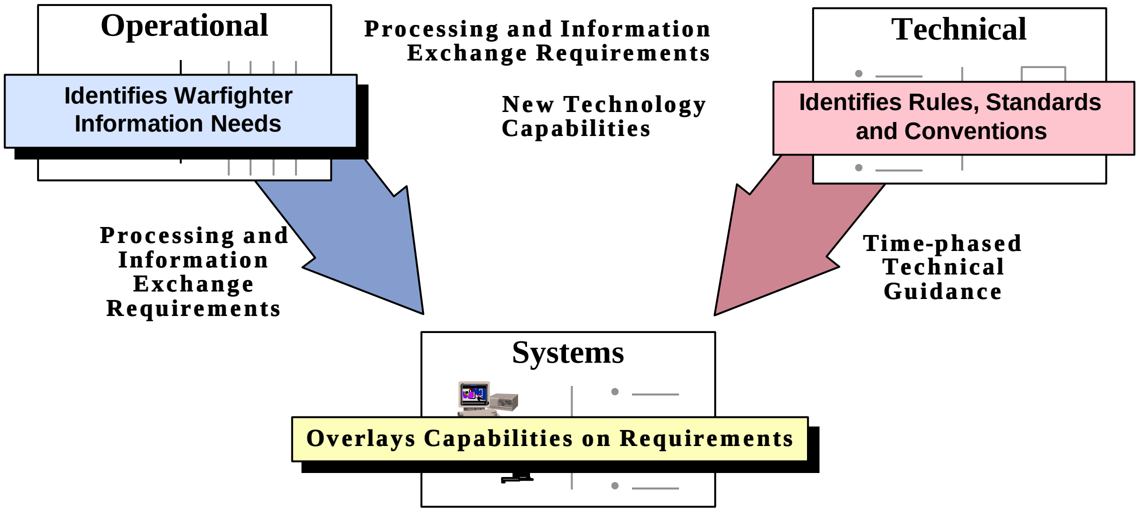

Operational
Identifies Warfighter Information Needs
Processing and Information Exchange Requirements
New Technology Capabilities
Technical
Identifies Rules, Standards and Conventions
Processing and Information Exchange Requirements
Time-phased Technical Guidance
Systems
Overlays Capabilities on Requirements

FIGURE 1-1. THE DIFFERENT ARCHITECTURES

1.1.2.3 Systems Architecture

A Systems Architecture (SA) is a description, including graphics, of the systems and interconnections providing for or supporting a warfighting function. The SA defines the physical connection, location, and identification of the key nodes, circuits, networks, warfighting platforms, etc., and allocates system and component performance parameters. It is constructed to satisfy Operational Architecture requirements in the standards defined in the Technical Architecture. The SA shows how multiple systems within a domain or an operational scenario link and interoperate, and may describe the internal construction or operations of particular systems in the SA.

1.1.3 Scope

The ATA applies to all systems that produce, use, or exchange information electronically. The ATA will be used by anyone involved in the management, development or acquisition of new or improved systems. Within the Army, the Vice Chief of Staff, Army and the Army Acquisition Executive have jointly made each Milestone Decision Authority (MDA), Major Army Command (MACOM), Program Executive Officer (PEO), Program or Product Manager (PM), Advanced Technology Demonstration (ATD) Manager, Advanced Concept and Technology Demonstration (ACTD) Manager, and Advanced Concept and Technology (ACT) II Manager responsible for compliance with this ATA. System developers will comply with the ATA in order to ensure that products meet interoperability, performance, and sustainment criteria. Combat developers will use the ATA in developing requirements and functional descriptions. Battle Labs will use the ATA to ensure that the fielding of their "good ideas" is not unduly delayed by the cost and time required for wholesale reengineering to meet interoperability standards. Army Staff Principals will ensure that systems belonging to the Headquarters Department of the Army (HQDA) and HQDA Field Operating Agencies (FOAs) comply with the ATA.

Expanding the scope and the focus of the ATA from Version 3.1 to 4.0 required more than adding standards for weapons and sustaining base systems. It required a qualitative growth in perspective. In order to fully achieve the Force XXI vision of total, seamless integration and synchronization of military power, the Army must achieve and maintain interoperability across a continuum of several dimensions at once:

1. Among battlefield weapons systems, sensors and shooters -- tanks, aircraft, Unmanned Aerial Vehicles (UAVs);
2. Among C3I and Support systems;
3. Along the vertical and horizontal dimensions of organizational and command structures;
4. Across the Joint dimension among Army, Air Force, Navy, United States Marine Corps (USMC), JCS/Commander-in-Chief (CINC), & DISA at the lowest practical echelon;
5. Across the power projection dimension - from the sustaining base forward to the Company Command Post;
6. Across the time and technology generation dimension - to achieve backward and forward compatibility and interoperability.

The scope of ATA Version 4.5 continues to support the Army's needs over all these dimensions.

Compliance is enumerated in an implementation/migration plan. A system is compliant with the ATA if it meets, or is implementing an approved plan to meet, all applicable ATA mandates. In practical terms, progress toward compliance is assessed through a migration strategy and a planning process that considers a host of resource, management, and operational issues that affect overall system development and determine the best approach for satisfying a validated user need. Army senior leaders have set a "Mark-On-The-Wall" for systems to comply with the ATA. They have mandated that by 2000 all Division XXI systems must meet the critical interoperability standards identified in their migration plans and by 2006 ALL systems must meet ALL applicable ATA standards. The Army Digitization Office (ADO) (http://www.ado.army.mil) has the lead for monitoring progress toward compliance with the ATA.

1.1.4 Background

The evolution of national military strategy in the post cold war era and the economic reality of a shrinking budget have resulted in a new vision for the Department of Defense. This vision, sponsored by the Joint Chiefs of Staff (JCS), is Joint Vision 2010. This conceptual template articulates how America's Armed Forces will channel the vitality and innovation of its people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting. It highlights the need for information superiority, enhanced jointness, and ability to participate in Multinational Operations. It recognizes an increased reliance on information systems, technology advances, and interoperability to provide the decisive edge in combat. The associated Service visions are articulated in the following documents: The Army Strategy:*The Enterprise Vision*; The Air Force

Strategy: *Horizon*; The Navy Strategy: *Copernicus…Forward*; and the Marine Corps Strategy: *Sea Dragon*.

To achieve the principles outlined in *The Army Enterprise Vision*, the Army developed and published the *Army Enterprise Implementation Plan*. This plan provided a blueprint for migration, directed tasks to implement *The Vision*, and provided a management structure. One of the tasks of the implementation plan was that a Technical Architecture be established to support the seamless sharing of information on a worldwide basis. The plan directed the Office of the Director of Information Systems for Command, Control, Communications, and Computers (ODISC4) to develop and implement an Army Technical Architecture, with the support of various organizations. The relationship of the ATA to DOD and other Service Architectures is shown in Figure 1-2.

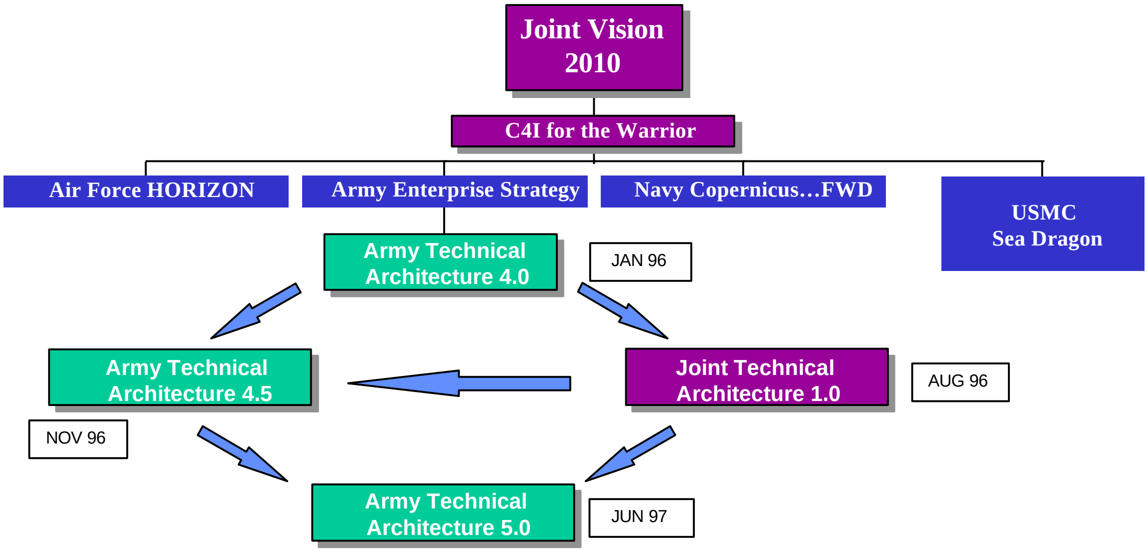


FIGURE 1-2. ATA LINEAGE

The ATA follows an azimuth set by the DOD. On 13 October 1993, the DOD issued a memorandum that included guidance for the incorporation of "interoperability, technical integration, DOD standard data, and integrated databases to provide higher quality and lower cost information technology services for all users." This memorandum further stated that "Integration implies seamless, transparent operation of DOD systems based on a shared or commonly-derived architecture (functional or technical) and standard data." On 29 June 1994, the DOD reinforced this change in direction through a memorandum, entitled "Specifications & Standards -- A New Way of Doing Business", calling for "the use of performance and commercial specifications and standards in lieu of military specifications and standards, unless no practical alternative exists". Additionally, DOD has recently published a Joint Technical Architecture (JTA) for Command, Control, Communications, Computers, and Intelligence (C4I) Systems (Note: The JTA used ATA Version 4.0 as its starting point). The ATA is fully responsive to all these mandates.

The first Army Technical Architecture, Version 3.1, was published on 31 March 1995. This version was mandated for use by the Army Acquisition Community with a requirement to provide a plan for migrating all systems to conform to the mandated standards. Results from a review of many of these plans, plus numerous comments from the field, provided the basis for ATA Version 4.0. This version incorporated improvements as well as expanded the scope to address Weapons Systems, Sustaining Base Systems, and Information Security. Since information exchanged between weapons systems often travels via C3I systems, the standards in Version 3.1 of the TA remained the core and baseline of this expanded ATA. In order to be more discriminating in the applicability of standards and to extend the ATA without complicating the base document, Version 4.0 added appendices for each of four focus areas or “domains” - Sustaining Base & Office Automation, C3I, Weapons, and Modeling & Simulation. ATA Version 4.5 builds upon the expanded groundwork of ATA Version 4.0, updates evolving mandated and emerging standards, and aligns existing C4I-oriented mandates with the JTA. Appendix H contains the list of changes in ATA Version 4.5 with respect to Version 4.0. Due to its broader scope, the ATA Version 4.5 will continue to be the central source of Technical Architecture guidance for Army systems.

1.1.5 Basis for the ATA

The ATA is based on five primary sources: (1) acquisition reform initiatives such as the mandate to use widely accepted commercial standards; (2) standards used in existing Army systems; (3) the Defense Information Infrastructure (DII) Strategic Enterprise Architecture (SEA) and Common Operating Environment (COE); (4) guidance provided by the DOD's Technical Architecture Framework for Information Management (TAFIM), Version 2.0; and (5) the Joint Technical Architecture (JTA) Version 1.0.

1.2 TECHNICAL ARCHITECTURE

The technical direction within this document represents the evolving implementation of the 1994 Army Science Board (ASB) recommendations to develop a strong, enforceable technical architecture with a heavy emphasis on commercial standards and profiles. The intent is to achieve interoperability while reducing cost, by leveraging the large investment industry has made in developing and implementing standards-based technologies that are in widespread use. Every effort has been made to avoid closed commercial or military-unique standards. The standards contained herein are based primarily on commercial “open systems” technologies (open systems approach) that are being adopted by the joint community. Military standards are used only where absolutely necessary. A hierarchy of standards by family was developed to guide selection of specific standards for incorporation in this version of the ATA. The general order of preference, subject to modifications due to specific operational interoperability requirements and acceptance in the commercial marketplace (market acceptance), was standards specified by neutral standard groups such as IEEE or International Organization for Standardization (ISO), followed by industry consortiums such as the Open Systems Foundation, then vendor standards that are so widely supported as to be de facto industry standards, and finally government standards such as Federal Information Processing Standards (FIPS) and Military Standards (MIL-STDs).

NOTE: Some of the Government standards specified in the ATA are actually a profile of a commercial standard. A profile amplifies but does not modify the basic standard; that is, it specifies values for parameters or options, or it clarifies implementation details. Where these modifications are brief, they are listed directly along with the referenced standard they affect. All non-commercial standards mandated in the ATA have met the requirements of the DOD Commercial Standards Policy and can be used without any additional requests for waiver or exception to policy.

1.2.1 COMMON OPERATING ENVIRONMENT/ DOMAINS

An increasing amount of Army system development effort is spent in developing and testing computer software. In addition, even when software development is completed on schedule, few systems these days operate in isolation, so an additional amount of time and effort must be spent on maintaining specialized interfaces to external systems that are themselves changing over time. To alleviate this problem the concept of a Common Operating Environment (COE) was developed. It is a powerful mechanism that standardizes the external environment interface and the Application Program Interface (API) for a mission application system developer and maintains interoperability over time because the common software substrate is upgraded as a whole. It also frees the mission application developer to concentrate efforts on enhancing operational functionality rather than building common services.

DOD has adopted the Defense Information Infrastructure (DII) COE with its first implementation being the Global Command and Control System (GCCS) COE, which was referenced for use in Version 3.1 of the Army TA. This COE lays the foundation for the provision of standardized, common services and is described as a software architecture, an approach for building interoperable systems, a collection of reusable software components, a software infrastructure, and a set of guidelines and standards. The main emphasis in this version of the ATA is utilizing the COE concept, its software architecture, and building to a standard layer of APIs. The ATA does not mandate specific COE software or hardware products which are more appropriate for a Systems Architecture.

Studies of software reuse in Army and DOD systems indicate that the largest potential for reusing mission application software and process models is within a domain where functions and methods are the same. To better facilitate mission-application software reuse, a structure of domains, or common focus areas, are shown in Figure 1-3.

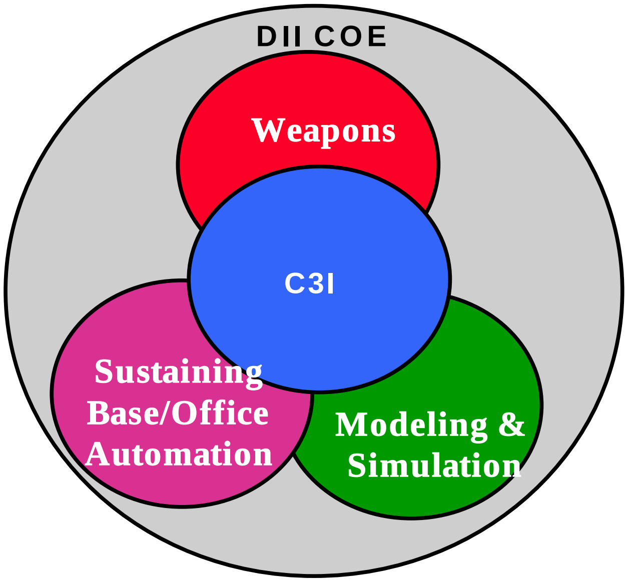


FIGURE 1-3 ARMY SYSTEM DOMAINS

There is only one DII COE. However, one specific COE implementation of software components and infrastructure cannot satisfy the requirements of all systems. The ATA envisions the tailoring of software components and infrastructure within a hierarchy of implementations of the COE, starting with high level domains, with specialized component sets tailored for each common area. In this way, common reusable software and products are inherited downward and either used as is, or replaced or augmented with more specialized software modules.

1.2.2 DOCUMENT ORGANIZATION

This document consists of six sections: (1) Overview; (2) Information Processing Standards; (3) Information Transfer Standards; (4) Information Modeling and Data Exchange Standards; (5) Human-Computer Interfaces; and (6) Information Security. These sections provide the core standards which apply to all systems.

In addition, there is an appendix for each domain containing exceptions (replace a core standard with a domain standard) or extensions (add a domain standard in addition to a core standard). A lead agency for each domain, shown in parentheses below, has been designated to further develop each domain appendix.

- Appendix D - Sustaining Base & Office Automation. (PEO-Standard Army Management Information System (STAMIS)).
- Appendix E - C3I. (PEO-Command, Control, and Communications Systems (C3S)).
- Appendix F - Weapons. (Weapons Systems Technical Architecture Working Group).
- Appendix G - Modeling and Simulation. (Simulations, Training and Instrumentation Command (STRICOM)).

Each section, except for the overview, is divided into three subsections as follows:

- *Introduction* - This subsection is for information only. It provides background descriptions and definitions that are unique to the section.
- *Mandates* - This subsection contains the mandatory standards (and profiles) within the section. Mandatory standards shall be implemented by systems that have a need for the corresponding interoperability-related services. A standard is mandatory in the sense that if a service is going to be implemented, it shall be implemented in accordance with the associated ATA standard. If a service is provided by more than one standard (e.g., local area network standards), the appropriate standard should be selected based on system requirements. Many standards have optional parts, or parameters that can affect interoperability. In those cases a commercial standard may be further modified by a standard profile to ensure proper operation.
- *Emerging Standards*- This subsection provides guidance for designing "forward compatibility" into systems. It lists standards that are not yet mandatory, but that probably will be adopted in the near future. The expectation is that emerging standards will be elevated to mandatory status when commercial implementations of the standards mature. System developers must design with an eye to these emerging standards so that they can be readily incorporated into future upgrades.

1.2.2.1 Information Processing Standards

Section 2 mandates government and commercial information processing standards the Army will use to develop integrated, interoperable systems that meet the warfighter's information processing requirements. This section also describes the Common Operating Environment (COE) concept and individual processing standards.

1.2.2.2 Information Transfer Standards

Section 3 describes the information standards and profiles that are essential for information transfer, interoperability, and seamless communications. This section mandates the use of the open-systems standards used for the Internet and the Defense Information Systems Network (DISN). These networks use the Internet Protocol (IP) suite, which provides communications interoperability between systems that are on different platforms or communications networks.

1.2.2.3 Information Modeling and Data Exchange Standards

Section 4 mandates the use of integrated information modeling to define functional and information requirements. Information modeling consists of Integrated Computer Aided Manufacturing Definition Function Method (IDEF0) process modeling and Integrated Computer Aided Manufacturing Definition Extended Data Method (IDEF1X) data modeling. The DOD Enterprise Model forms the overall framework for development and/or extension of process models for specific programs. The role of the DOD Command and Control (C2) Core Data Model and the Defense Data Dictionary System (DDDS), formerly the Defense Data Repository System (DDRS), are explained. The section describes the use of existing standard messages as an interim solution until mechanisms for the exchange of standard data elements are finalized.

1.2.2.4 Human-Computer Interfaces

Section 5 provides a common framework for Human-Computer Interface (HCI) design and implementation in Army automated systems. The objective is the standardization of user interface implementation options, enabling Army applications to appear and behave in a reasonably consistent manner. The section specifies HCI design guidance, mandates, and standards. The standardization of HCI appearance and behavior within the Army will result in higher productivity, shorter training time, and reduced development costs.

1.2.2.5 Information Security

The determination of security services to be used and their strength is one primary aspect of developing the security policy for an information domain or system. The choices made are dependent on policy, requirements, threats, vulnerabilities, and acceptable risk. This determination is an operational decision and is beyond the scope of the ATA. However, once the determination is made of which security services are needed, their strength, and at what system level to best provide each service, this section prescribes what standards and protocols are used to satisfy security requirements, maintain interoperability, and reduce cost through reuse.

To be effective, security standards must be integrated into and used with the other information standards in the ATA. Therefore this section is structured to shadow the overall organization of the ATA in order that readers can easily link security topics with the related subject area in the core sections of the ATA.

This page was intentionally left blank.

SECTION 2
INFORMATION PROCESSING STANDARDS

2.1 INTRODUCTION

2.1.1 Purpose

The purpose of this section is to specify the ATA information processing standards the Army will use to develop integrated, interoperable systems that directly or indirectly support the warfighter.

Information processing standards support the objectives of reducing life cycle cost and time of development, easing software integration and maintenance, and improving interoperability. The primary mechanism is the *concept* of a Common Operating Environment (COE) that provides a set of reusable common software services via standard Application Program Interfaces (APIs). By building modular applications that use a common software infrastructure accessed through a stable set of APIs, developers should be able to "plug and play" their applications into a centrally maintained infrastructure. The use of the standard APIs allows the COE and mission applications to be quickly integrated and updated relatively independent of each other. Use of a COE allows developers to concentrate their efforts on building mission area applications rather than building duplicative system service infrastructure software. Common standards such as Structured Query Language (SQL) to communicate with relational database management systems and Computer Graphics Metafile (CGM) to store graphics support the objective of interoperability. Systems developed to these standards combined with the appropriate standards in the following sections should be able to share services (retrieve authorized data from each others databases) and data (such as an overlay). The use and evolution of the COE and the ATA standards it embodies, will advance the goal of building systems that are compatible while minimizing program costs through systematic software reuse. The Army software reuse policy is defined in the Army Reuse Policy document.

2.1.2 Scope

This section applies to mission area, support application, and application platform service software developed or procured by the Army that process information for systems specified in paragraph 1.1.3. This section does not cover communications standards needed to transfer information between systems (refer to Section 3), nor standards relating to information modeling (process, data, and simulation), data elements, or military unique message set formats (refer to Section 4).

2.1.3 Background

The COE concept is introduced in Section 1. The COE software infrastructure is implemented with a set of modular software that provide generic functions or services such as operating system services. These services or functions are accessed by other software through standard APIs. The DII COE may have to be adapted and tailored to meet the specific requirements of a domain. The key is that domain implementations adhere to the COE concept in that they provide standard modularized software services that are consistent with the TAFIM Technical Reference Model (TRM) and that application programmers have access to these services through standard APIs.

The individual standards contained in this section and applicable appendices that will be used to implement a domain COE are presented within the framework of the TAFIM TRM. This reference model was intentionally generalized and does not imply any specific system architecture. Its purpose is to provide a common conceptual framework, and define a common vocabulary so that diverse components within DOD can better coordinate acquisition, development and support of DOD systems. The TAFIM TRM organizes software into two entities, an Application Software Entity and an Application Platform Entity. The Application Software Entity communicates with the Application Platform Entity through an API. The Application Platform Entity communicates with the external environment through the External Environment Interface (EEI). The TAFIM TRM decomposes these entities into subcategorizes as shown in Figure 2-1. The application software entity and associated mandates are detailed in Section 2.2.1 while the Application Platform's seven major service areas and associated mandates are detailed in Section 2.2.2.1. Section 2.2.2.2 defines the Application Platform Cross-Area Services and their associated mandates.

2.2 MANDATES

The ATA mandates the*COE concept*and the use of the DII COE 2.0 public APIs. The COE concept is described as a software architecture, an approach for building interoperable systems, a common collection of reusable software components, a software infrastructure, and a set of guidelines and standards. A detailed description of the of the COE concept is contained in the DII COE Version 2.0 Baseline Specification, Section 2, 28 June 1996. If a required service is not available in the DII COE, software developed shall adhere to the individual processing standards in this section and the applicable domain appendix.

2.2.1 Application Software Entity

The Application Software Entity includes both mission area applications and support applications. Mission area applications implement specific user's requirements and needs (e.g., maneuver control, personnel, materiel management, and weapon system operations and control). This application software may be commercial off-the-shelf (COTS), government off-the-shelf (GOTS), custom-developed software, or a combination of these.

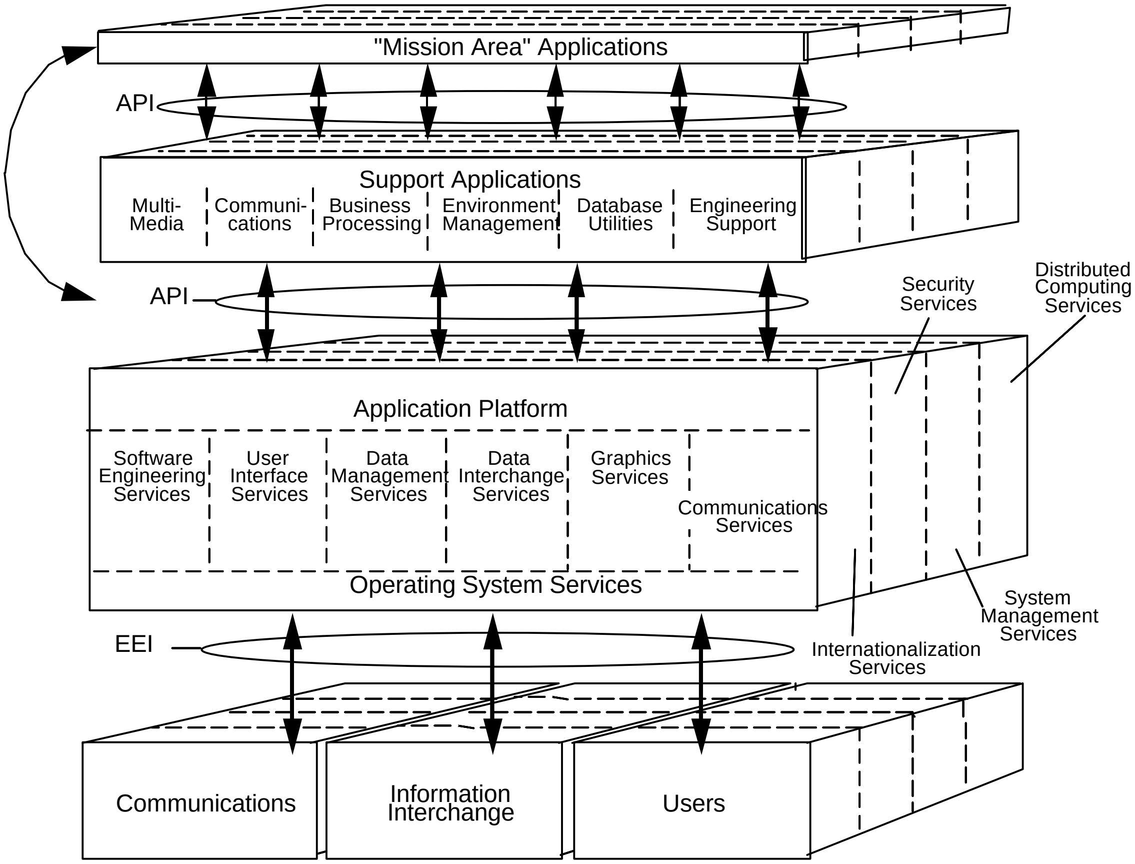


FIGURE 2-1 TAFIM TRM, VERSION 2.0

Support applications are common applications (e.g., E-mail and word processing) that can be standardized across individual or multiple mission areas and are the first layer of the COE. The services they provide can be used to develop mission-area-specific applications or can be made available to the user. The TAFIM TRM defines six support application categories: Multimedia; Communications; Business Processing; Environment Management; Database Utilities; and Engineering Support. The definitions of these categories are found in the TAFIM, Volume 2, Section 2.4.2.

The Application Software Entity includes all Army application software. All domains shall distinguish between their common support applications and mission area applications. Mission area applications shall use the DII COE support applications to the maximum extent possible. If a new support application segment must be developed, it shall use all applicable DII COE lower level application platform service APIs that are compliant with the standards in this section. In the absence of a compliant DII COE component segment, developers will utilize the mandated individual standards contained in this section and segment their component In Accordance With (IAW) the DII COE Integration and Runtime Specification (I&RTS) Version 2.0, 23 Oct 1995.

2.2.2 Application Platform Entity

The Application Platform Entity is the second layer of the COE, and includes the common, standard application platform services upon which the required functionality is built. The Application Platform Entity is used by the COE support applications and unique mission area applications software. The Application Platform Entity is composed of service areas and cross-area services. The definitions of these service areas are found in the TAFIM, Volume 2, Section 2.4.3 and 2.4.4 respectively. The corresponding mandates are provided in the following subsections.

2.2.2.1 Service Areas

The TAFIM TRM defines seven service areas within the Application Platform Entity: software engineering, user interfaces, data management, data interchange, graphics, network, and operating system services.

2.2.2.1.1 Software Engineering Services

The software engineering services provide system developers the tools appropriate to the development and maintenance of applications. These include programming languages, language bindings and object code linking, and Computer Aided Software Engineering (CASE) environments and tools. The following subsections specify applicable standards that such software engineering tools shall implement.

2.2.2.1.1.1 Programming Languages

Language services provide the basic syntax and semantic definition for use by developers to describe the desired software function.

Ada is mandated in DOD Directive 3405.1 for use in all DOD custom developed software. This mandate does not include software that is developed and maintained commercially. Software development shall be based on Ada 95. Ada 95 is backward-compatible with the Ada 83 language specification.

The *Assistant Secretary of Defense Memorandum, Subject: Delegations of Authority and Clarifying Guidance on Waivers from the Use of the Ada Programming Language* requires the DOD Services to implement a waiver process. Developers requesting an Ada waiver shall do so IAW HQDA LTR 25-92-1,*"Implementation of the Ada Programming Language,"* and extended by HQDA LTR 25-94-1 and LTR HQDA 25-95-1.

- ISO/International Electrotechnical Commission (IEC) 8652:1995 (Ada 95), Ada Reference Manual, Language and Standard Libraries.

2.2.2.1.1.2 Language Bindings and Object Linking

Language bindings and object code linking provide the ability for software to access services and software through APIs that have been defined independently of the computer language. Ada bindings shall be used to provide the interface to COTS or GOTS software that is developed in other languages. The following standard is mandated.

- IEEE 1003.5:1992, POSIX: Ada Language Interfaces Part 1: Binding for System API.

2.2.2.1.1.3 CASE Environments and Tools

CASE tools and environments include tools for requirements specification, design, analysis, creating, and testing code. The ATA does not mandate specific tools. Section 4 mandates standards that data modeling Computer Automated Software Engineering (CASE) tools will follow.

2.2.2.1.2 User Interface Services

These services*implement*the Human-Computer Interface (HCI) style and control how users interact with the system. The ATA mandates Common Desktop Environment which is based on X Window System and Open Software Foundation (OSF) Motif. The following standards apply:

- FIPS Pub 158-1, X Window System, Version 11, Release 5.
- OSF, 1992, Motif Application Environment Specification, Release 1.2.
- OSF/Motif Inter Client Communications Convention Manual (ICCCM).
- X/Open C323, Common Desktop Environment (CDE) Version 1.0, April 1995.

Refer to Section 5 for HCI style guidance and standards.

2.2.2.1.3 Data Management Services

Central to most systems is the sharing of data between applications. The data management services provide for the independent management of data shared by multiple applications. These services include data dictionary/directory services and database management systems (DBMS) services.

These services support the definition, storage, and retrieval of data elements from monolithic and distributed, relational DBMSs. These services also support platform-independent file management (e.g., the creation, access, and

destruction of files and directories). The following standards are mandated for any system required to use a Relational Database Management System:

- FIPS Pub 127-2, Database Language - SQL.

2.2.2.1.4 Data Interchange Services

The data interchange services provide specialized support for the exchange of data and information between applications and to and from the external environment. These services include document, graphics data, geospatial data, imagery data, product data, electronic data, video data, atmospheric data, and oceanographic data interchange services. The standards below are mandated.

2.2.2.1.4.1 Document Interchange

These services provide the specifications for encoding data and the logical and visual structure of electronic documents.

- FIPS Pub 152, Standard Generalized Markup Language (SGML) - Interchange format for conveying the logical structure of office documents.
- RFC 1866: 1995, HyperText Mark-up Language (HTML), Version 2.0 - Interchange format used by the World Wide Web (WWW) for HyperText format and embedded navigational links.

Table 2-1 identifies file formats for the interchange of common document types such as text documents, presentation graphics, spreadsheets, and data bases. Some of these formats are controlled by individual vendors, but all of these formats can be translated by multiple company's products. In support of the standards mandated in this section, Table 2-1 identifies DOD conventions for file name extensions for documents of various types. The majority of the extensions are automatically generated by the commercial product. The following file formats are mandated when exchanging applicable document types between DOD organizations. (Note: Native commercial products such as Microsoft Word 6.0 are not being mandated):

- Applications acquired or developed for the production of documents shall be capable of generating at least one of the formats listed in Table 2-1 for the appropriate document type.
- All organizations shall at a minimum be capable of reading and printing all of the formats listed below for the appropriate document type.

2.2.2.1.4.2 Graphics Data Interchange

These services are supported by device-independent descriptions of picture element raster and vector graphics.

- FIPS Pub 128-1, Computer Graphics Metafile (CGM) - Interchange format for vector graphics data.
- ISO 10918-1, Joint Picture Expert Group (JPEG) - Interchange graphics compression format for raster graphics of photographic images.
- JPEG File Interchange Format (JFIF), Version 1.02, C-Cube Microsystems for raster graphics data encoded using the ISO 10918-1: 1994, Joint Photographic Expert Group (JPEG) algorithm.

2.2.2.1.4.3 Geospatial Data Interchange

For mapping, charting, and geodesy (MC&G) services, collectively known as geospatial services, the following standards are mandated in support of non-civil engineering DOD military operations:

- MIL-STD-2411, Raster Product Format (RPF) - Defense Mapping Agency (DMA) format for raster-based products which , such as Compressed Arc Digitized Raster Graphics (CADRG), Controlled

Image Base (CIB), and Digital Point Positioning Data Base (DPPDB). MIL-STD-2411 is based on National Imagery Transmission Format Standard (NITFS) (MIL-STD-2500A) described below.

- MIL-STD-2407, Vector Product Format (VPF) - DMA format for vector-based products used by geographic information system (GIS) and other DOD systems. VPF standard products include Vector Map (VMap) Levels 0-2, Urban Vector Map (UVMap), Digital Nautical Chart (DNC), VMap Aeronautical Data (VMap AD), Vector Product Interim Terrain Data (VITD), Digital Topographic Data (DTOP), Littoral Warfare Data (LWD), and World Vector Shoreline Plus (WVS+).
- MIL-D-89020, Digital Terrain Elevation Data (DTED) - DMA format used by DTED Levels 1 and 2.
- MIL-STD-2401, World Geodetic System 84 (WGS-84) 21 March 1994 - DOD's standard global reference system developed by the DMA. WGS-84 is employed by the NAVSTAR Global Positioning System (GPS) and modern weapons and systems. Latitude and longitude data shall use WGS-84 in accordance with CJCSI 3900.01, and standard coordinate data elements as discussed in Section 4.

TABLE 2-1 - DOCUMENT INTERCHANGE FORMATS

Document Type	Standard/Vendor Format	Recommended File Name Extension	Reference
Plain Text	ASCII Text	.txt	
Compound Document *	Acrobat 2.0	.pdf	Vendor
	HTML 2.0	.htm	IETF
	MS Word 6.0	.doc	Vendor
	Rich Text Format	.rtf	Vendor
	WordPerfect 5.2	.wp5	Vendor
Briefing - Graphic Presentation	Freelance Graphics 2.1	.pre	Vendor
	MS Powerpoint 4.0	.ppt	Vendor
Spreadsheet	Lotus 1-2-3 Release 3.x	.wk3	Vendor
	MS Excel 5.0	.xls	Vendor
Database	Dbase 4.0	.dbf	Vendor

Note: * **-** Compound documents contain embedded graphics, tables, and formatted text. Note that not all special fonts, formatting, or features supported in the native file format may convert accurately.

2.2.2.1.4.4 Imagery Data Interchange

The NITFS is a DOD and Federal Intelligence Community suite of standards for the exchange, storage, and transmission of digital imagery products. NITFS provides a package containing information about the image, the image itself, and optional overlay graphics. It was developed and mandated by Assistant Secretary of Defense (ASD) Command, Control, Communications, and Intelligence (C3I) for the dissemination of digital imagery from overhead collection platforms. Guidance on applying the suite of standards can be found in Military Handbook (MIL-HDBK)-1300A. The following standards are mandated for secondary imagery dissemination:

- MIL-STD-2500A, National Imagery Transmission Format (Version 2.0) for file format.
- MIL-STD-188-196, Bi-Level Image Compression.
- MIL-STD-188-199, Vector Quantization Decompression.
- ANSI/ISO 8632: 1992, Computer Graphics Metafile (CGM) as profiled by FIPS 128-1 and MIL-STD-2301.
- ISO/IEC 10918-1: 1994, Joint Photographic Experts Group (JPEG) as profiled by MIL-STD-188-198A. Although the NITFS uses the same ISO JPEG algorithm as mandated in section 2.2.2.1.4.2, the NITFS file format is not interchangeable with the JFIF file format.

2.2.2.1.4.5 Product Data Interchange

These services include technical drawing specifications, documentation, and other data required for product design and manufacturing.

- MIL-PRF-28000A, Initial Graphics Exchange Specification (IGES) - Interchange format for computer-aided design (CAD) data, such as technical illustrations and engineering drawings.

2.2.2.1.4.6 Electronic Data Interchange

These services are used to create an electronic environment (paperless) for the exchange of data.

- FIPS Pub 161-1, Electronic Data Interchange (EDI) - Interchange format for documents that are highly structured (e.g., consisting of a sequence of numeric or alphanumeric fields rather than free-form text).

Refer to Section 4.2.4 for additional requirements on message standards.

2.2.2.1.4.7 Video Data Interchange

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 Mbps). 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. The following standards are mandated:

- ISO 11172-1, Motion Pictures Expert Group (MPEG) Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 1: Systems.
- ISO/IEC 11172-1: 1993/Cor. 1:1995 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 1: Systems Technical Corrigendum 1.
- ISO/IEC 11172-2: 1993 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 2 Video.

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 Megabits per second (Mbits/s). MPEG-2 has also been extended to cover HDTV. The following standards are mandated:

- ISO 13818-1: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 1: Systems.
- ISO 13818-2: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 2: Video.

Video Teleconferencing (VTC) standards are specified in Section 3.

2.2.2.1.4.8 Atmospheric Data Interchange

The following formats were established by the World Meteorological Organization (WMO) Commission for Basic Systems (CBS) for meteorological data and published under the Manual for Codes, Volume 1, Part B, Binary Codes, WMO No. 306. The following standards are mandated:

- FM 92-X-GRIB - The WMO Format for the Storage of Weather Product Information and the Exchange of Weather Product Messages in Gridded Binary (GRIB) Form. GRIB was developed for the transfer of gridded data fields, including spectral model coefficients, and of satellite images. A GRIB record (message) contains values at grid points of an array, or a set of spectral coefficients, for a parameter at a single level or layer as a continuous bit stream. It is an efficient vehicle for transmitting large volumes of gridded data to automated centers over high speed telecommunication lines using modern protocols. It can equally well serve as a data storage format. While GRIB can use predefined grids, provisions have been made for a grid to be defined within the message.
- FM 94-X-BUFR - The WMO Binary Universal Format for Representation (BUFR) of meteorological data. Besides being used for the transfer of data, BUFR is used as an on-line storage format and as a data archiving format. A BUFR record (message) containing observational data of any sort also contains a complete description of what those data are: the description includes identifying the parameter in question, (height, temperature, pressure, latitude, date, and time), the units, any decimal scaling that may have been employed to change the precision from that of the original units, data compression that may have been applied for efficiency, and the number of binary bits used to contain the numeric value of the observation. BUFR is a purely binary or bit oriented form.
- Data Exchange Format (DEF) - Appendix 30 to the TAWDS/Integrated Meteorological System (IMETS) Implementation Document for Communication Information Data Exchange (CIDE).

2.2.2.1.4.9 Oceanographic Data Interchange

Standard transfer formats are required for the pre-distribution of oceanographic information. WMO GRIB and the BUFR file transfer formats are used for this purpose. The GRIB and BUFR extensions include several extensions, including provision for additional variables, additional originating models, a standard method to encode tables and line data; a method to encode grids (tables) with an array of data at each grid point (table entry); and a method to encode multiple levels in one GRIB message. The following WMO CBS format for oceanographic data use is mandated:

- FM 94-X-BUFR - The WMO Binary Universal Format for Representation (BUFR) of oceanographic data.

2.2.2.1.5 Graphic Services

These services support the creation and manipulation of graphical images. These services include device-independent, multidimensional graphic object definition, and the management of hierarchical database structures containing graphics data. The standards that apply are:

- FIPS Pub 120-1 (change notice 1), Graphical Kernel System (GKS) - for 2-D graphics.
- FIPS Pub 153, Programmers Hierarchical Interactive Graphics Systems (PHIGS) - for 3-D graphics.

2.2.2.1.6 Communications Services

These services support the distributed applications that require data access and applications interoperability in networked environments. The standards that apply are provided in Section 3.

2.2.2.1.7 Operating System Services

These core services are necessary to operate and administer a computer platform and to support the operation of application software. These services include kernel operations, shell and utilities. These services shall be accessed by applications through applicable standard Portable Operating System Interface (POSIX) APIs. Not all operating system services are required to be implemented, but those that are used shall comply with the standards. The following standards apply.

- IEEE 1003.1, Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API).
- IEEE 1003.2, POSIX: Shell and Utilities (as profiled by FIPS Pub 189-1).
- IEEE 1003.2d, POSIX: Shell and Utilities - Batch Environment.
- IEEE 1003.5:1992, POSIX: Ada Language Interfaces Part 1: Binding for System API.

2.2.2.2 Application Platform Cross-Area Services

The TAFIM TRM defines four application platform cross-area services: internationalization, security, system management, and distributed computing services.

2.2.2.2.1 Internationalization Services

The internationalization services provide a set of services and interfaces that allow a user to define, select, and change between different culturally related application environments supported by the particular implementation. These services include character sets, data representation, cultural convention, and native language support.

In order to interchange text information between systems, it is fundamental that systems agree on the character representation of textual data. The following character set coding standards are mandated for the interchange of 8-bit and 16-bit textual information respectively:

- ISO/IEC 8859-1:1987, Information Processing - 8-Bit Single-Byte Coded Character Sets - Part 1: Latin Alphabet No. 1.
- ISO/IEC 10646-1:1993, Information Technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane.

2.2.2.2.2 Security Services

These services assist in protecting information and computer platform resources. In order to fully meet security requirements, these services must often be combined with security procedures which are beyond the scope of the ATA. Security services include security policy, accountability, and assurance. Refer to Section 6 for security service standards.

2.2.2.2.3 System Management Services

These services provide capabilities to manage an operating platform and its resources and users. System management services include configuration management, fault management, and performance management. The standards that apply are provided in Section 3.2.1.4.

2.2.2.2.4 Distributed Computing Services

These services allow various tasks, operations, and information transfers to occur on multiple, physically-dispersed or logically-dispersed, computer platforms. These services include global time, data, file and name services, thread services, and remote process services. The OSF Distributed Computing Environment (DCE) Version 1.1 standard is mandated. The standards that apply are:

- X/Open C309 - DCE Remote Procedure Call.
- X/Open C310 - DCE Time Services.
- X/Open C312 - DCE Directory Services.

2.3 EMERGING STANDARDS

2.3.1 DII COE

The Army is committed to the COE concept and will mandate DII COE 3.0 APIs as they become stable.

2.3.2 Service Area Standards

Within Data Interchange Services, HTML 3.2 is expected to be mandated once approved by the Internet Engineering Task Force (IETF), and implemented in commercial and freeware products. In addition, wavelet image compression techniques are still being reviewed for inclusion in the NITFS imaging standard.

Within Operating System Services, it is expected that the draft IEEE P1003.x POSIX standards will be adopted once they become final. In addition, the X/Open Single UNIX Specification (SUS) (previously referred to as Specification 1170) is an emerging standard. It is also expected that POSIX, 1003.5b will be approved in 1996 which will deal with real-time interfaces and Ada 95 improvements as well as provide a "wide" character set suitable for dealing with Asian languages.

Within Distributed Computing Services, the emerging standards include the Common Object Request Broker Architecture (CORBA) 2.0 and DCE Authentication and Security Specification (P315).

Within Data Management Services, the emerging standards include the ISO/IEC 9075-3, 1995 Call Level Interface, and draft DIS 9075-4, Database Language SQL, Part 4: Persistent Stored Modules (SQL/PSM).

SECTION 3

INFORMATION TRANSFER STANDARDS

3.1 INTRODUCTION

3.1.1 Purpose

Information transfer standards and profiles are described in this section. These standards provide seamless communications and information transfer interoperability for Army systems.

3.1.2 Scope

This section identifies standards that support the transfer of data, video, imagery, and multimedia. The standards described in this section apply at the external interfaces between computer systems (i.e., hosts), routers, and communications networks. These standards do not apply at the interfaces between hosts and peripherals (e.g., storage devices, sensors, and weapons control). Where operational or system requirements dictate the need for tactical data links, the data link standards in Section 4.2.4.4 shall apply.

3.1.3 Background

The standards herein are drawn from widely accepted, commercial standards. In particular, the ATA makes use of the same open-systems architecture used for the Internet and the Defense Information Systems Network (DISN). These networks provide for communications interoperability between systems that may be on different communications networks.

3.1.3.1 Communications Framework

System components are categorized here as hosts, networks, and routers. Hosts are computers that generally execute application programs on behalf of users and share information with other hosts via networks. Networks may be relatively simple (e.g., point-to-point links) or have complex internal structures (e.g., network of packet switches). Routers interconnect two or more networks and forward packets across network boundaries. Routers are distinct from hosts in that they are normally not the destination of data traffic.

Host standards are specified in Section 3.2.1. Router standards are specified in Section 3.2.2. Within the OSI reference model, the standards in these sections map to the internetwork layer and above. These standards support logical end-to-end interface connections. Hosts and routers connect to networks using the corresponding network interface protocols. The network protocols correspond to the physical, data link, and intranet layers that are defined by the Open Systems Interconnection (OSI) reference model. Network standards are specified in Section 3.2.3.

3.1.3.2 Protocol Standards

A number of the standards mandated in this section are published by the Internet Architecture Board (IAB). The IAB is responsible for the Internet Protocol (IP) suite, and documents these protocols using Request for Comments (RFCs) and Standards (STDs). STDs are a subseries of notes within the RFC series that are formal Internet "Standards." When a protocol is defined by both an RFC and a STD, the ATA uses the STD nomenclature.

The ATA mandates only a small subset of protocols within the entire IP suite. Other protocols within the IP suite can be used if they provide services that are not offered by any of the mandated protocols.

3.1.3.3 Protocol Profiles

Protocol standards generally have multiple options and parameters that can assume a range of values. Some of these options and parameters have local significance, and can be selected to optimize performance or provide unique services for a specific application. Other options and parameters have global significance, and must be consistent across multiple applications to support seamless communications.

To foster interoperability, a profile may be established for a protocol standard that has options and parameters with global significance. The profile imposes particular values for these options and parameters. Where appropriate, profiles are listed in Section 3.2 next to their corresponding standards. For efficiency, if a profile indicates only several options and parameters, the profile is not listed. Instead, the required options and parameters to be exercised are listed along with the protocol standard in the appropriate section.

3.2 MANDATES

3.2.1 Host Standards

All hosts shall adhere to STD-3. This is an umbrella standard that references other documents and corrects errors in some of the referenced documents. STD-3 also adds additional discussion and guidance for an implementor.

3.2.1.1 Internetwork Layer Standards

STD-5 shall be used at the internetwork layer. STD-5 defines the IP protocol, which is a basic connectionless datagram service. All protocols within the IP suite use the IP datagram as the basic data transport mechanism. IP was designed to interconnect heterogeneous networks and operates over a wide variety of networks.

Within STD-5, 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 gateway redirection. IGMP provides multicast extensions for hosts to report their group membership to multicast routers.

All implementations of IP must pass the received Type-of-Service (TOS) values up to the transport layer.

3.2.1.2 Transport Layer Standards

Either STD-6 or STD-7 shall be used at the transport layer. These two protocols provide fundamentally different services. STD-6 defines the User Datagram Protocol (UDP), which provides a connectionless, datagram service to applications not requiring reliable, sequenced communications. STD-7 defines the Transmission Control Protocol (TCP), which provides a reliable, connection-oriented transport service.

TCP shall implement the PUSH flag and the Nagle Algorithm, as defined in IAB Standard 3.

3.2.1.3 Application and Support Standards

- *File transfer* - Basic file transfer shall be accomplished using the File Transfer Protocol (FTP) protocol. FTP provides a reliable, file transfer service for text or binary files. While designed to be used by other programs, it includes a direct interactive user interface to enable access to remote file servers. FTP, which uses TCP as a transport service, is specified in STD-9. FTP implementations must support for reception the Store Unique (STOU) and Abort (ABOR) commands.

- *Remote terminal* - Basic remote terminal services shall be accomplished using Telecommunications Network (TELNET). TELNET provides a virtual terminal capability that allows a user to "log on" to a remote system as though the user's terminal was directly connected to the remote system. TELNET, which uses TCP as a transport service, is specified in STD-8.

- *Electronic mail* - The standard for electronic mail is Defense Message System (DMS)-compliant X.400. This provides a full-featured, electronic mail service, as specified in Allied Communication Publication (ACP) 123 and U.S. Supplement No. 1. Note that X.400 is not an Internet standard, and must operate over TCP through the use of STD-35.

- *Directory services* - International Telecommunications Union (ITU) X.500 is mandated for use with DMS. X.500 which provides directory and security services that may be used by users or DMS-compliant applications to locate other users and resources on the network. Note that X.500 is not an Internet standard, and must operate over TCP through the use of STD-35.

- *Translating names to addresses* - The Domain Name System (DNS) provides the service of translating between host names and IP addresses. DNS, which uses TCP as a transport service, is specified in STD-13.

- *Booting without disks* - The BootStrap Protocol (BOOTP) provides a mechanism for a diskless system to initialize itself from a server. BOOTP, which uses UDP as a transport service, is specified in RFC-951, with additional clarifications provided in RFC-1542. Vendor extensions are specified in RFC-1533.

- *Dynamic configuration*- The Dynamic Host Configuration Protocol (DHCP) is used to dynamically assign an IP address and provide other information necessary to configure a host to operate on a network. 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. DHCP, which uses UDP as a transport service, is specified in RFC-1541.
- *HyperText transfer*- The HyperText Transfer Protocol (HTTP) is used to support HyperText search and retrieval. HTTP, which uses TCP as a transport service, is defined in RFC-1945. Uniform Resource Locators (URLs), which specify how objects are identified with HTTP, are defined in RFC-1738 and RFC-1808.

3.2.1.4 Network Management Standards

Network management standards provide the capability to remotely manage network objects, such as host computers, routers, and local wide area networks. Network management provides the capability to monitor the status of the network objects; to start, reconfigure or terminate network objects; and to detect the loss of network objects in order to support automated fault recovery. Network management also includes the capability to control a network's topology; maintain network routing tables; monitor the network load; and make routing adjustments to optimize throughput into multiple logical domains; maintain network routing tables; monitor the network load; and make routing adjustments to optimize throughput.

To support the information exchange with network managers, network objects shall implement the Simple Network Management Protocol (SNMP) set of management protocols. The set consists of STD-15 (Simple Network Management Protocol), STD-16 (Structure of Management Information), and STD-17 (Management Information Base). SNMP uses UDP as a transport service.

3.2.1.5 Video Teleconferencing (VTC) Standards

VTC terminals operating at data rates of 56-1920 kilobits per second (kbps) shall comply with VTC001-Rev1, Industry Profile for Video Teleconferencing, Revision 1, dated April 25, 1995. The purpose of the profile is to provide interoperability between VTC terminal equipment, both in point-to-point and multipoint configurations. This profile is based on the ITU H.320 and T.120 series of recommendations. VTC terminals operating at low bit rates (9.6-28.8 kbps) shall comply with ITU-T H.324, Terminal for Low Bit Rate Multimedia Communications, dated March 19,1996.

3.2.1.6 Global Position System (GPS) Standards

GPS User Equipment must employ Precise Position Service (PPS) user equipment incorporating both Selective Availability and Anti-Spoofing features to support combat operations. The GPS guidelines that are documented in ASD Memorandum *Development, Procurement, and Employment of DoD Global Position System User Equipment, 30 April 1992* must be followed. Emerging interface standards between hosts and GPS are identified in Section 3.3.1.

3.2.2 Router Standards

All routers shall adhere to RFC-1812. This is an umbrella standard that references other documents and corrects errors in some of the referenced documents. RFC-1812 also adds additional discussion and guidance for an implementor.

Some of the standards that were mandated for hosts in Section 3.2.1 also apply to routers. Specifically, the following standards apply to routers: IP (STD-5), UDP (STD-6), TCP (STD-7), TELNET (STD-8), DNS (STD-13), SNMP (STD-15, STD-16, and STD-17), and BOOTP (RFC-951, RFC-1533, and RFC-1542).

Hosts can implement router functionality. When they do so, they shall adhere to the appropriate router standards.

The Trivial FTP (TFTP) protocol, as specified in STD-33, may be used in conjunction with BOOTP to initialize routers.

Routers exchange connectivity information with other routers to determine network connectivity and adapt to changes. This enables routers to determine, on a dynamic basis, where to send IP packets.

- *Interior routing*- Routes within an Autonomous System (AS) are considered local routes that are administered and advertised locally by means of an interior gateway protocol. Routers shall use the Open Shortest Path First (OSPF) V2 protocol for interior gateway routing. OSPF V2, which uses IP directly, is specified in RFC-1583. To support Class D group addresses, the multicast extensions to OSPF are specified in RFC-1584.
- *Exterior routing*- Exterior gateway protocols are used to specify routes between ASs. Routers shall use the Border Gateway Protocol (BGP) V4 for exterior gateway routing. BGP V4, which uses TCP as a transport service, is specified in RFC-1771 and RFC-1772.

3.2.3 Network Standards

This section identifies the network interface standards that have been adopted by the ATA. These standards support a range of performance needs. The selection of specific network standards for a given application should be based on system-related requirements, such as cost and speed-of-service.

These standards operate at the physical and link layers, and in some instances, at the intranet sublayer of the network layer. These standards are not generally defined by RFCs. However, RFCs are used to define how these networks interface with IP (e.g., address resolution). The network standards are identified in the following subsections.

3.2.3.1 Serial Lines

For full duplex, synchronous or asynchronous, point-to-point communication, the following standards are mandated:

- IAB Standard 51/RFC-1661/RFC-1662, Point-to-Point Protocol (PPP), July 1994.

- RFC-1332, PPP Internet Protocol Control Protocol (IPCP), May 26, 1992.
- RFC-1333, PPP Link Quality Monitoring, May 26, 1992.
- RFC-1334, PPP Authentication Protocols, October 20, 1992.
- RFC-1570, PPP Link Control Protocol (LCP) Extensions, January 11, 1994.

The serial line interface shall comply with one of the following mandated standards:

- Electronics Industries Association (EIA) 232E, Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, July 1991.
- EIA 449, General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, February 1980. (This calls out EIA 422B and 423B.)
- EIA 530A, High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment, June 1992, Including Alternate 26-Position Connector, 1992. (This calls out EIA 422B and 423B.)

3.2.3.2 Ethernet

Ethernet is the most common network technology available. Data is transmitted at 10 Megabits per second (Mbps) over a cable, which is shared by multiple hosts. The hosts use a carrier sense multiple access with collision detection (CSMA/CD) scheme to control access to the cable. At the physical layer, Ethernet shall be implemented with any of four different types of cable. The implementations (and cable types) shall be as defined by the IEEE as: 10Base-5 (thick coaxial); 10Base-2 (thin coaxial); 10Base-T (unshielded twisted pair); and 10Base-F (fiber-optic cable). Platforms that must physically connect to a Joint Task Force Local Area Network shall support an IEEE 802.3, 10Base-T connection.

Ethernet's physical layer and CSMA/CD access scheme are specified in IEEE 802.3. The interface between Ethernet and IP shall be in accordance with STD-37 and STD-41.

For higher-speed requirements, 100-Mbps Ethernet technology shall be implemented in accordance with the Fast Ethernet standard, IEEE 802.3u. This standard supports auto-negotiation of the media speed, making it possible for dual-speed Ethernet interfaces to run at either 10 or 100 Mbps automatically.

3.2.3.3 Fiber Distributed Data Interface (FDDI)

FDDI is a mature high-speed network standard. Data is transmitted at 100 Mbps over either multimode or singlemode fiber-optic cable. FDDI is defined by a series of International Organization for Standardization (ISO) standards. These standards shall apply: 9314-1 (physical layer), 9314-2 (media access control), and 9314-3 (medium dependent). In addition, the Station Management (SMT) protocol defined in ANSI X3.229 shall be used.

The Logical Link Control (LLC) layer for FDDI shall be as specified in IEEE 802.2. The interface between FDDI and IP shall be in accordance with STD-36.

3.2.3.4 Asynchronous Transfer Mode (ATM)

ATM is a high-speed switching technology that takes advantage of low bit-error rate transmission facilities to accommodate intelligent multiplexing of voice, data, video, imagery, and composite inputs over high-speed trunks. The ATM Forum's *User-Network Interface (UNI) Specification, Version 3.1, September 1994*, shall be used as the set of network access protocols for ATM switches. The UNI Specification supports operation over fiber-optic and twisted pair cables, with data rates of 1.5, 2, 45, 51, 100, and 155 Mbps. In addition, a 25.6 Mbps interface is supported in accordance with *25.6 Mb/s over Twisted Pair Cable Physical Interface*

The *Private Network-Network Interface (PNNI) Specification, Version 1* is mandated. PNNI supports the distribution of topology information between switches and clusters of switches to allow paths to be computed through the network. PNNI also defines the signaling to establish point-to-point and point-to-multipoint connections across the ATM network.

The protocol layers consist of an ATM Adaptation Layer (AAL), the ATM layer, and a physical layer. The role of AAL is to divide the variable-length data units into 48-octet units to pass to the ATM layer. There are currently four defined AAL protocols to support different service classes. The ATA mandates two of these AAL protocols. AAL1 shall be used to support constant bit rate service, which is sensitive to cell delay, but not cell loss. AAL5 shall be used to support variable bit rate service. AAL1 and AAL5 are specified in ANSI T1.630 and T1.635, respectively. IP packets shall be transported over AAL5, in accordance with RFC-1577.

Ethernet can be emulated by ATM networks using *Local Area Network (LAN) Emulation over ATM, Version 1.0* This permits ATM networks to be deployed without disruption of host network protocols and applications.

3.2.3.5 X.25

X.25 is an international standard that has been widely adopted for packet-switched networks. X.25 defines the interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE). The DTE generally refers to the router or host equipment side of the interface, and the DCE refers to the communications network side.

The standards that apply to DTEs are different from (but fully compatible with) the standards that apply to DCEs. For DCEs, ITU X.25 shall be used at the data link and packet (i.e., intranet) layers. For DTEs, ISO 7776 shall be used at the data link layer and ISO 8208 shall be used at the packet layer.

At the physical layer, the X.25 interface shall be in accordance with Recommended Standard (RS)-232, RS-422/423/449, or RS-530.

The method of interworking IP with X.25 interfaces shall be as specified in RFC-1356. For the X.25 interface to the Army Data Distribution System (ADDS), the profile shall be in accordance with ACCS-A3-407-008D. For all other X.25 interfaces, the profile shall be in accordance with ANSI X3.100.

3.2.3.6 Integrated Services Digital Network (ISDN)

ISDN is an international standard used to support integrated voice and data over standard twisted-pair wire. ISDN defines a Basic Rate Interface (BRI) and Primary Rate Interface (PRI) to provide digital access to ISDN networks. These interfaces support both circuit-switched and packet-switched services.

The BRI and PRI physical layers are specified by I.430 and I.431, respectively. The profiles for BRI and PRI are National ISDN 1 and 2, respectively. The BRI physical layer uses two wires to provide two B channels (64 kbps) for information transport and one D channel (16 kbps) for signaling. The PRI physical layer uses four wires to provide 23 B channels (64 kbps) for information transport and one D channel (64 kbps) for signaling. The B channels can provide clear channel services or packet based, point-to-point services.

For B channels configured for packet-switched services, the data link and network layers shall be the same as specified in X.25. IP packets shall be encapsulated and transmitted over ISDN as specified in RFC-1356. For B channels configured for clear channel services, IP packets shall be encapsulated and transmitted using PPP over ISDN as specified in RFC-1618.

For D channels, the data link layer is specified in Q.921 and the network layer is specified in Q.931.

3.2.3.7 MIL-STD-188-220A

Combat Net Radios (CNRs) are a family of radios that provide voice and data communications for mobile users. These radios provide a half-duplex, broadcast transmission media with potentially high bit error rates. With the exception of High Frequency (HF) networks, MIL-STD-188-220A shall be used as the standard communications net access protocol for CNR networks. The method by which IP packets are encapsulated and transmitted is specified in MIL-STD-188-220A.

3.2.4 Summary of Packet Standards

For reference purposes, Figure 3-1 shows a summary of the information transfer standards used for packet-switching that are mandated within the ATA.

3.3 EMERGING STANDARDS

Commercial communications standards and products will evolve over time. The ATA must evolve, as well, to benefit from these standards and products. The purpose of this section is to provide notice of those standards that are not yet a part of the ATA, but are expected to be adopted in the near future.

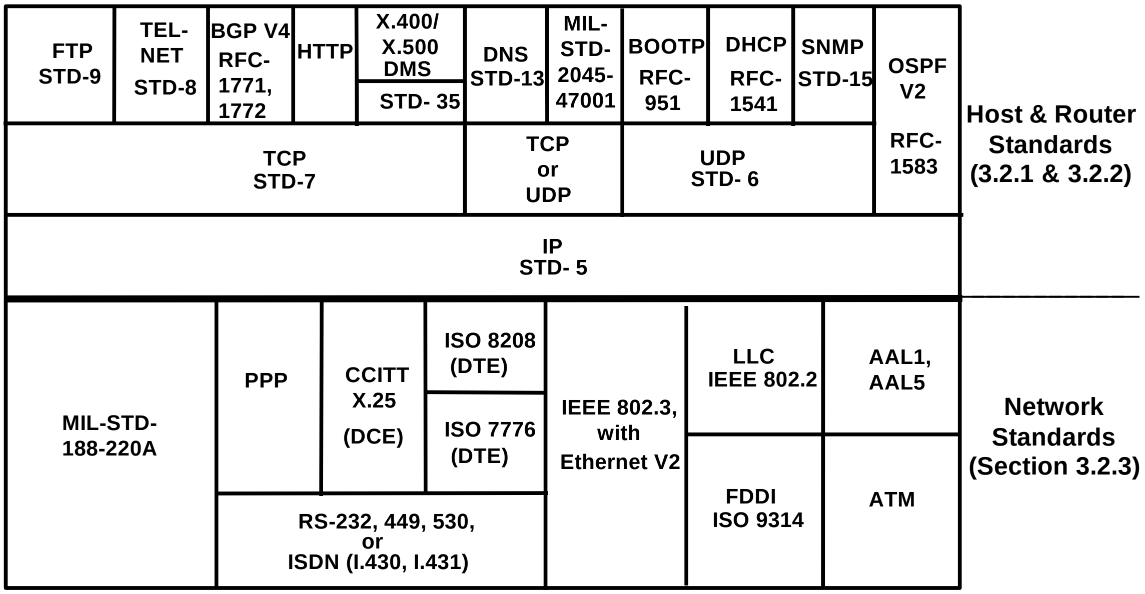


FIGURE 3-1. SUMMARY OF THE PACKET-SWITCHED TRANSFER STANDARDS

3.3.1 Emerging Host Standards

- *IP Next Generation/Version 6 (IPv6)*- IPv6 is being designed to provide better internetworking capabilities than are currently available within IP (Version 4). IPv6 will include support for expanded addressing and routing capabilities, authentication and privacy, autoconfiguration, and increased quality of service capabilities. IPv6 is described in RFC-1883, RFC-1884, RFC-1885, and RFC-1886.

- *Mobile Host Protocol* -The primary aim of this protocol is to provide information reachability for the mobile host. The intent is that a mobile host should not have to perform any special actions because of host migration. A mobile IP protocol is currently available as an Internet draft, entitled IP Mobility Support.

- *GPS Standards*- For the GPS standard, the following Interface Control Documents (ICDs) are under review: User Equipment ICD for the RS-232/RS-422 Interface of DoD Standard GPS User Equipment Radio Receivers (Draft) (ICD-GPS-153); GPS Receiver Application Module Interface, Parallel Dual Port Interface (Draft) (ICD-GPS-155); and Precise Time and Time Interval (PTTI) Interface, Rev A (ICD-GPS-060).

- *VTC Standards*- The following draft standards are part of the H.320 and T.120 suite, and are pending approval: H.323 (for use over Ethernet and FDDI networks) and T.128 (for audio visual control of multipoint multimedia systems).

3.3.2 Emerging Network Standards

- *Wireless network standards*- The IEEE 802.11 Committee is developing standards for wireless services across three transmission media: spread-spectrum radio; narrowband radio; and infrared energy. Wireless technology is useful in environments requiring mobility of the users or flexible network establishment and reconfiguration.

- *Personal Communications Services (PCS) and Mobile Cellular* - PCS will support both terminal mobility and personal mobility. Terminal mobility is based on wireless access to the public switched telephone network (PSTN). Personal mobility allows users of telecommunication services to gain access to these services from any convenient terminal (either wireline or wireless). Mobile cellular radio can be regarded as an early form of "personal communications service" allowing subscribers to place and receive telephone calls over the PSTN wherever cellular service is provided. The three predominant competing world-wide methodologies for digital PCS and Mobile Cellular access are: Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), and Global System for Mobile Communications (GSM). Of these three, CDMA offers the best technical advantages for military applications based on its utilization of Direct Sequence Spread Spectrum (DSSS) techniques for increased channel capacity, low probability of intercept (LPI), and protection against jamming. CDMA's low transmission power requirements should also reduce portable power consumption. The PCS standard for CDMA is J-STD-008 (Draft). The Mobile Cellular standard for CDMA is IS-95-A. 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 require support of multiple protocols to access region-specific international digital PCS/Mobile Cellular infrastructures.

- *The Common Management Information Protocol (CMIP)* - CMIP provides the information exchange capability to support the Common Management Information Service (CMIS). CMIS provides Open Systems Interconnection (OSI) management services to management applications. CMIP is specified in ISO/IEC 9596-1, also known as International Telephone and Telegraph Consultative Committee (CCITT) X.711. CMIS is specified in ISO/IEC 9595, also known as CCITT X.710. CMIS and CMIP are components of the OSI management framework, where ISO/ IEC 7498-4 (CCITT X.700) provides a general introduction to management concepts and where ISO/IEC 10040 (CCITT X.701) provides for an overview of the framework. CMIP is evolving and is generally accepted for switched telecommunications services. While CMIP is not mandated in the ATA, it is recognized as a protocol in current use within designated Army systems. It is expected that CMIP will evolve/coexist with SNMP to share parameters and agents in common, with added capabilities and a new manager-to-manager relationship.

SECTION 4
INFORMATION MODELING AND DATA EXCHANGE STANDARDS

4.1 INTRODUCTION

4.1.1 Purpose

This section identifies the minimum information standards applicable to information modeling and exchange of information for all systems. Information standards pertain to activity or process models, data models, data definitions, and data exchange.

4.1.2 Scope

This section provides implementation direction affecting the definition, design, development, and testing of information models and data exchange among systems. It is applicable at all organization levels and environments (e.g., tactical, strategic, sustaining base, and interfaces to weapons systems). This chapter is divided into two sections: data standardization and data exchange. Data Standardization mandates apply to all systems or components of systems. Data Exchange mandates apply to all information components that must interact with any external system or device. For example, some systems are in completely enclosed environments (e.g., an on-board missile guidance system that must signal to the weapon's on-board steering control) and may not need to comply specifically with these sections. The materiel developer must determine if his particular system or component within the system requires ANY interaction with the external environment. Those systems or components that require an external interface must adhere to the Data Exchange Standards. If in doubt, plan for interoperability until the system requirements determine otherwise.

The relationship of the Information Standards to the TAFIM is illustrated in Figure 4-1. Process models identify functionality required of mission area applications and identify the information required in the data model. The data model identifies the logical information requirements and metadata, which will be developed into physical database schemata and standard data elements. Once implemented in operational systems, the data will be shared using generic data exchange standards.

4.1.3 Background

An information model is a representation at one or more levels of abstraction of a set of real-world processes, products, and interfaces. A process (or activity) model is a representation of a mission area application, composed of one or more related activities, and data (i.e., abstract data types) is the product of each activity. A data model defines entities and their data elements and illustrates the entities' interrelationships. An interface model ties disparate processes together for some combined functionality. This chapter focuses on the use of process and data models. Interface models are customized to fit a particular project, hence system developers should create and use interface models as necessary.

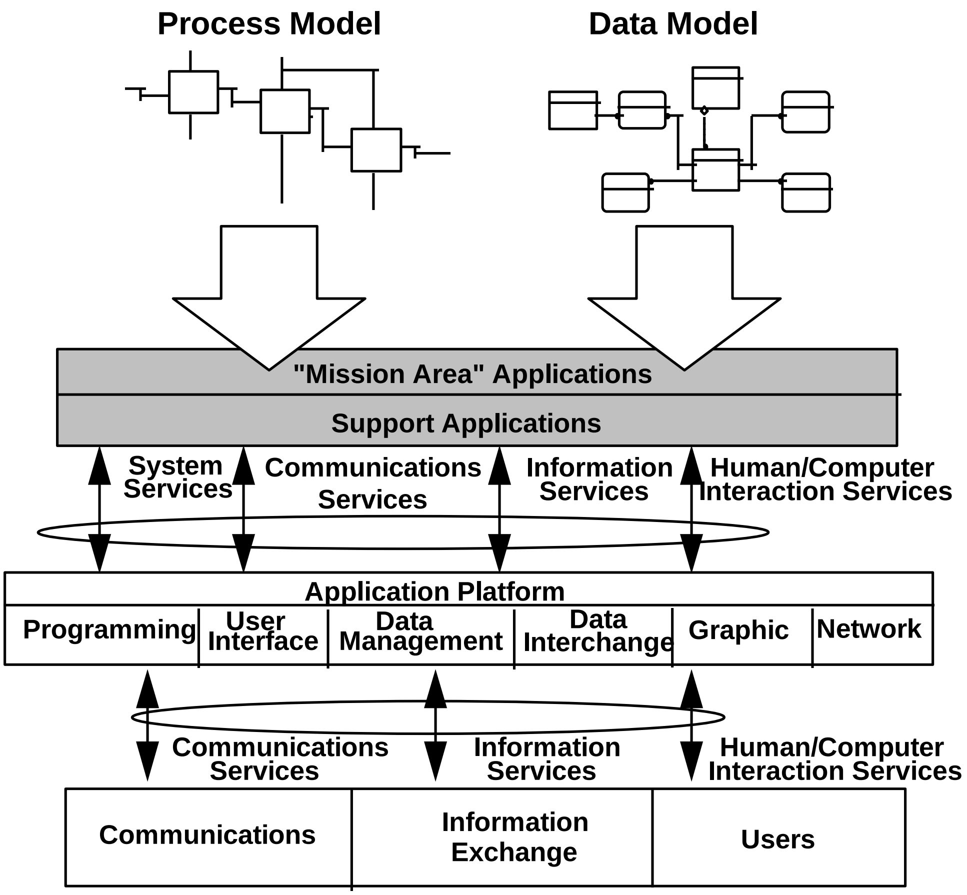


FIGURE 4-1. RELATIONSHIP OF TAFIM TO INFORMATION STANDARDS

To support the identification of information and information interchange requirements, the DOD has selected the **I**ntegrated Computer Aided Manufacturing **DEF**inition (IDEF) modeling methodology. DOD Directive 8320.1 requires IDEF0 in accordance with FIPS Pub 183 and IDEF1X in accordance with FIPS Pub 184 as the standard for function method and extended data method, respectively. The IDEF Modeling methodology defines an unambiguous set of the following components:

- Symbols (i.e., syntax) associated with modeling concepts and ideas.
- Rules for composing these symbols into abstract constructs.
- Rules for mapping "meanings" (i.e., semantics) to these constructs.
- Definitions of the relationships between activities and entities.

Information Standards define a logical view of data (meaning and contextual use) within an architecture. The process model is a view of the activities, both automated and manual, that an organization must perform in order to achieve its mission. Modeling an organization's processes and data: begins at the highest logical level, is decomposed into lower logical levels, and is communicated in a format that the users, particularly the subject matter experts, can easily understand and use.

In order to provide a single authoritative source for data definitions and documentation standards, the DOD created the Defense Data Dictionary System. The DDDS, which is managed by the Defense Information Systems Agency (DISA), is a DOD-wide central database that includes standard data entities, data elements and, soon, data models. The DDDS is used to collect and integrate individual data models into a DOD enterprise data model and to document content and format for data elements. Recent studies show three necessary data characteristics must be known to define interoperable databases. First, the context view of data must be developed to understand how data elements interact with each other. Second, a data element definition must be unambiguous. Third, the foreign key identifiers must be defined in parent to child data relationships. These characteristics are contained within the combination of the DDDS, IDEF0 and IDEF1X models. Figure 4-2 provides an objective view of how the process and data modeling standards contained in this section will support the development of interoperable systems.

Today, battlefield information exchange is accomplished by sending messages. The definition and documentation of these messages are provided by various messaging standards, such as Variable Message Format (VMF), and the U.S. Message Text Format (USMTF). Each message standard provides a means to define message form and functions (i.e., transfer syntax), which includes the definition of the message fields that are contained in each message. The message fields, which are currently defined in the various message standards, are not mutually consistent across message types, nor are they based on any process or data models, either within a message system or across message systems. Newer techniques can provide direct database-to-database exchange of data, without the user having to follow a rigid format. To use these newer techniques, the message fields must be converged with the data element set that is developed through the process and data modeling efforts defined in this section (4.2.1 and 4.2.2). This set is compliant with the Department of Defense data element standards established in accordance with the DOD 8320.1 series of directives.

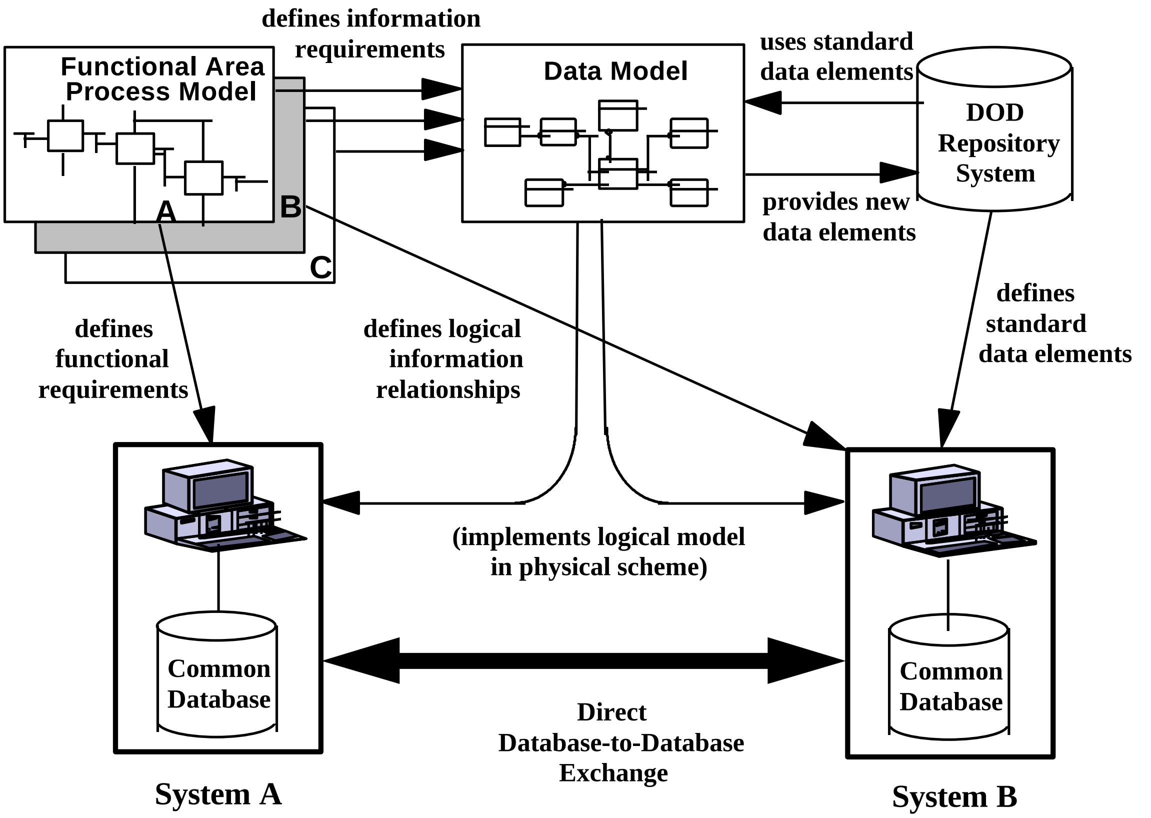

defines information requirements
Functional Area Process Model
A
B
C
Data Model
uses standard data elements
DOD Repository System
provides new data elements
defines functional requirements
defines logical information relationships
defines standard data elements
(implements logical model in physical scheme)
Common Database
Common Database
Direct Database-to-Database Exchange
System A
System B

FIGURE 4-2. OBJECTIVE INFORMATION EXCHANGE ARCHITECTURE

4.2 MANDATES

4.2.1 Process Model

System acquisition and development begin with the identification of the need (Mission Need Statement) for a system to rectify a capability deficiency and the development of an Operational Requirements Document (ORD). Prior to beginning system development (Milestone II) and prior to major software upgrades to existing systems, the ORD shall be used to model information products and requirements using the IDEF0 methodology (FIPS Pub 183) to a level of detail sufficient to identify each entity in the data model that is involved in an activity. The activity model shall form the basis for data model development or refinement. The activity model will be validated against the requirements document and doctrine and then approved by the combat developer. The activity model that is contained in the DOD Process Model Repository (currently managed by the Army Corps of Engineers) shall be used as a reference for extending activity models for specific programs.

The doctrinally based process models shall be used to describe the baseline functional and interface requirements. These models will normally be used in systems development in the system's User Functional Description (UFD). System developers can maintain traceability of requirements back to these process models. The process model will be enhanced and refined to accommodate the increased knowledge inherent in system development. An approved process model, by the materiel developer, can support criteria for Milestone II and III decisions.

As activity models are developed, security levels shall be considered. Most process models are unclassified even if the content of one or more activity characteristics (see ICOM below) is classified. However, if the developer determines that parts of the model must contain classified information, appropriate regulatory safeguards will be met. Different parts of the models can be labeled with different security labels. It must be possible to classify an entire model or to classify only certain activities and inputs, controls, outputs, and mechanisms (ICOM) within a model. Activities and ICOMs must have a provision for hierarchical (e.g., SECRET, TOP SECRET) and non-hierarchical (e.g., US ONLY, RELROK) security classification levels for the case where the model is unclassified, but the data is classified. It must be possible for a model to assume a range of security classification levels during its life cycle development as requirements are refined. It must be possible to classify a previously unclassified model when it is re-used within a different context.

4.2.2 Data Model

The basis for data modeling shall be the DOD Defense Data Model (DDM). The DDM is a corporate-wide data model that provides the standard meaning and use of specific data elements to the developers of all DOD systems. Adherence to the DDM will ensure DOD agencies are data interoperable among all systems. Tactical systems must incorporate applicable C2 Core Data Model (C2CDM) elements. The C2CDM is a subset of the DDM. Both reside in the DDDS. It provides the tactical metadata and modeling elements for all DOD. New information requirements that are derived from data models and approved through the DOD Data Standardization Program (Department of Defense Directive (DODD) 8320 Series) will be used to extend the DDM and C2CDM as appropriate. Computer Automated Software Engineering (CASE) tools that support IDEF1X diagrams shall be used to extend the model with additional logical entities, attributes, and relationships. The IDEF1X syntax and diagramming conventions shall be in accordance with FIPS Pub 184. Data model development shall proceed in accordance with DOD 8320.1-M-1.

The data models shall be used in software requirements analyses and design activities as a logical basis for physical database design. Developers of new and existing systems shall maintain traceability between their physical database schema and the DDM and C2CDM, as applicable, allowing links from interface requirements to database population and update processes. A top level data model will be prepared for Milestone II decisions; a fully attributed data model will be assessed during the Preliminary Design Review and Critical Design Review.

As data models are developed, security levels and caveats shall be considered. Most data models are unclassified even if the content of one or more data elements is classified. However, if the developer determines that parts of the model must contain classified information, appropriate regulatory safeguards will be met.

4.2.3 Data Definitions

System developers shall use the DDDS as a primary source of data element standards. DOD Directive 8320.1 provides the procedures for Data Administration. DOD 8320.1-M-1 provides data element standardization procedures. A classified version of the DDDS is being developed to support standardization of classified data elements and data models.

4.2.4 Data Exchange

4.2.4.1 Data Exchange Applicability

This section covers the exchange of information among mission area applications within the same system or among different systems. This is the scope of the term "data exchange." The exchange of information among applications shall be based on the logical data models developed as the result of identifying information requirements through activity or process models. The data model identifies the logical information requirements, which shall be developed into physical database schemata and standard data elements. The standard data elements shall be exchanged using the data management, data interchange and distributed computing services of application platforms (Refer to Section 2 for further guidance on these services). The intent is to exchange information directly between systems without the constraint of formatted messages.

For purposes of this document we must clarify subtle differences between "data exchange" and "data interchange." Data Exchange is the system or *application-independent* ability of data elements to be shared. Data Interchange, on the other hand, is system or *application-specific* sharing of objects such as documents, images, etc. Hence, this section discusses data exchange as the *generic* ability of a system or application to share data. Data Interchange standards, such as JFIF, form part of the DII COE and facilitate the sharing of data through the use of system or application *formats*. Key references include Section 2.2.2.1.3, for SQL standards in Data Management Services, and Section 2.2.2.1.4 for Data Interchange Services.

The message sets described below are mandated as the current means of transferring information until mechanisms that use standard data elements are approved. *DISA is the proponent for information exchange using standard data.*

4.2.4.2 Variable Message Format (VMF) Messages

VMF messages shall be used for information transfer between systems requiring variable bit-oriented messages. VMF messages are specified in the Joint VMF Technical Interface Design Plan (TIDP). VMF messages shall use MIL-STD-2045-47001 as a connectionless application layer. MIL-STD-2045-47001 provides common message-handling information for VMF messages, such as destination addresses, precedence, security classification, data and time, and operator receipt/compliance.

4.2.4.3 US Message Text Format (USMTF) Messages

USMTF messages will be used when required for Joint interoperability if standard data exchange is not possible. USMTF messages are documented in MIL-STD-6040 (formerly JCS Publication 6-04). USMTF messages are character based and usually limited to the teletype character set.

4.2.4.4 Tactical Digital Information Link (J Series) Messages

The J-Series Family of TDLs allow information exchange using common data element structures and message formats which support time critical information. They include Air Operations/Defense, Maritime, Fire Support, and Maneuver Operations. These are the primary data links for exchange of bit-oriented information. The family consists of LINK 16, LINK 22, and the Variable Message Format (VMF), and interoperability is achieved through the use of J-Series family messages and data elements. The policy and management of this family are described in the Joint Tactical Data Link Management Plan (JTDLMP), dated April 1996.

New message requirements shall use these messages and data elements, or use the message construction hierarchy described in the JTDLMP. The mandated standards for information exchange between systems that use a Joint Tactical Data Link are:

- Joint Tactical Information Distribution System (JTIDS) Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 3 August 1994.
- STANAG 5516, Edition 1, Tactical Data Exchange - LINK 16, Ratified 2 March 1990.

4.2.4.5 Remote Procedure Calls

The Distributed Computing Environment (DCE) provides the capability to exchange standard data among heterogeneous platforms, DBMS and legacy data structures using Remote Procedure Calls (RPCs). Interfaces of this type can be defined using the DCE Interface Definition Language (IDL) but must use applicable data elements from the DDDS. See Section 2.2.2.2.4 for specific standards.

4.2.5 Modeling and Simulation Information and Data Exchange Standards

Refer to Appendix G for information standards, both mandated and emerging, that are unique to the modeling and simulation domain.

Refer to Section 5 for data exchange standards containing the specification of symbol codes that are critical to information exchange and interoperability (e.g., FM-101-5-1 and MIL-STD-2525).

4.3 EMERGING STANDARDS

4.3.1 Activity Modeling

Currently, there are no known emerging Activity Model Standards.

4.3.2 Data Modeling

Emerging standards will be adopted when appropriate. A prime example consists of Object Oriented Analysis (OOA), Object Oriented Programming (OOP), Object Oriented Data Modeling, and Object Oriented DBMS'. Although there is no formal standard supporting this new paradigm, government and industry are inexorably gravitating to the object oriented techniques, in order to overcome the inherent design limitations of IDEF. It is anticipated that the C2CDM will ultimately be portrayed as an object model. IDEF1X is currently undergoing a face lift, in order to be more viable in an object-oriented environment. The new version has been tentatively called IDEF97, Conceptual Schema Modeling.

This standard accommodates object-oriented methods (OOM). IDEF1X97 is being developed by the IEEE IDEF1X Standards Working Group of the IEEE 1320.2 Standards Committee. The standard describes two styles of the IDEF1X model. The key-style is used to produce information models which represent the structure and semantics of data within an enterprise and is backward-compatible with the US Government's Federal Standard for IDEF1X, FIPS 184. The identity-style is a wholly new language which provides system designers and developers a robust set of modeling capabilities covering all static and many dynamic aspects of the emerging object model. This identity-style can, with suitable automation support, be used to develop a model which is an executable prototype of the target object-oriented system. The identity-style can be used in conjunction with emerging dynamic modeling techniques to produce full object-oriented models.

4.3.3 Data Exchange

The Army with DISA Joint Interoperability and Engineering Organization (JIEO) is working to develop the strategy and policy for migration from the current multiple bit-oriented and character-oriented tactical data link message formats to a minimal family of DOD 8320.1-M-1 compliant information exchange standards. A normalized unified data/message element dictionary will be developed based on the Defense Data Model (DDM) and associated data element standards. The dictionary will support both character and bit-oriented representation of the standard data and their domain values. Message standards will then establish the syntax for standard data packaging to support mission requirements (e.g., character or bit-oriented, fixed or variable format, etc.). The unified data dictionary will ensure that multiple representations are minimized and transformation algorithms are standardized.

Message and data element standards must be independent of the information transport standards, protocols and profiles. Refer to Section 3 of this document for information transfer standards.

USMTF messages are character based and documented in MIL-STD-6040 which represents the 1995 baseline version to which all non-standard Joint interoperability messages are to adhere. (An emerging 1997 version is expected to replace the 1995 version.)

This page was intentionally left blank.

SECTION 5
HUMAN-COMPUTER INTERFACES

5.1 INTRODUCTION

5.1.1 Purpose

This section provides a common framework for Human-Computer Interface (HCI) design and implementation in Army automated systems. The objective is to standardize user interface design and implementation options thus enabling Army applications within a given domain to appear and behave consistently. The standardization of HCI appearance and behavior within the Army will result in higher productivity, shorter training time, and reduced development, operation, and support costs. This section specifies HCI design guidance, mandates, and standards.

5.1.2 Scope

This section applies to the human interface of automated systems described in Paragraph 1.1.3. This version mandates the design of graphical and character-based displays and controls for Army automated systems.

5.1.3 Background

The objective of system design is to ensure system reliability and effectiveness. To achieve this objective the human must be able to interact effectively with the system. Humans interact with automated systems using the HCI. The HCI includes the appearance and behavior of the interface, physical interaction devices, graphical interaction objects, and other human-computer interaction methods. A good HCI is both easy to use and appropriate to the operational environment. It exhibits a combination of user-oriented characteristics such as intuitive operation, ease and retention of learning, facilitation of user task performance, and consistency with user expectations.

The need to learn the appearance and behavior of different system HCIs increases both the training burden and the probability of operator error. What is required are interfaces that exhibit a consistent appearance and behavior both within and across applications and systems.

5.2 MANDATES

5.2.1 General

The predominant types of HCIs include graphical user interfaces (GUIs) and character-based interfaces. For all DOD automated systems, the near-term goal is to convert character-based interfaces to a GUI. Although GUIs are the preferred user interface, some specialized interfaces (e.g., embedded/weapons systems) may require use of character-based or alternative interfaces due to operational, technical, or physical constraints. These specialized interfaces shall be defined by domain-level style guides and further detailed in system-level user interface specifications. However, graphical and character-based interface styles shall not be mixed within the same system or family of systems.

5.2.1.1 Graphical User Interfaces

Graphical user interfaces for Army automated systems shall be based on a commercial user interface style in accordance with paragraph 5.2.2.1. Hybrid GUIs that mix user interface styles (e.g., Motif with Windows) shall not be created.

Developers shall investigate use of a commercial GUI style, or subset thereof, before developing a custom GUI. Operational, technical, or physical constraints associated with certain types of systems (e.g., embedded/weapons systems) may not permit the use of a commercial GUI style. If a non-commercial GUI is necessary as the basis for the HCI, developers shall provide detailed justification and receive approval before proceeding with development.

5.2.1.2 Character-based Interfaces

Systems with an approved requirement for a character-based interface shall comply with the character-based interface design criteria contained in the *DOD HCI Style Guide*.

While not mandated, additional guidance for developing character-based interfaces can be found in ESD-TR-86-278, *Guidelines for Designing User Interface Software* (Smith and Mosier 1986).

5.2.1.3 Symbology

MIL-STD-2525A, *Common Warfighting Symbology*, is mandated. A portion of MIL-STD-2525A is based on FM 101-5-1, *Operational Terms and Graphics*. Note that MIL-STD-2525A only describes the symbol construction and appearance. Developers should consult appropriate doctrinal publications such as FM 101-5-1 for the doctrinal meaning and use of Military symbology.

5.2.1.4 Security

The HCI shall comply with Section 6 of the Army Technical Architecture; Appendix A, Security Presentation Guidelines, DOD HCI Style Guide; and other applicable portions of the DOD HCI Style Guide.

5.2.2 Style Guides

Figure 5-1 illustrates the hierarchy of style guides that shall be followed to maintain consistency and good HCI design within the Army. This hierarchy, when applied according to the HCI design process mandated in the DOD HCI Style Guide, provides a framework that supports iterative prototype-based HCI development. The process starts with top-level general guidance and uses prototyping activities to develop system-specific design rules.

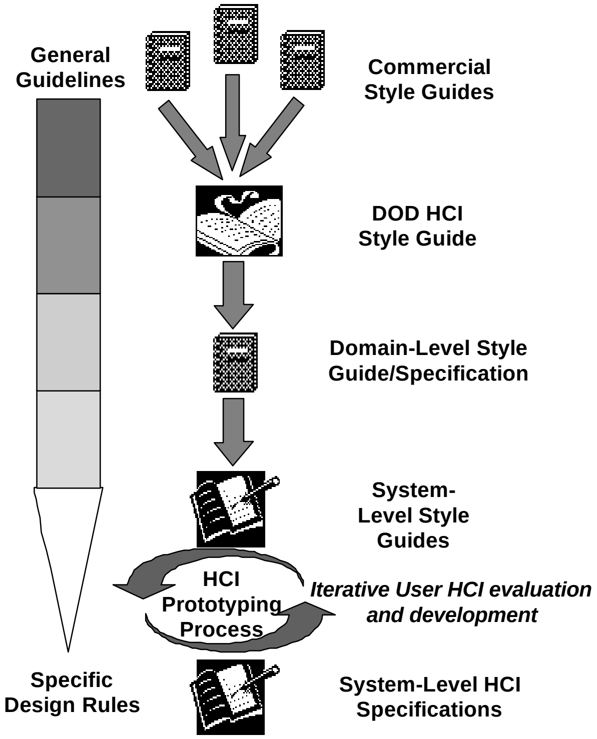

General Guidelines
Commercial Style Guides
DOD HCI Style Guide
Domain-Level Style Guide/Specification
System-Level Style Guides
HCI Prototyping Process
Iterative User HCI evaluation and development
Specific Design Rules
System-Level HCI Specifications

FIGURE 5-1. HIERARCHY OF STYLE GUIDES

The interface developer shall use the selected commercial GUI style guide, refinements provided in the*DOD HCI Style Guide,*and the appropriate domain-level style guide, as well as input from human factors specialists, to create the system-specific HCI. The following paragraphs include specific guidance regarding the style guide hierarchy levels.

5.2.2.1 Commercial Style Guides

A commercial GUI style shall be selected as the basis for user interface development. The GUI style selected is usually driven by the mandates specified in Section 2 (User Interface

Services and Operating System Services). The following commercial GUI style guide is mandated.

- Open Software Foundation (OSF)/MotifTM Style Guide, Revision 1.2 (OSF 1992).

OSF/Motif is a non-proprietary interface style that supports the DOD goal for an open systems environment. Use of non-commercial GUI styles is addressed in paragraph 5.2.1.1.

5.2.2.2 DOD HCI Style Guide

The DOD HCI Style Guide, Volume 8 of the TAFIM, was developed as a guideline document presenting recommendations for good human-computer interface design. This document focuses on human-computer behavior and concentrates on elements or functional areas that apply to DOD applications. These functional areas include such things as security classification display, mapping display and manipulation, decision aids, and embedded training. This style guide, while emphasizing commercial GUIs, contains interface design criteria that can be used for all types of systems including those which employ character-based interfaces.

Although the *DOD HCI Style Guide* is not intended to be strictly a compliance document, it does represent DOD policy. Army systems shall therefore conform to the interface design criteria contained in the *DOD HCI Style Guide.*

Although the general principles given in this document apply to all interfaces, some specialized areas require separate consideration. Specialized interfaces, such as those used in real time weapon system applications, have interface requirements that are beyond the scope of the *DOD HCI Style Guide.* These systems shall comply with their domain-level style guide and follow the general principles and HCI design guidelines presented in the *DOD HCI Style Guide*.

5.2.2.3 Domain-level Style Guides

A domain-level HCI style guide shall be developed by each approved domain within the Army. These style guides will reflect the consensus on HCI appearance and behavior for a particular domain (e.g., C3I) within the Army. The domain-level style guide will be the compliance document and may be supplemented by a system-level style guide created as an appendix to the domain-level style guide.

The C3I domain has adopted the *User Interface Specifications for the Defense Information Infrastructure (DII)* as their domain-level style guide.

The weapons system domain has adopted the *U.S. Army Weapon Systems Human-Computer Interface (WSHCI) Style Guide* as their domain-level style guide. The WSHCI style guide will be extended by developing sub-domain style guides for the Real-Time/Near-Real-Time (RT/NRT) weapons system sub-domains of ground, aviation, missile, and soldier systems.

Until a domain develops its domain-level style guide, it shall comply with paragraph 5.2.2.2 above and the*User Interface Specifications for the Defense Information Infrastructure (DII).*

5.2.2.4 System-level Style Guides

System-level style guides provide the special tailoring of commercial, DOD, and domain-level style guides. These documents include explicit design guidance and rules for the system while maintaining the appearance and behavior provided in the domain-level style guide. If needed, the system-level style guide will be created as an appendix to the applicable domain-level style guide. The system-specific appendix will specify unique requirements not addressed in the domain-level style guide.

5.3 EMERGING USER INTERFACE STYLES, SPECIFICATIONS, AND STANDARDS

The Army Technical Architecture mandates the development of a domain-level HCI style guide for each approved domain within the Army. Currently, a domain-level style guide exists for the C3I domain. Efforts are underway to develop domain-level style guides for other domains. These emerging domain-level style guides will be mandated for use when they are completed, coordinated across domains, and approved.

MIL-STD-1472D which has been canceled will be republished as a Design Criteria Standard and will be cited when it is approved. Expected publication date is December 1996.

The CDENext Style Guide, a commercial style guide for the Common Desktop Environment (CDE), is projected to be released in late 1996. This style guide merges features of Motif 2.0 and the CDE Version 1.0 with enhancements.

Currently, research is underway to investigate non-traditional user interfaces. Such interfaces may be gesture-based and may involve processing multiple input sources, such as voice and spatial monitors. Ongoing research and investigation include the use of virtual reality and interface agents. Interface agents autonomously act on behalf of the user to perform various functions, thus allowing the user to focus on the control of the task domain. The Army will integrate standards for non-traditional user interfaces as research matures and commercial standards are developed.

This page was intentionally left blank.

SECTION 6
INFORMATION SECURITY

6.1 INTRODUCTION

6.1.1 Purpose

This section describes the information security standards that apply to Army systems that produce, use or exchange information electronically. These standards provide the warfighter with a seamless flow of timely, accurate, accessible, and secure information.

6.1.2 Scope

The standards described in this section are drawn primarily from formally developed national and international standards. In order to be effective, security standards must be integrated into and used with the other information standards in the ATA. Therefore this section is structured to mirror the structure of the ATA itself with security standards organized corresponding to each ATA section. An additional subsection has been provided to address security unique considerations. This section assumes a level of knowledge of information security above an operational level.

6.1.3 Background

The TAFIM provides a blueprint for the Defense Information Infrastructure (DII), capturing the evolving vision of a common, multipurpose, standards-based technical infrastructure. The DOD Goal Security Architecture (DGSA), Volume 6 of the TAFIM, provides a comprehensive view of the architecture from the security perspective. The DGSA is a generic architectural framework for developing mission specific security architectures. The DGSA provides the basis of the security standards discussion in this section of the ATA. While the DGSA is oriented toward future systems, today's technology and standards can be used to achieve DGSA-consistent systems that are on the path to complete implementation of the DGSA.

Systems that process sensitive data must be certified and accredited before use. Certification is the technical evaluation of an Automated Information System's (AIS's) security features and other safeguards, made in support of the accreditation. Accreditation is the authorization by the Designated Approving Authority (DAA) that an automated system may be placed into operation. Therefore, system developers should open dialog with the DAA concurrently with their use of the ATA, as DAA decisions can affect the applicability of standards within specific environments.

Security requirements and engineering should be determined in the initial phases of design. The determination of security services to be used and the strength of the mechanisms providing the services are primary aspects of developing the specific security architectures to support specific domains. Section 6 of the ATA is used after operational architectural decisions are made regarding the security services needed and the required strengths of protection of the mechanisms providing those services. Section 6 of the ATA can also be used to assess the relevance of standards that can be met with evaluated commercial and government-provided components and protocols. The ATA can be used as a tool to evaluate elements of the system architecture regarding operational security requirements, standards compliance, interoperability with other systems, and cost reduction through software reuse.

Other technical architectural decisions must be made after considering Army enterprise level regulations. Army Regulation (AR), Information System Security (AR 380-19) contains the necessary references to other standards and mandates that must be considered by a system developer. Comprehensive system and security engineering are the basis for selecting proper combinations of standards to develop a system that meets the needs of mission security requirements.

6.2 INFORMATION PROCESSING SECURITY STANDARDS

Information processing security services are defined in ISO 7498-2. These services include authentication, access control, data integrity, data confidentiality, non-repudiation and availability. Availability management is not included in this international standard but is specifically called out in the DGSA for the local communications system and communications network management facilities. ISO 10181, OSI Security Frameworks, extends this list of services by including security audit and key management.

As a general requirement, all Army systems must demonstrate that they meet the applicable security profile described in both AR 380-19 and the DOD Trusted Computer System Evaluation Criteria standard, DOD 5200.28-STD.

6.2.1 Mandated Standards

6.2.1.1 Application Software Entity

The DOD Multilevel Security Initiative (MISSI) provides products for protecting information in electronic form. Its use is currently mandated for electronic mail and will be extended to other areas as products become available. The various specifications and types of products available that implement the security services are identified in the MISSI Implementation Guide. One of the products is the FORTEZZA card, a Personal Computer (PC) card (formerly known as a Personal Computer Memory Card International Association (PCMCIA) card) that provides several security services for electronic mail. Some security functions that would normally be invoked by applications are described in Section 6.3.1.1.1. The interface to the FORTEZZA card is described in:

- FORTEZZA Application Implementor's Guide, MD4002101-1.52, 5 March 1996.

- FORTEZZA Cryptologic Interface Programmer's Guide, MD4000501-1.52, 30 January 1996.

Evaluation Criteria Standards, which describe security designations such as classes C2, B1, etc. are contained in:

- DOD 5200.28-STD, The Department of Defense Trusted Computer System Evaluation Criteria, December 1985.
- National Computer Security Center (NCSC)-TG-021, Version-1, Trusted Database Management System Interpretation, April 1991.

6.2.1.2 Application Platform Entity

The following standard is mandated for security auditing or alarm reporting:

- DOD 5200.28-STD, The Department of Defense Trusted Computer System Evaluation Criteria, December 1985.

Authentication Security Standard:

If Open Software Foundation (OSF) Distributed Computing Environment (DCE) Version 1.1 is used, the following authentication standard is mandated:

- RFC-1510, The Kerberos Network Authentication Service, V.5, 10 September 1993.

6.2.2 Emerging Standards

6.2.2.1 Application Software Entity

FORTEZZA provided security services for functions other than electronic mail are still emerging and are not yet mandated. However, systems should strongly consider the possibility of a mandate in the near future.

Generic Data Unit Protection API:

Applications, where data needs to be protected without any on-line connection with the intended recipient(s) of that data, could make use of a generic security service. Subsequent to being protected, the data unit can be transferred to the recipient(s), or to an archive where it may be processed days or years later as unprotected. The Independent Data Unit Protection (IDUP)-GSS-API extends the GSS-API (RFC-1508) for non-session protocols and applications requiring protection of a generic data unit (such as a file or message) in a way which is independent of the protection of any other data unit and independent of any concurrent contact with designated "receivers" of the data unit.

- Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API), 13 June 1996, draft-ietf-cat-idup-gss.05.txt.

6.2.2.2 Application Platform Entity

The following draft IEEE standards define a standard interface and environment for POSIX-based computer operating systems that require a secure environment:

- IEEE P1003.1e, POSIX Part 1: System API - Protection, Audit, and Control Interfaces, Draft 15.
- IEEE P1003.2c, POSIX Part 2: Shell and Utilities - Protection and Control Interfaces, Draft 15.
- DII 10164-9, SC21 N9390, Information Technology - Open System Interconnection - Systems Management - Part 9: Objects and Attributes for Access Control (final text).

Army systems that are required to exchange information at multiple sensitivity levels require a standard labeling format to identify the sensitivity level of the information. The following labeling standard applies:

Security Alarm Reporting:

- ISO/IEC 10164-7, 1992, Information Technology-Open System Interconnection - Systems Management - Part 7: Security Alarm Reporting Function, (ITU-T X.736) 1992.

6.2.2.3 Remote Authentication

Remote Authentication Dial In User Service (RADIUS), et. al., July 1996, is an Internet draft that describes a protocol for carrying authentication, authorization, and configuration information between a Network Access Server that desires to authenticate its links and a shared Authentication Server.

6.2.2.4 Generic Security Service Application Program Interface (GSS API)

The Generic Security Service Application Program Interface (GSS-API) (RFC 1508), September 1993, definition provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments. This specification defines GSS-API services and primitives at a level independent of underlying mechanism and programming language environment, and is to be complemented by other, related specifications:

- Documents defining specific parameter bindings for particular language environments.
- Documents defining token formats, protocols, and procedures to be implemented in order to realize GSS-API services atop particular security mechanisms.

6.2.2.5 Security Management Protocols

Progress toward approval of SNMP V2 has been slow. In the meantime CMIP has been adopted by many developers for the management of circuit-switched systems. It is envisioned that a future Network and System Management standard will incorporate features of both SNMP V2 and CMIP for packet-switched and circuit-switched environments respectively. Developers should build or use products that are based on these standards to the maximum extent possible.

- ISO/IEC 9596-1, 1991, Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) - Part 1: Specification (includes Amendments 1 and 2 of 9596-1, 1990), ISO/IEC JTC1 SC21/WG4, IS June 1991 (ITU-T X.711, 1991).
- IEEE 802.10c/D6 Standard for Interoperable LAN Security-Part C: Key Management, IEEE, Draft 6 issued 1994; draft 7 in-process, (security management/key management/protocols).

The MISSI system performs a number of functions through the exchange of administrative messages between MISSI components. These messages are characterized by the fact that they are all necessary for "system management" of MISSI-protected networks rather than being user-based messages. The following was created to provide a standard framework for defining these messages:

- SDN.703, MISSI Management Protocol (MMP), Revision 1.0, 7 June 1996.

6.3 INFORMATION TRANSFER SECURITY STANDARDS

This section discusses the security standards that have an impact on the information transfer security services.

6.3.1 MANDATES

6.3.1.1 MISSI

6.3.1.1.1 MISSI Cryptographic Algorithms

- MISSI's current FORTEZZA card includes a CAPSTONE chip containing a time stamping capability and four algorithms. The algorithms can be found in FIPS PUB 180-1, National Institute of Standards and Technology (NIST) Secure Hash Algorithm (SHA) (NIST; April 1995); FIPS PUB 186, NIST Digital Signature Standard (DSS) algorithm (NIST; 19 May 1994); National Security Agency (NSA)-developed Type II confidentiality algorithm (SKIPJACK); and NSA-developed Type II Key Exchange Algorithm (KEA), NSA, R21-Tech-23-94, 12 July 1994.

The following API governs the interface to the services of the FORTEZZA card:

- FORTEZZA Cryptologic Interface Programmers Guide MD4000501-1.52, 30 January 1996.

Design of the operating system drivers and/or hardware adapters to use the resources provided by the FORTEZZA card need the technical detail contained in the Interface Control Document (ICD). For the card, this can be found in for the FORTEZZA Crypto Card ICD, Version P1.5, 22 December 1994, and in FORTEZZA Plus Crypto Card ICD, Release 3.0, 01 June 1995.

For those systems that need to escrow an encryption key, the following standard applies:

- FIPS PUB 185, NIST, 9 February 1994, Escrowed Encryption Standard.

6.3.1.1.2 Security Protocols

Security protocols that are algorithm independent, such as Message Security Protocol (MSP) and Network Layer Security Protocol (NLSP), can readily take advantage of these algorithms. Many of the protocols developed under the Secure Data Network System (SDNS) program and published under NIST in report NISTIR 90-4250, have become part of MISSI. MISSI currently uses MSP for messaging, Key Management Protocol (KMP), and Security Protocol at Layer 3 (SP3). SP3 is used in two MISSI products, the Tactical End-to-End Encryption Device (TEED) and the Network Encryption System (NES). Additionally, MISSI has recently added FIPS PUB 196, Entity Authentication Using Public Key Cryptography, 16 September 1996, as its identification and authentication (I&A) protocol.

The following standard is mandated for Army systems that are required to exchange security attributes, for example sensitivity labels:

- MIL-STD-2045-48501, Common Security Label, 25 January 1995.

6.3.1.1.3 MISSI Digital Signature Infrastructure

Wide-spread use of MISSI is dependent upon the successful establishment of a certificate and key management infrastructure. This infrastructure is responsible for the proper creation distribution and revocation of the end user's public key certificates. These certificates are based on ITU-T Rec. X.500 (ISO/IEC 9594-1) Directory Infrastructure and ITU-T Rec. X.509 Version 3 (ISO/IEC 9594-8.2), The Directory: Authentication Framework, 1993. Until the planned DMS X.500 directory infrastructure components are in place, developers must use an interim non-standard local caching system.

6.3.1.2 Transport Mechanisms

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

6.3.2 Emerging Standards

6.3.2.1 Security Association Management

- ISP-421/94.05.15 Revision 1.0: The ISDN Security Program (ISP) Security Association Management Protocol (SAMP).

6.3.2.2 Secure World Wide Web (WWW) Transactions

EDI is the current DOD mandated mechanism for electronic commerce and will probably continue to be supported by industry for large volume, commodity-type procurements at the wholesale level. EDI requires translation software to convert business application information into an EDI information standard. A common standard in the United States is the ANSI X.12 EDI format.

There are several competing schemes for encryption; however, the two predominant and totally incompatible approaches are Netscape's Secure Courier and Microsoft's Secure Transaction Technology. Both of these schemes use the same Secure Sockets Layer (SSL) encryption scheme.

The Internet Draft for SSL being considered for standardization:

- For SSL, Internet DraftSecure Sockets Layer (SSL) Protocol, Version 3.0, draft-freier-ssl-version3-01.txt, 13 March 1996.

6.3.2.3 Networking Security Standards

- Security Architecture for the Internet Protocol (RFC 1825).
- IP Authentication Header (RFC 1826), with IP Authentication using Keyed MD5 (RFC 1828).
- IP Encapsulating Security Payload (ESP) (RFC 1827), with The ESP DES-CBC Transform (RFC 1829).
- IEEE 802.10, IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS), IEEE, 1992.
- IEEE 802.10a, Standard for Interoperable LAN Security-The Model, IEEE, Draft Jan 1989.
- IEEE 802.10b, Standard for Interoperable LAN Security-Part B: Secure Data Exchange, IEEE, 1992.

6.3.2.4 Security Protocols

The Common Internet Protocol Security Options (CIPSO) of the following emerging standard is expected to adopt MIL-STD-2045-48501, Common Security Label:

- Trusted Systems Interoperability Group (TSIG) Trusted Information Exchange for Restricted Environments (TSIX(RE)) 1.1.

6.3.2.5 Other

- ISO/IEC 10021-1, 1990/DAM 4, Information Technology-Message Handling Systems (MHS)-Part 1: System and Service Overview-Amendment 4: Interpersonal Messaging Security Extensions, ISO/IEC JTC1 SC18/WG4, IS 1990 (ITU-T X.400).

6.3.3 Summary of Standards

Table 6-1 shows a mapping of common protocols and security standards and protocols that may be used to provide the required security services. International Organization for Standardization (ISO) 7498-2 Security Service Recommendations (1989), provides a list of applicable security services and makes recommendations for their implementation.

The appropriate security services required for any Army system must be determined during that system's security engineering process. This process must be closely coordinated with the system's designated approving authority (DAA), who will be cognizant of the germane security policies.

TABLE 6-1 NOTIONAL MAPPING OF PROTOCOLS AND SECURITY STANDARDS

Layer	Common Protocols		Security Standards/Protocols
		M	**DOD 5200.28-STD**(Orange Book)
		M	**FIPS PUB 180-1**(Secure Hash Standard)
	Interactive Session:	M	**FIPS PUB 185**(Escrowed Encryption Standard)
Application		M	**FIPS PUB 186**(Digital Signature Standard)
	Connection Oriented	M	**FIPS PUB 196** (Entity Auth. Using Public Key Crypto.)
		M	**ITU X.509 v3**(Directory Auth. Framework)
	dialup	M	**KMP** (Key Management Protocol)
	FTP	M	**RFC 1510**(Kerberos)
	PPP/SLIP Setup	E	**GSS API**(Generic Security Services API, RFC 1508)
	rlogin	E	**IEEE 802.10C**(SILS Part c-Key Management)
	Telnet	E	**ISP-421/94.05.15 rev 1**(Sec Assoc Mgmt Protocol)
		E	**RADIUS**(Remote Authentication Dial-In User Service)
		E	**SSL** (Secure Socket Layer)
		M	**DOD 5200.28-STD**(Orange Book)
		M	**FIPS PUB 180-1**(Secure Hash Standard)
Presentation		M	**FIPS PUB 185**(Escrowed Encryption Standard)
	Non-Session:	M	**FIPS PUB 186**(Digital Signature Standard)
		M	**FIPS PUB 196** (Entity Auth. Using Public Key Crypto.)
	Connectionless	M	**FORTEZZA**(Interface Control Document)
		M	**FORTEZZA Plus**(Interface Control Document)
	Dir Server Access	M	**ITU X.509 v3**(Directory Auth. Framework)
	E-Mail	M	**KMP** (Key Management Protocol)
	EDI	M	**MD4000501-1.52**(FORTEZZA Crypto. Prog. Guide)
	WWW	M	**MD4002101-1.52**(FORTEZZA Appl. Imple. Guide)
Session		M	**MSP** (Message Security Protocol)
		M	**RFC 1510**(Kerberos)
		E	**IDUP-GSS API**(Indepen. Data Unit Prot.-GSS API)
		E	**IEEE 802.10c**(SILS Part c-Key Management)
		E	**IEEE P1003.1e** (POSIX, Protection)
		E	**IEEE P1003.2c** (POSIX, Shell and Utilities)
		E	**SSL** (Secure Socket Layer)
		E	**TSIX(RE) 1.1**(Trstd Sec Info Ex Restricted Envir)
Transport		E	**ISP-421/94.05.15 rev 1**(Sec Assoc Mgmt Protocol)
	ATM	E	**NLSP (SP3)**(Network Layer Security Protocol)
	TCP/IP	E	**RFC 1825**(IP Security Architecture)
	UDP	E	**RFC 1826**(IP Authentication Header)
	X.25	E	**RFC 1829**(IP Encapsulating Security Payload)
Network		E	**SILS** (Standards for Interoperable LAN Security)
		E	**TLSP (SP4)**(Transport Layer Security Protocol)
	ATM	E	**ISP-421/94.05.15 rev 1**(Sec Assoc Mgmt Protocol)
Data Link	**Ethernet**	E	**SDE** (Secure Data Exchange)
	FDDI	E	**SILS** (Standards for Interoperable LAN Security)
Physical	**IEEE 802.3**	E	**SP2** (Security Protocol Layer 2)
	X.25		
Media	**ATM**		No current security standards
	RF		

Notes: M is for mandated and E is for emerging.

6.4 INFORMATION MODELING AND DATA EXCHANGE SECURITY STANDARDS

The DGSA discusses the need for a separation mechanism to mediate all calls to security critical functions and ensure strict isolation is maintained. A security management information base (SMIB) will contain the description of objects that are managed by the separation mechanism. However, the object class definitions for managing critical security functions are not currently standardized. Therefore, standards identified in the two following sections are provided for information and migration planning but are NOT mandated for use.

6.4.1 Mandated Standards

None mandated at this time.

6.4.2 Emerging Standards

- ISO/IEC 10165 Series, Information Technology - Open Systems Interconnection - Structure of Management Information - Parts 1- 4, 1993 - 1994.
- DII 10164-9, SC21 N9390, Information Technology - Open Systems Interconnection - Systems Management - Part 9: Objects and Attributes for Access Control (Final Text), ISO/IEC JTC1 SC21/WG4, DII April 1993, target IS Mar. 1994 (ITU-T X.741) (strict isolation/security critical functions/elements of management information; decision and enforcement separation/separation policy representation/elements of management information; constrained dispersion/transfer system/security information objects, elements of management information; security management/systems management/elements of management information).

6.5 HUMAN-COMPUTER INTERFACE SECURITY STANDARDS

One aspect of the human-computer interface is the need to identify individual users of an end system. End systems in turn need to be able to authenticate remote entities whether they are users, other end systems, or relay systems. The standards listed below identify the existing techniques for authentication. Specific selection of a standard should be mission specific.

6.5.1 Mandated Standards

6.5.1.1 Security Banners and Screen Labels

- Department of Defense (DOD). 1994b*Department of Defense Human Computer Interface Style Guide, TAFIM* (Version 2.0), Volume 8, 30 September 1994.

6.5.2 Emerging Standards

6.5.2.1 Entity Authentication

- ISO/IEC 9798-1, 1991, Entity Authentication Mechanisms, Part 1- 4: General Model, ISO/IEC JTC1 SC27/WG2, 1991 - 1995, (strict isolation/protection mechanisms/techniques).

6.5.2.2 Personal Authentication

- WD 9798-5, SC27 N 1104 (Project 1.27.03.05), Entity Authentication Mechanisms - Part 5: Entity Authentication Using Zero Knowledge Techniques, ISO/IEC JTC1 SC27/WG2, WD, target CD 1995, DII 1996, and IS 1997.

6.6 SECURITY RELATED DOCUMENTS

While most system planners and architects look to standards to arrive at a basic set of requirements, systems security is driven by policy. Security policy appears at many levels, including federal laws (e.g., The Privacy Act) and policy for the handling of national intelligence information (e.g., Director of Central Intelligence Directive (DCID) 1/16). Such policies do not have directly associated standards, yet their compliance requirements can affect both the system and technical architectures.

For those systems required or desiring to use a cryptographic device to protect privacy act information and other, unclassified, non-Warner Act exempt information, the Data Encryption Standard (DES) may apply. The DES is found in FIPS PUB 46-2 Data Encryption Standard, December 1993.

The C2 Protect initiative addresses those measures taken to maintain effective C2 of U.S. Army forces. While there are no technical standards mandated, it does establish a library of tasks and actions necessary to implement, manage, and support the initiative.

APPENDIX A - ACRONYMS

AAL	ATM Adaptation Layer
ABOR	Abort
ACP	Allied Communication Publication
ACT	Advanced Concept and Technology
ACTD	Advanced Concept Technology Demonstration
ADDS	Army Data Distribution System
ADO	Army DigitizationOffice
AIS	Automated Information Systems
ALSP	Aggregate Level Simulation Protocol
ANSI	American National Standards Institute
API	Application Programming Interface
AR	Army Regulation
AS	Autonomous System
ASAS	All Source Analysis System
ASB	Army Science Board
ASD	Assistant Secretary of Defense
ATA	Army Technical Architecture
ATD	Advanced Technology Demonstration
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
BRI	Basic Rate Interface
BUFR	Binary Universal Format for Representation
C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
C3S	Command, Control, and Communications Systems
C4I	Command, Control, Communications, Computers, and Intelligence
C2CDM	C2 Core Data Model
CAD	Computer-Aided Design
CADRG	Compressed ARC Digitized Raster Graphics
CASE	Computer Aided Software Engineering
CBS	Commission for Basic Systems
CCITT	International Telephone and Telegraph Consultative Committee (now ITU-T)
CDE	Common Desktop Environment
CDMA	Code Division Multiple Access
CGI	Computer Generated Imagery
CGM	Computer Graphics Metafile
CIB	Controlled Image Base

CIDE	Communication Information Data Exchange
CINC	Commander-in-Chief
CIPSO	Common Internet Protocol Security Options
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CMMS	Conceptual Models of the Mission Space
CNR	Combat Net Radio
COE	Common Operating Environment
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off-the-Shelf
CSMA/CD	Carrier Sense Multiple Access / Collision Detection

DAA	Designated Approving Authority
DBMS	Database Management System
DCE	Distributed Computing Environment
DCE	Data Circuit-Terminating Equipment
DCID	Director of Central Intelligence Directive
DDDS	Defense Data Dictionary System
DDM	Defense Data Model
DDRS	Defense Data Repository System (now DDDS)
DEF	Data Exchange Format
DES	Data Encryption Standard
DGSA	DOD Goal Security Architecture
DHCP	Dynamic Host Configuration Protocol
DII	Defense Information Infrastructure
DIS	Distributed Interactive Simulation
DISA	Defense Information Systems Agency
DISC4	Director of Information Systems for Command, Control, Communications, and Computers
DISN	Defense Information Systems Network
DMA	Defense Mapping Agency
DMS	Defense Message System
DNC	Digital Nautical Chart
DNS	Domain Name System
DOD	Department of Defense
DODD	Department of Defense Directive
DPPDB	Digital Point Positioning Data Base
DSS	Digital Signature Standard
DSSS	Direct Sequence Spread Spectrum
DTE	Data Terminal Equipment
DTED	Digital Terrain Elevation Data
DTOP	Digital Topographic Data

EDI	Electronic Data Interchange

EEI	External Environment Interface
EIA	Electronics Industries Association
ESP	Encapsulating Security Payload
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standards
FOA	Field Operating Agency
FTP	File Transfer Protocol
GCCS	Global Command and Control System
GIS	Geographic Information System
GKS	Graphical Kernel System
GOA	Generic Open Architecture
GOTS	Government Off-the-Shelf
GPS	Global Positioning System
GRIB	Gridded Binary
GSM	Global System for Mobile Communications
GSS	Generic Security Service
GUI	Graphical User Interface
HCI	Human-Computer Interface
HF	High Frequency
HLA	High Level Architecture
HQDA	Headquarters Department of the Army
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
I&A	Identification & Authentication
I&RTS	Integration & Runtime Specification
IAB	Internet Architecture Board
IAW	In Accordance With
ICCCM	Inter Client Communications Convention Manual
ICD	Interface Control Document
ICMP	Internet Control Message Protocol
ICOM	Inputs, Controls, Outputs, and Mechanisms
IDEF	Integrated Computer Aided Manufacturing Definition
IDEF0	Integrated Computer Aided Manufacturing Definition Function Method
IDEF1X	Integrated Computer Aided Manufacturing Definition Extended Data Method
IDL	Interface Definition Language
IDUP	Independent Data Unit Protection
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force

IGES	Initial Graphics Exchange Specification
IGMP	Internet Group Management Protocol
IMETS	Integrated Meteorological System
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPv6	IP Next Generation/Version 6
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	ISDN Security Program
ITU	International Telecommunications Union
JCS	Joint Chiefs of Staff
JFIF	JPEG File Interchange Format
JIEO	Joint Interoperability and Engineering Organization
JPEG	Joint Picture Expert Group
JTA	Joint Technical Architecture
JTDLMP	Joint Tactical Data Link Management Plan
JTIDS	Joint Tactical Information Distribution System
kbps	kilobits per second
KEA	Key Exchange Algorithm
KMP	Key Management Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LLC	Logical Link Control
LPI	Low Probability of Intercept
LWD	Littoral Warfare Data
M&S	Modeling & Simulation
MACOM	Major Army Command
Mbits/s	Megabits per second
Mbps	Megabits per second
MCG&I	Mapping Cartographic, Geospatial & Imaging
MC&G	Mapping, Charting, and Geodesy
MDA	Milestone Decision Authority
MHS	Message Handling System
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MISSI	Multilevel Information System Security Initiative
MMP	MISSI Management Protocol
MPEG	Motion Pictures Expert Group
MSP	Message Security Protocol

NCSC	National Computer Security Center (see NSA)
NES	Network Encryption System
NIST	National Institute of Standards and Technology
NITFS	NITF Standard
NLSP	Network Layer Security Protocol
NSA	National Security Agency
RT/NRT	Real-Time/Near-Real-Time
OA	Operational Architecture
ODBC	Open Data Base Connectivity
ODISC4	Office of the Director of Information Systems for Command, Control, Communications, and Computers
ODMG	Object Data Management Group
OOA	Object Oriented Analysis
OOM	Object-oriented methods (OOM
OOP	Object OrientedProgramming
OOT	Object Oriented Technology
OOTW	Operations-Other-Than-War
ORD	Operational Requirements Document
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Services
PDU	Protocol Data Unit
PEO	Program Executive Office
PHIGS	Programmers Hierarchical Interactive Graphics System
PM	Program/Product Manager
PNNI	Private Network-Network Interface
POSIX	Portable Operating System Interface
PPP	Point-to-Point Protocol
PPS	Precise Position Service
PRI	Primary Rate Interface
PSM	Persistent Stored Modules
PSTN	Public Switched Telephone Network
PTTI	Precise Time and Time Interval
RADIUS	Remote Authentication Dial In User Service
RDT&E	Research, Development, Test & Evaluation
RFC	Request for Comment
RPC	Remote Procedure Calls
RPF	Raster Product Format

RS	Recommended Standard
SA	Systems Architecture
SAE	Society of Automotive Engineers
SAMP	Security Association Management Protocol
SDNS	Secure Data Network System
SEA	Strategic Enterprise Architecture
SEDRIS	Synthetic Environment Data Representation Interchange Specification
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SIF	Simulation Information Format
SILS	Standard for Interoperable LAN Security
SMIB	Security Management Information Base
SMT	Station Management
SNMP	Simple Network Management Protocol
SP3	Security Protocol at Layer 3
SQL	Structured Query Language
SSL	Secure Sockets Layer (of HTTP)
STAMIS	Standard Army Management Information System
STD	Standard
STOU	Store Unique
STRICOM	Space and Strategic Defense Command
SUS	Single UNIX Specification
TA	Technical Architecture
TAFIM	Technical Architecture Framework for Information Management
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TEED	Tactical End-to-End Encryption Device
TELNET	Telecommunications Network
TFTP	Trivial File Transfer Protocol
TIDP	Technical Interface Design Plan
TIDP-TE	Technical Interface Design Plan - Test Edition
TOS	Type-of-Service
TRM	Technical Reference Model
TSIG	Trusted Systems Interoperability Group
TSIX(RE)	Trusted Information Exchange for Restricted Environments
UAV	Unmanned Aerial Vehicle
UCS	Universal Multiple-Octet Coded Character Set
UDP	User Datagram Protocol
UFD	User Functional Description
UNI	User-Network Interface
URL	Uniform Resource Locator

USMC	United States Marine Corps
USMTF	United States Message Text Format
UVMap	Urban Vector Map
VMap AD	VMap Aeronautical Data
VITD	Vector Interim Terrain Data
VMap	Vector Map
VMF	Variable Message Format
VPF	Vector Product Format
VTC	Video Teleconferencing
WGS-84	World Geodetic System 84
WMO	World Meteorological Organization
WSHCI	Weapon Systems Human-Computer Interface
WSTAWG	Weapon System Technical Architecture Working Group
WVS+	World Vector Shoreline Plus
WWW	World Wide Web

This page was intentionally left blank.

APPENDIX B - LIST OF REFERENCES

B.1 MILITARY

B.1.1 DOD References

CJCSI 3900.01, Position Reference Procedures

DOD 5200.28-STD, DOD Trusted Computer System Evaluation Criteria (Orange Book), December 1985

DOD 8320.1-M-1, Department of Defense Data Element Standardization Procedures, January 1993

DOD Directive 3405.1, Computer Programming Language Policy, 2 April 1987

DOD Directive 8320.1, DOD Data Administration, September 1991

ICD-GPS-060, Precise Time and Time Interval (PTTI) Interface, Rev A

ICD-GPS-153, GPS User Equipment Radio Receivers (Draft)

ICD-GPS-155, GPS Receiver Application Module Interface, Parallel Dual Port Interface (Draft)

MD4000501-1.52, FORTEZZA Cryptologic Interface Programmer's Guide, 30 January 1996

MD4002101-1.52, FORTEZZA Application Implementor's Guide, 5 March 1996

MIL-D-89020, Digital Terrain Elevation Data (DTED)

MIL-HDBK-1300A, National Imagery Transmission Format Standard (NITFS)

MIL-PRF-28000A, Initial Graphics Exchange Specification (IGES)

MIL-STD-188-196, Bi-Level Image Compression

MIL-STD-188-198A, Joint Photographic Experts Group (JPEG) Image Compression for the National Imagery Transmission Format Standard, 15 December 1993

MIL-STD-188-199, Vector Quantization Decompression

MIL-STD-188-220A, Interoperability Standard for Digital Message Transfer Device Subsystem

MIL-STD-1477B, Symbols for Army Air Defense System Displays, 30 September 1993

MIL-STD-2045-47001, Interoperability Standard For Connectionless Data Transfer Application Layer Standard

MIL-STD-2045-48501, Common Security Labeling, 25 January 1995

MIL-STD-2301, Computer Graphics Metafile (CGM) Implementation Standard for the National Imagery Transmission Format Standard, 18 June 1993

MIL-STD-2401, World Geodetic System 84 (WGS-84), 21 March 1994

MIL-STD-2407, Vector Product Format (VPF)

MIL-STD-2411, Raster Product Format (RPF)

MIL-STD-2500A, National Imagery Transmission Format (NITF), Version 2.0

MIL-STD-2525A, Common Warfighting Symbology, Draft

MIL-STD-6040, US Message Text Format (USMTF) Electronic Document System, CDU95V01, 1 October 1995 (formerly Joint Pub 6-04)

NCSC-TG-005, Trusted Network Interpretation, 31 July 1987

NCSC-TG-021, Version-1, Trusted Database Management System Interpretation, April 1991

STANAG 5516, Edition 1, Tactical Data Exchange - LINK 16, Ratified 2 March 1990

(No Number) Assistant Secretary of Defense Memorandum, Delegations of Authority and Clarifing Guidance on Waivers from the Use of the Ada Programming Language

(No Number) ASD Memorandum, Development, Procurement, and Employment of DoD Global Position System User Equipment, 30 April 1992

(No Number) Department of Defense Joint Technical Architecture (JTA), Version 1.0, 22 August 1996

(No Number) DII COE Version 2.0 Baseline Specification, 28 June 1996

(No Number) DII COE Integration and Runtime Specification (I&RTS), Version 2.0, 23 October 1995

(No Number) DOD Memorandum, Subject: Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement, 13 October 1993

(No Number) DOD Memorandum, Subject: Specifications & Standards -- A New Way of Doing Business, 29 June 1994

(No Number) DOD Technical Architecture Framework for Information Management (TAFIM), Volume 2: Technical Reference Model Version 2.0, Defense Information Systems Agency Center for Standards, 30 September 1994

(No Number) DOD Technical Architecture Framework for Information Management (TAFIM), Volume 6: DOD Goal Security Architecture (DGSA), Version 2.0, Defense Information Systems Agency Center for Standards, 30 September 1994

(No Number) DOD Technical Architecture Framework for Information Management (TAFIM), Volume 8: Department of Defense HCI Style Guide Version 2.0, Defense Information Systems Agency Center for Standards, 30 September 1994

(No Number) FORTEZZA Crypto Card Interface Control Document, Revision P1.5, 22 December 1994, FOUO

(No Number) FORTEZZA Plus Crypto Card Interface Control Document, Release 3.0, 1 June 1995, FOUO

(No Number) Interface Specification Version 1.0, (M&S HLA), 15 September 1996

(No Number) Joint Tactical Data Link Management Plan (JTDLMP), April 1996

(No Number) Joint VMF Technical Interface Design Plan (TIDP)

(No Number) JTIDS Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 3 August 1994

(No Number) Joint Tactical Information Distribution System (JTIDS) Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 3 August 1994

(No Number) M&S HLA Rules Version 1.0, 15 September 1996

(No Number) Object Model Template Version 1.0, (M&S HLA), 15 September 1996

(No Number) The Under Secretary of Defense for Acquisition and Technology, DOD High Level Architecture (HLA) for Simulations, 10 September 1996

(No Number) User Interface Specifications for the Defense Information Infrastructure (DII), Version 2.0, 1 April 1996

B.1.2 Army References

ACCS-A3-407-008D, Interface Specification for the Army Data Distribution System (ADDS) Interface

AR 380-19, Army Regulation, Information Systems Security, 1 August 1990

HQDA LTR 25-92-1, Implementation of the Ada Programming Language

HQDA LTR 25-94-1, Implementation of the Ada Programming Language

HQDA LTR 25-95-1, Implementation of the Ada Programming Language

FM 101-5-1, Operational Terms and Graphics

(No Number) Army Technical Architecture Implementation, Mark-On-The-Wall Message, Department of the Army, 6 June 1996

(No Number) Command and Control (C2) Core Data Model, Version 2, Defense Information Systems Agency, 1 July 1994

(No Number) Department of the Army C4I Technical Architecture, Version 3.1, 31 March 1995

(No Number) Department of the Army Technical Architecture, Version 4.0, 30 January 1996

(No Number) HQDA Memorandum, Subject: 1994 Army Science Board Study: Technical Architecture for Army C4I, 28 July 1994

(No Number) The Army Enterprise Implementation Plan, 8 August 1994

(No Number) The Army Enterprise Strategy, the Vision, 20 July 1993

(No Number) U.S. Army Weapon Systems Human-Computer Interface (WSHCI) Style Guide, September 1996

B.1.3 Other Government Agency References

ACP 123 U.S. Supplement No. 1, Common Messaging Strategy and Procedures, November 1995

DCID 1/16, Director of Central Intelligence Directive

FIPS Pub 46-2, Data Encryption Standard, December 1993

FIPS Pub 120-1, Graphical Kernel System (GKS) (Change Notice 1)

FIPS Pub 127-2, Database Language - SQL

FIPS Pub 128-1, Computer Graphics Metafile (CGM)

FIPS Pub 152, Standard Generalized Markup Language (SGML)

FIPS Pub 153, Programmers Hierarchical Interactive Graphics Systems (PHIGS)

FIPS Pub 158-1, X Window System, Version 11, Release 5, October 1993

FIPS Pub 161-1, Electronic Data Interchange (EDI)

FIPS Pub 180-1, National Institute of Standards and Technology (NIST) Secure Hash Algorithm (SHA), April 1995

FIPS Pub 183, Integration Definition for Function Modeling (IDEF0), December 1993

FIPS Pub 184, Integration Definition for Data Modeling (IDEF1X), December 1993

FIPS Pub 185, NIST Escrowed Encryption Standard, February 1994

FIPS Pub 186, NIST Digital Signature Standard (DSS) Algorithm, May 1994

FIPS Pub 189-1

FIPS Pub 196, Entity Authentication Using Public Key Cryptography, 16 September 1996.

NISTIR 90-4250, Network Transport and Message Security Protocol (Report)

R21-Tech-23-94, NSA-developed Type II Key Exchange Algorithm (KEA), 12 July 1994

(No Number) National Security Agency (NSA)-developed Type II confidentiality algorithm (SKIPJACK)

B.2 COMMERCIAL REFERENCES

ANSI J-STD-008, Personal Station - Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum PCS System, Draft

ANSI T1.630, ATM Adaption Layer for Constant Bit Rate Services Functionality and Specification, 1993

ANSI T1.635, ATM Adaptation Layer Type 5, Common Part Functions and Specification, 1994

ANSI X3.100, Interface between DTE and DCE for Operation with PSDN, or between Two DTEs, by Dedicated Circuit, 1989

ANSI X3.229, Fiber Distribution Data Interface (FDDI) - Station Management (SMT)

ANSI/ISO 8632: 1992, Computer Graphics Metafile (CGM)

DIS 9075-4, Database Language SQL, Part 4: Persistent Stored Modules (SQL/PSM) (Draft)

EIA 232E, Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, July 1991

EIA 449, General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, February 1980

EIA 530A, High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment, June 1992, Including Alternate 26-Position Connector, 1992

EIA/TIA/IS-41-C, Cellular Radiotelecommunications Intersystem Operations

ESD-TR-86-278, Guidelines for Designing User Interface Software, Smith and Mosier, 1986

FM 92-X-GRIB, The WMO Format for the Storage of Weather Product Information and the Exchange of Weather Product Messages in Gridded Binary (GRIB) Form

FM 94-X-BUFR, The WMO Binary Universal Format for Representation (BUFR)

IDUP-GSS-API, Independent Data Unit Protection Generic Security Service Application Program Interface, 13 June 1996

IEEE 610.12, Software Engineering Terminology, 30 March 1990

IEEE 802.2, Local and Metropolitan Area Networks, Part 2: Logical Link Control, 1994

IEEE 802.3, Local and Metropolitan Area Networks, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 1993

IEEE 802.3u, Local and Metropolitan Area Networks, Part 3: CSMA/CD Access Method and Physical Layer Specifications, 1995

IEEE 802.10, Local and Metropolitan Area Networks, Part 10: Interoperable LAN/MAN Security (SILS), 1992

IEEE 802.10a, Standard for Interoperable LAN Security-The Model, (Draft) Jan 1989

IEEE 802.10b, Standard for Interoperable LAN Security-Part B: Secure Data Exchange, 1992

IEEE 802.10c/D6, Standard for Interoperable LAN Security-Part C: Key Management, (Draft), 1994

IEEE 1003.1, Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) (ISO 9945-1)

IEEE 1003.2, POSIX: Shell and Utilities

IEEE 1003.2d, POSIX: Shell and Utilities - Batch Environment

IEEE 1003.5:1992, POSIX: Ada Language Interfaces Part 1: Binding for System API

IEEE 1003.5b, POSIX (Draft)

IEEE 1278.1, DIS Application Protocols, 1995

IEEE 1278.2, DIS Communication Services and Profiles, 1995

IEEE 1278.3, DIS Exercise Management and Feedback, 1995

IEEE P1003.1e, POSIX-Part 1: System API-Protection, Audit and Control Interfaces (C language), Draft 15

IEEE P1003.2c, POSIX-Part 2: Shells and Utilities-Protection and Control Interfaces, Draft 15

ISO 7498-2, Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, 1989

ISO 7776, Data Communication High-Level Data Link Control Procedures - Description of the X.25 LAPB-compatible DTE Data Link Procedures, 1986

ISO 8208, Data Communications - X.25 Packet Layer Protocol for Data Terminating Equipment, 1989

ISO 8652, Ada Reference Manual, Language and Standard Libraries, 15 February 1995

ISO 9314-1, Fibre Distributed Data Interface (FDDI) - Pt 1: Token Ring Physical Layer Protocol (PHY)

ISO 9314-2, Fibre Distributed Data Interface (FDDI) - Pt 2: Token Ring Media Access Control (MAC)

ISO 9314-3, Fibre Distributed Data Interface (FDDI) - Pt 3: Physical Layer Medium Dependent (PMD)

ISO 10918-1: 1994, Joint Picture Expert Group (JPEG)

ISO 11172, Coding of Moving Pictures and Associated Audio for Digital Storage Media up to 1.5 Mbps

ISO 11172-1, Motion Pictures Expert Group (MPEG), Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 1: Systems

ISO 13818-1: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 1: Systems

ISO 13818-2: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 2: Video

ISO/IEC 8859-1:1987, Information Processing - 8-Bit Single-Byte Coded Character Sets - Part 1: Latin Alphabet No. 1

ISO/IEC 9075-3: 1995, Call Level Interface (Draft)

ISO/IEC 9596-1, 1991, Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) - Part 1: Specification (ITU-T X.711), 1991

ISO/IEC 9636, Information Technology-Computer Computer Graphics-Interfacing Techniques for Dialogue with Graphics Devices (CGI)

ISO/IEC 9798-1, 1991 Entity Authentication Mechanisms, Part 1- 4: General Model, 1991-1995

ISO/IEC 10021-1 1990/DAM 4, Information Technology-Message Handling Systems (MHS) - Part 1: System and Service Overview - Amendment 4: Interpersonal Messaging Security Extensions,ISO/IEC JTC1 SC18/WG4, IS (ITU-T X.400), 1990

ISO/IEC 10164-7, Information Technology - Open System Interconnection - Systems Management - Part 7: Security Alarm Reporting Function, ISO/IEC JTC1 SC21/WG4, IS May 1992 (ITU-T X.736, 1992)

ISO/IEC 10165, Open Systems Interconnection - Structure of Management Information - Parts 1- 4, 1993 - 1994

ISO/IEC 10646-1: 1993, Information Technology - Universal Multiple-Octet Coded Character Set (UCS), Part 1: Architecture and Basic Multilingual Plane

ISO/IEC 11172-1: 1993/Cor. 1:1995 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 1: Systems Technical Corrigendum 1

ISO/IEC 11172-2: 1993 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 2 Video

ISP-421/94.05.15 Revision 1.0, The ISDN Security Program (ISP) Security Association Management Protocol (SAMP)

ITU H.320, Narrow-Band Visual Telephone Systems and Terminal Equipment, 1996

ITU H.323, Visual Telephone Systems and Equipment for Local Area Networks Which Provide a Non-Guaranteed Quality of Service (Draft)

ITU I.430, Basic User-Network Interface - Layer 1 Specification, 1995

ITU I.431, Primary Rate User-Network Interface - Layer 1 Specification, 1993

ITU Q.921, ISDN User-Network Interface - Data Link Layer Specification, 1993

ITU Q.931, ISDN User-Network Interface - Layer 3 Specification for Basic Call Control, 1993

ITU-T X.25, Interface Between DTE and DCE for Terminals Operating in the Packet Mode on Public Data Networks

ITU-T H.324, Terminal for Low Bit Rate Multimedia Communications, 19 March 1996

ITU-T X.500, The Directory - Overview of Concepts, Models, and Services - Data Communication Networks Directory, 1993 (ISO/IEC 9594-1)

ITU-T X.509, The Directory: Authentication Framework, Version 3, 1993 (ISO/IEC 9594-8.2)

ODBC 2.0, Open Data Base Connectivity

OSF 1992, Open Software Foundation (OSF)/Motif Style Guide, Revision 1.2

RFC-951, Bootstrap Protocol, September 1985

RFC-1332, The PPP Internet Protocol Control Protocol (IPCP), May 1992

RFC-1333, PPP Link Quality Monitoring, May 1992

RFC-1334, PPP Authentication Protocols, October 1992

RFC-1356, Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode, August 1992

RFC-1508, Generic Security Service Application Program Interface (GSS-API), September 1993

RFC-1510, The Kerberos Network Authentication Service, V.5, September 1993

RFC-1533, DHCP Options and BOOTP Vendor Extensions, October 1993

RFC-1541, Dynamic Host Configuration Protocol, October 1993

RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, October 1993

RFC-1570, PPP LCP Extensions, January 1994

RFC-1577, Classical IP and ARP over ATM, January 1994

RFC-1583, OSPF Version 2, March 1994

RFC-1584, Multicast Extensions to OSPF, March 1994

RFC-1618, PPP over ISDN, May 1994

RFC-1738, Uniform Resource Locators (URL), December 1994

RFC-1771, A Border Gateway Protocol 4 (BGP-4), March 1995

RFC-1772, Application of the Border Gateway Protocol in the Internet, March 1995

RFC-1808, Relative Uniform Resource Locators, June 1995

RFC-1812, Requirements for IP Version 4 Routers, June 1995

RFC-1825, Security Architecture for the Internet Protocol, August 1995

RFC-1826, IP Authentication Header, August 1995

RFC-1827, IP Encapsulating Security Payload (ESP), August 1995

RFC-1828, IP Authentication using Keyed MD5, August 1995

RFC-1829, The ESP DES-CBC Transform, August 1995

RFC-1866, HyperText Mark-up Language (HTML), Version 2.0, 1995

RFC-1883, Internet Protocol, Version 6 (IPv6) Specification, January 1996

RFC-1884, IP Version 6 Addressing Architecture, January 1996

RFC-1885, Internet Control Message Protocol (ICMPv6) for IPv6, January 1996

RFC-1886, DNS Extensions to support IP Version 6, January 1996

RFC-1945, HyperText Transfer Protocol -- HTTP/1.0, May 1996

RS-232-D, Interface Between DTE and DCE Employing Serial Binary Data Interchange, June 1981

RS-449, General Purpose 37-Position and 9-Position Interface for DTE and DCE Employing Serial Binary Data Interchange, November 1987

RS-530, High-Speed 25-Position Interface for DTE and DCE

SAE AS4893, Generic Open Architecture (GOA) Framework, Society of Automotive Engineers (SAE)

SDN.703, MISSI Management Protocol (MMP), Revision 1.0, 7 June 1996

STD-3, Host Requirements, October 1989 (Also RFC-1122, RFC-1123)

STD-5, Internet Protocol, September 1981 (Also RFC-791, RFC-950, RFC-919, RFC-922, RFC-792, RFC-1112)

STD-6, User Datagram Protocol, August 1980 (Also RFC-768)

STD-7, Transmission Control Protocol, September 1981 (Also RFC-793)

STD-8, Telnet Protocol, May 1983 (Also RFC-854, RFC-855)

STD-9, File Transfer Protocol, October 1985 (Also RFC-959)

STD-13, Domain Name System, November 1987 (Also RFC-1034, RFC-1035)

STD-15, Simple Network Management Protocol, May 1990 (Also RFC-1157)

STD-16, Structure of Management Information, May 1990 (Also RFC-1155, RFC-1212)

STD-17, Management Information Base, March 1991 (Also RFC-1213)

STD-33, Trivial File Transfer Protocol, July 1992 (Also RFC-1350)

STD-35, ISO Transport Service on top of the TCP (Version 3), May 1978 (Also RFC-1006)

STD-36, Transmission of IP and ARP over FDDI Networks, January 1993 (Also RFC-1390)

STD-37, An Ethernet Address Resolution Protocol, November 1982 (Also RFC-826)

STD-41, Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984 (Also RFC-894)

STD-51, The Point-to-Point Protocol (PPP), July 1994 (Also RFC-1661, RFC-1662)

TIA/EIA/IS-95-A, Mobile Station - Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System

WD 9798-5, SC27 N 1104 (Project 1.27.03.05), Entity Authentication Mechanisms - Part 5: Entity Authentication Using Zero Knowledge Techniques, ISO/IEC JTC1 SC27/WG2, WD, target CD 1995, DII 1996, and IS 1997

WMO No. 306, Manual for Codes, Volume 1, Part B, Binary Codes

X/Open C309, DCE Remote Procedure Call

X/Open C310, DCE Time Services

X/Open C312, DCE Directory Services

X/Open C323, Common Desktop Environment (CDE) Version 1.0, April 1995

X/Open P315, DCE Authentication and Security Specification (Draft)

VTC001, Industry Video Teleconferencing Profile, Corporation for Open Systems (COS), Revision 1, April 1995

(No Number) ATM Forum 25.6 Mb/s over Twisted Pair Cable Physical Interface

(No Number) ATM Forum Local Area Network (LAN) Emulation over ATM, Version 1.0, af-lane-0021.000, August 1996

(No Number) ATM Forum Private Network-Network Interface (PNNI) Specification, Version 1, WP 510-1728WC-B, 1 August 1995

(No Number) ATM Forum User-Network Interface (UNI) Specification, Version 3.1, September 1994

(No Number) Common Object Request Broker Architecture (CORBA) 2.0 (Draft)

(No Number) IP Mobility Support

(No Number) JPEG File Interchange Format (JFIF), Version 1.02

(No Number) Open Software Foundation (OSF)/MotifTM Style Guide, Revision 1.2, 1992

(No Number) OSF/Motif Inter Client Communications Convention Manual (ICCCM)

(No Number) Remote Authentication Dial In User Service (RADIUS), July 1996 (Draft)

(No Number) Secure Sockets Layer (SSL) Protocol, Version 3.0, draft-freier-ssl-version3-01.txt, 13 March 1996 (Draft)

(No Number) TAWDS/Integrated Meteorological System (IMETS) Implementation Document for Communication Information Data Exchange (CIDE), Data Exchange Format (DEF) - Appendix 30

(No Number) The Windows Interface: An Application Design Guide, Microsoft Press, 1992

(No Number) Trusted Systems Interoperability Group (TSIG) Trusted Information Exchange for Restricted Environments (TSIX(RE)) 1.1 (draft)

(No Number) Win32 APIs, Microsoft Win32 Programmers Reference Manual, Volumes 1-5, Microsoft Press, January 1993

(No Number) Win32 APIs, Window Management and Graphics Device Interface, Volume 1, Microsoft Win32 Programmers Reference Manual, Microsoft Press, 1993

(No Number) X/Open Single UNIX Specification (SUS)

This page was intentionally left blank.

APPENDIX C - GLOSSARY

Access control

Process of limiting access to the resources of an IT product only to authorized users, programs, processes, systems, or other IT products.

Accreditation

The managerial authorization and approval, granted to an ADP system or network to process sensitive data in an operational environment, made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements, e.g., TCSEC, for achieving adequate data security. Management can accredit a system to operate at a higher/lower level than the risk level recommended (e.g., by the Requirements Guideline-) for the certification level of the system. If management accredits the system to operate at a higher level than is appropriate for the certification level, management is accepting the additional risk incurred.

Application Platform Entity

The application platform is defined as the set of resources that support the services on which application software will execute. It provides services at its interfaces that, as much as possible, make the implementation-specific characteristics of the platform transparent to the application software. (TAFIM, Version 2.0, Volume 2)

Application Program Interface (API)

The interface, or set of functions, between the application software and the application platform. (NIST Special Report, APP)

Application Software Entity

Mission-area and support applications. A common set of support applications forms the basis for the development of mission-area applications. Mission-area should be designed and developed to access this set of common support applications. Applications access the Application Platform via a standard set of APIs. (TAFIM, Version 2.0, Volume 2)

Architecture

An architecture is defined as the structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time. (IEEE 610.12)

An architecture is a composition of (1) components (including humans) with their functionality defined (Technical), (2) requirements that have been configured to achieve a prescribed purpose or mission (Operational), and (3) their connectivity with the information flow defined (System). (OS-JTF)

Authentication

(1) To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

(2) To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

Character-based interface

A non-bit mapped user interface in which the primary form of interaction between the user and system is through text.

Commercial Item

1) Any item customarily used by the general public for other than governmental purposes, that has been sold, leased, or licensed to the general public, or that has been offered for sale, lease or license to the general public.

2) Any item that evolved from an item described in 1) above through advances in technology or performance that is not yet available in the commercial market, but will be available in time to meet the delivery requirements of the solicitation.

3) Any item that, but for modifications of a type customarily available in the commercial market or minor modifications made to meet DOD requirements, would satisfy the criteria in 1) or 2) above.

4) Any combination of items meeting the requirements of 1, 2, or 3 above or 5 below that are of a type customarily combined and sold in combination to the general public.

5) Installation services, maintenance services, repair services, training services, and other services if such services are procured for support of any item referred to paragraphs 1, 2, 3. or 4 above, if the sources of such services

- offers such services to the general public and the DOD simultaneously and under similar terms and conditions and

- offers to use the same work force for providing the DOD with such services as the source used for providing such services to the general public.

6) Services offered and sold competitively, in substantial quantities, in the commercial marketplace based on established catalog prices of specific tasks performed and under standard commercial terms and conditions.

7) Any item, combination of items or service referred to in 1 through 6 above notwithstanding the fact that the item or service is transferred between or among separate divisions, subsidiaries, or affiliates of a contractor.

8) A nondevelopmental item developed exclusively at private expense and sold in substantial quantities, on a competitive basis, to State and local governments.

(DRAFT 6/30/95 NDI HANDBOOK/ Federal Acquisition Streamlining Act of 1994 DOD 5000.37H)

Commercial-off-the-shelf (COTS)

See the definition of Commercial Item found above. (OS-JTF 1995)

Compliance

Compliance is enumerated in an implementation/migration plan. A system is compliant with the ATA if it meets, or is implementing an approved plan to meet, all applicable ATA mandates.

Data Integrity

(1) The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

(2) The property that data has not been exposed to accidental or malicious alteration or destruction.

Domain

A distinct functional area that can be supported by a family of systems with similar requirements and capabilities. An area of common operational and functional requirements.

External Environment Interface (EEI)

The interface that supports information transfer between the application platform and the external environment. (NIST Special Report, APP)

Graphical User Interface (GUI)

System design that allows the user to effect commands, enter into transaction sequences, and receive displayed information through graphical representations of objects (menus, screens, buttons, etc.).

Human-Computer Interface (HCI)

Hardware and software allowing information exchange between the user and the computer.

Hybrid Graphical User Interface

A GUI that is composed of toolkit components from more than one user interface style.

Integration

Two or more software applications that must run on the same physical processor(s) and under the same operating system.

Interoperability

(1) The ability of two or more systems or components to exchange data and use information. (IEEE STD 610.12)

(2) The ability of two or more systems to exchange information and to mutually use the information that has been exchanged. (Army Science Board)

Market Acceptance

Means that an item has been accepted in the market as evidenced by annual sales, length of time available for sale, and after-sale support capability. (DRAFT 6/30/95 NDI HANDBOOK/ Federal Acquisition Streamlining Act of 1994 DOD 5000.37H)

Motif

User interface design approach based upon the "look and feel" presented in the OSF/MotifTM style guide. MotifTM is marketed by the Open Software Foundation.

Non Developmental Item (NDI)

1) Any commercial item.

2) Any previously developed item in use by a US Federal, State or Local government agency or a foreign government with which the US has a mutual defense cooperation agreement.

3) Any item described in subparagraph 1 or 2, above, that requires only minor modification in order to meet the requirements of the procuring agency.

4) Any item currently being produced that does not meet the requirement of paragraphs 1, 2, or 3 above, solely because the item is not yet in use.

(DRAFT 6/30/95 NDI HANDBOOK/ Federal Acquisition Streamlining Act of 1994 DOD 5000.37H)

Open Software Foundation (OSF)

Consortium of computer hardware and software manufacturers whose membership includes over seventy of the computer industry's leading companies.

Open System

A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered components to be utilized across a wide range of systems with minimal changes, to interoperate with other components on local and remote systems, and to interact with users in a style that facilitates portability. An open system is characterized by the following:

- Well defined, widely used, non-proprietary interfaces/protocols, and

- Use of standards which are developed/adopted by industrially recognized standards bodies, and

-Definition of all aspects of system interfaces to facilitate new or additional systems capabilities for a wide range of applications, and

- Explicit provision for expansion or upgrading through the incorporation of additional or higher performance elements with minimal impact on the system.

(IEEE POSIX 1003.0/D15 as modified by the Tri-Service Open Systems Architecture Working Group)

Open Systems Approach

An open systems approach is a business approach that emphasizes commercially supported practices, products, specifications and standards. The approach defines, documents, and maintains a system technical architecture that depicts the lowest level of system configuration control. This architecture clearly identifies all the performance characteristics of the system including those that will be accomplished with an implementation that references open standards and specifications. (OS-JTF)

Operational Architecture (OA)

An Operational Architectureis a description (often graphical) of the operational elements, assigned tasks, and information flows required to support the warfighter. It defines the type of information, the frequency of the exchange, and what tasks are supported by these information exchanges. (JTA 1.0)

Portability

The ease with which a system, component, data, or user can be transferred from one hardware or software environment to another. (TAFIM, Version 2.0, Volume 1/3)

Real Time

Real time is a mode of operation. Real Time systems require events, data, and information to be available in time for the system to perform its required course of action. Real Time operation is characterized by scheduled event, data, and information meeting their acceptable arrival times. (OS-JTF)

Real Time Systems

Systems which provide a deterministic response to asynchronous inputs. (OS-JTF)

Reference Model

A reference model is a generally accepted abstract representation that allows users to focus on establishing definitions, building common understandings and identifying issues for resolution. For Warfare and Warfare Support System (WWSS) acquisitions, a reference model is necessary to establish a context for understanding how the disparate technologies and standards required to implement WWSS relate to each other. Reference modules provide a mechanism for identifying key issues associated with portability, scalability, and interoperability. Most importantly reference modules will aid in the evaluation and analysis of domain specific architectures. (TRI-SERVICE Open Systems Architecture Working Group)

Scalability

The capability to adapt hardware or software to accommodate changing work loads. (OS-JTF)

Security

(1) The combination of confidentiality, integrity, and availability.

(2) The quality or state of being protected from uncontrolled losses or effects. Note: Absolute security may in practice be impossible to reach; thus the security "quality" could be relative. Within state models of security systems, security is a specific "state" that is to be preserved under various operations.

Standard

A document that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. Standards may also establish requirements for selection, application, and design criteria of material. (DOD 4120.3-M)

Standards based architecture

Is an architecture based on an acceptable set of standards governing the arrangement, interaction, and interdependence of the parts or elements that together may be used to form a weapons systems, and whose purpose is to insure that a conformant system satisfies a specified set of requirements. (OS-JTF)

System

(1) People, machines and methods organized to accomplish a set of specific functions. (FIPS 11-3)

(2) An integrated composite of people, products, and processes that provides a capability or satisfy a stated need or objective. (DOD 5000.2)

(3) In the ATA, the term "system" refers to those items that produce, use or exchange information.

(4) Systems of systems such as ASAS or AFATDS are NOT considered monolithic systems for ATA compliance. For example, targeting and fire direction data passed to the fire direction center may come from outside the local system and travel over common data networks, and therefore compliance with the ATA is an important design consideration.

Systems Architecture (SA)

A Systems Architectureis a description, including graphics, of the systems and interconnections providing for or supporting a warfighting function. The SA defines the physical connection, location, and identification of the key nodes, circuits, networks, warfighting platforms, etc., and allocates system and component performance parameters. It is constructed to satisfy Operational Architecture requirements in the standards defined in the Technical Architecture. The SA shows how multiple systems within a domain or an operational scenario link and interoperate, and may describe the internal construction or operations of particular systems in the SA. (JTA 1.0)

Technical Architecture (TA)

A Technical Architecture is the minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The technical architecture identifies the services, interfaces, standards, and their relationships. It provides the technical guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed. (JTA 1.0)

Technical Reference Model (TRM)

A target framework and profile of standards for the DOD computing and communications infrastructure. (TAFIM, Version 2.0, Vol. 1/OS-JTF)

Weapons System

A combination of one or more weapons with all related equipment, materials, services, personnel and means of delivery and deployment (if applicable) required for self sufficiency. (JCS Pub 1-02)

This page was intentionally left blank.

APPENDIX D - SUSTAINING BASE/OFFICE AUTOMATION DOMAIN EXCEPTIONS AND EXTENSIONS

D.1 DOMAIN DESCRIPTION

The Sustaining Base/Office Automation Domain consists of automated systems that perform service support, business and office automation functions.

D.2 INFORMATION PROCESSING STANDARDS

D.2.1 Mandates

User Interface Services

This domain shall develop or acquire applications that follow the following user interface services:

- Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993, Microsoft Press.

Data Management Services

This domain shall develop or acquire client applications that follow the following data management services.

- Open Data Base Connectivity (ODBC), ODBC 2.0: Provides standard call level APIs between database application clients and the database server.

Operating System Services

This domain shall develop or acquire applications that follow the following operating system services:

- Win32 APIs, Microsoft Win32 Programmers Reference Manual, Volumes 1-5, 1993, Microsoft Press.

D.2.2 Emerging Standards

Within the Software Engineering Services, it is expected that publicly available Ada 95 bindings to Win32 APIs will be adopted.

D.3 INFORMATION TRANSFER STANDARDS

There are no exceptions or extensions to the standards in the main body of the ATA.

D.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS

There are no exceptions or extensions to the standards in the main body of the ATA.

D.5 HUMAN-COMPUTER INTERFACES

D.5.1 Mandates

D.5.1.1 Exceptions

There are no exceptions to the standards in the main body of the ATA.

D.5.1.2 Extensions

The following commercial HCI style guide is an extension to the mandates for this domain.

- The WindowsTM Interface: An Application Design Guide, Microsoft Press, 1992.

D.5.2 Emerging Standards

There are no exceptions or extensions to the standards in the main body of the ATA.

D.6 INFORMATION SECURITY

There are no exceptions or extensions to the standards in the main body of the ATA.

APPENDIX E - C3I DOMAIN EXCEPTIONS AND EXTENSIONS

E.1 DOMAIN DESCRIPTION

The C3I Domain consists of command and control, communications, intelligence, and electronic warfare systems.

E.2 INFORMATION PROCESSING STANDARDS

E.2.1 Mandates

There are no exceptions or extensions to the standards in the main body of the ATA.

E.2.2 Emerging Standards

There are no exceptions or extensions to the standards in the main body of the ATA.

E.3 INFORMATION TRANSFER STANDARDS

There are no exceptions or extensions to the standards in the main body of the ATA.

E.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS

There are no exceptions or extensions to the standards in the main body of the ATA.

E.5 HUMAN-COMPUTER INTERFACES

The *User Interface Specifications for the Defense Information Infrastructure* defines the appearance and behavior of the user interface for DII applications and has been adopted as the domain-level style guide/specification for C3I systems within the Army. This document adopts X Windows, Motif and CDE and supplements the basic guidelines set forth in the *DOD HCI Style Guide*.

E.6 INFORMATION SECURITY

There are no exceptions or extensions to the standards in the main body of the ATA.

This page was intentionally left blank.

APPENDIX F - WEAPONS SYSTEM DOMAIN EXCEPTIONS AND EXTENSIONS

F.1 THE WEAPONS SYSTEM DOMAIN

Weapons systems communicate and receive information in support of their warfighting users. Weapons systems provide Command and Control capabilities that require gathering, processing, and communicating data to the warfighter. The systems need to be deterministic, having a real-time response to the mission critical data that requires a specific action or reaction. Weapons systems are designed to support the warfighter with the primary focus on lethality, survivability, and battle management. Weapons systems are also sensors which gather data for the larger seamless architecture, therefore they too must interact and interoperate.

The Weapon System Technical Architecture Working Group (WSTAWG) was formed in response to an ADO/Director of Information Systems for Command, Control, Communications, and Computers (DISC4) meeting that determined weapons systems should be included in the Technical Architecture effort. The WSTAWG group is comprised of representatives from the Army Program Executive Offices, Program Managers Army Research and Development Centers, and others who are engaged in building weapons systems. The WSTAWG discussed the military, proprietary, and commercial standards, that they employ in their current system designs and briefed the results of their effort to the Army Digitization Office, Army Science Board, and Army System Engineering Office. The WSTAWG concluded that there was a need for additional domain analysis to help identify additional standards that would allow specific weapons system domains to share products, processes, and services.

The focus of the WSTAWG, for this revision of the ATA, concentrated only on interoperability standards and specifications that interface weapons systems to C4I systems and to other weapons systems. The goal remains to reduce the unit cost, life cycle cost, and deployment cost of today's weapons by incorporating Army Technical Architecture standards into designs for new and already fielded weapons systems.

Weapons systems operate in many different environments around the world. The systems include physical restrictions of size, weight, and power. Weapons systems must also meet specific performance requirements based on the mission of the platform. To this end, one standard does not fit all of the many sizes and shapes of today's Army weapons systems. As an example: operational, technical, and physical constraints associated with embedded weapons systems may not permit the use of the DII COE as currently defined. Therefore, the WSTAWG is currently exploring and identifying an extension of the DII COE for the weapons system domain. This domain specific COE implementation will allow the development of application software which can then be offered up for reuse to other systems within the weapons system domain and to other domains.

The WSTAWG is committed to its work on domain analysis to identify standards that provide a common form, fit, and function across platforms of a similar domain

(Interoperability and Intra-operability). When these standards are identified and agreed to, the WSTAWG will submit them through the Army Technical Architecture configuration management process for inclusion in the next revision.

F.2 INFORMATION PROCESSING STANDARDS

F.2.1 Mandates

F.2.1.1 Exceptions

Graphic Services

The standard that applies to this domain is:

- ISO/IEC 9636, Information Technology-Computer Graphics-Interfacing Techniques for Dialogue with Graphics Devices (CGI).

F.2.2 Emerging Standards

There are no exceptions to the standards in the main body of the ATA. The following draft standard is an extension to the emerging standards for this domain.

- Generic Open Architecture (GOA) Framework, Society of Automotive Engineers (SAE), SAE AS4893.

The purpose of this standard is to provide a framework to identify interface classes for applying open systems interface standards to the design of a specific hardware/software system. This framework is used to define an abstract architecture based on a generic set of interface points. The generic set of system interface points facilitate identification of critical interfaces.

It is intended that the GOA Framework be specialized for varying domains. A domain specific implementation of the GOA Framework will increase the chance that components/capabilities produced independently will "plug and play" and evolve affordably within the domain. The GOA Framework provides a basis for commonality for both vendors and users of components/capabilities. Application of the GOA Framework will impose constraints on individual domains and implementations. This will increase the likelihood that independently produced products will interoperate.

Application of the GOA Framework together with the appropriate open system interface standards is expected to provide the following benefits to future programs:

- Provide the basis for establishing a set of specifications, standards and procedures that will become common to all elements of a major system.
- Ensure that future systems can be upgraded and maintained with minimal redesign impact to the existing system by establishing the interfaces required to enable modular replacement of hardware and software.

- Promote availability of multiple sources of needed software and hardware, especially commercial off-the-shelf components.
- Provide a pool of hardware and software modules for multiple program commonality and re-use.
- Insure access to the architecture and its design documentation for any vendor or agency desiring to propose new uses and applications, and to facilitate competition to contain cost growth.

F.3 INFORMATION TRANSFER STANDARDS

There are no exceptions or extensions to the standards in the main body of the ATA.

F.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS

There are no exceptions or extensions to the standards in the main body of the ATA.

F.5 HUMAN-COMPUTER INTERFACES

F.5.1 Mandates

F.5.1.1 Exceptions

There are no exceptions to the standards in the main body of the ATA.

F.5.1.2 Extensions

While the primary standard for military symbology for the Air Defense sub-domain is MIL-STD-2525A, MIL-STD-1477B will be used as a supplement where MIL-STD-2525A symbology does not meet the Air Defense sub-domain's operational requirements, such as indicating an air track that is hostile but unengageable.

F.6 INFORMATION SECURITY

There are no exceptions or extensions to the standards in the main body of the ATA.

This page was intentionally left blank.

APPENDIX G - MODELING & SIMULATION DOMAIN EXCEPTIONS AND EXTENSIONS

G.1 DOMAIN DESCRIPTION

The Modeling and Simulation Domain consists of live, virtual and constructive modeling and simulations for training and combat analysis. Distributed Interactive Simulation (DIS) is a government/industry initiative to define an infrastructure for linking simulations of various types at multiple locations to create realistic, complex, virtual "worlds" for the simulation of highly interactive activities. This infrastructure brings together systems built for separate purposes, technologies from different eras, products from various vendors, and platforms from various services and permits them to interoperate. DIS exercises are intended to support a mixture of virtual entities (human-in-the-loop simulators), live entities (operational platforms and test and evaluation systems), and constructive entities (wargames and other automated simulations).

On September 10, 1996, the Under Secretary of Defense for Acquisition and Technology, signed a memorandum designating the new High Level Architecture (HLA) as the technical architecture for all simulations in the Department of Defense.

The DOD Modeling & Simulation (M&S) High Level Architecture (HLA) provides the framework for standards for the U.S. Army’s modeling and simulation. The M&S HLA builds on and extends the previous architectures and associated standards which have been developed and used successfully for specific classes of simulation. This includes the current Distributed Interactive Simulation (DIS) protocol standards which support networked, real-time platform-level virtual simulation and the Aggregate Level Simulation Protocol (ALSP) which is used to support distributed constructive simulations. The M&S HLA provides a common architecture for all classes of simulation and, consequently, M&S HLA standards encompass both the current DIS and ALSP.

G.2 INFORMATION PROCESSING STANDARDS

IEEE Standard 1278 is described in both the Information Transfer and the Information Modeling and Data Exchange sections of this appendix. Used together, these standards will define an interoperable simulated environment, and will specify the requirements that need to be met by simulations participating in a Distributed Interactive Simulation. There are no exceptions to the standards in the main body of the ATA. The following standards apply in addition to those found in the main body of the ATA.

G.2.1 Mandates

There are no exceptions to the standards in the main body of the ATA.

G.2.1.1 Information Processing Standards

The M&S HLA (DOD M&S HLA Mandated Baseline Definition, September 10, 1996) is defined by M&S HLA Rules, the M&S HLA Interface specification and the Object Model Template Specification.

- M&S HLA Rules Version 1.0, 15 September 1996: The M&S HLA rules describe the responsibilities of federates (simulations or supporting utilities) and federations (sets of simulations working together to support M&S HLA distributed applications). The rules comprise a set of underlying technical principles for the M&S HLA.
- Interface Specification Version 1.0, 15 September 1996: In the M&S HLA, federates interact with a runtime infrastructure (analogous to a special purpose distributed operating system) to establish and maintain a federation and to enhance information exchange among simulations. The M&S HLA interface specification defines the nature of these interactions, which are arranged into sets of basic RTI services.
- Object Model Template Version 1.0, 15 September 1996: The M&S HLA requires simulations and sets of interacting simulations ("federations") to each have an object model describing the entities represented in the simulations and the data to be exchanged across the federation. The M&S HLA object model template prescribes the method for recording the information in the object models, to include objects, attributes, and interactions, but it does not define the specific data (e.g., vehicles, unit types) that will appear in the object models.

G.2.2 Emerging Standards

M&S will become increasingly dependent on Object Oriented Technology (OOT). OOT emerging standards for simulation include:

1) Those contained in the Object Data Management Group (ODMG) document ODMG-93

2) The American National Standards Institute (ANSI) SQL3 (also called Object SQL)

3) The unnamed Unified Commercial Off The Shelf (COTS) standard approach being developed by the OOT industry.

The Conceptual Models of the Mission Space (CMMS) is a first abstraction of the real world and serves as a frame of reference for simulation development by capturing the features of the problem space. Those features are the entities involved in any mission and their key actions and interactions. The CMMS is a simulation neutral view of the real world and acts as a bridging function between the Warfighter, who owns the combat process and serves as the authoritative source for validating CMMS content, and simulation developers. Additionally, the CMMS provides a common viewpoint and serves a vehicle for communications among Warfighters, doctrine developers, trainers, C4I developers, analysts, and simulation developers. Such a foundation allows all concerned parties to be confident that simulations are founded in operational realism.

Standard representation of the natural environments will offer stability in the M&S Research, Development, Test & Evaluation (RDT&E) sampling requirements. Models of military operations depend on interaction with representations of natural environment including permanent and semi-permanent man-made features. Further realistic representation of military operations requires integration of weapons effects and resulting environments. This requires authoritative three-dimensional representations of the terrain, oceans, atmosphere, and space to include environmental quality issues (e.g., conservation, pollution prevention). Environmental representations must be seamless in terrain, ocean, atmosphere, and space boundary regions to fully present fully integrated data for M&S use.

The Synthetic Environment Data Representation Interchange Specification (SEDRIS) is a format-independent data representation model for interchanging synthetic environment databases, including any combination of (but not limited to): terrain, ocean, atmosphere, three-dimensional icons/models, features, topology, symbols, sound, textures, and special effects. Specifications have been developed and are in use for all of these models by the U.S. Army for with the exception of the sound, textures, and special effects. Simulation Information Format (SIF) will be replaced by the Synthetic Environment Data Representation Interchange Specification (SEDRIS).

G.3 INFORMATION TRANSFER STANDARDS

There are no exceptions to the standards in the main body of the ATA. The following standards apply in addition to those found in the main body of the ATA.

IEEE 1278.2-1995: DIS Communication Services and Profiles

SCOPE: This standard establishes the requirements for the communication services to be used in a Distributed Interactive Simulation application. This standard supports IEEE 1278.1-1995. Addressing of host computers is handled by the mechanisms provided by this document and incorporated within the profiles. This document provides two such profiles for use with existing DIS applications. Later versions of this standard will specify other profiles that may be used with DIS applications. It is up to the users to determine which profile will satisfy the requirements for a particular exercise. Furthermore, this document only addresses the communication services network layers 3 and 4 of the Open Systems Interconnection (OSI) Reference Model. It is envisioned that future versions of this document will address the remaining layers (5, 6, and parts of 7).

PURPOSE: The purpose of this document is to establish requirements for communication subsystems that support Distributed Interactive Simulations. This standard provides service requirements and associated profiles that can be individually selected to meet specific DIS system operational requirements. Profile-1 and profile-2 are currently the only profiles provided. It is expected that requirements for communication services applicable to emerging DIS applications such as Field Instrumentation will be more fully addressed in a future version.

G.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS

There are no exceptions to the standards in the main body of the ATA. The following standards apply in addition to those found in the main body of the ATA.

G.4.1 IEEE 1278.1-1995: DIS Application Protocols

SCOPE: This standard defines the format and semantics of data messages, also known as Protocol Data Units (PDUs), that are exchanged between simulation applications and simulation management.

PURPOSE: The PDUs provide information concerning simulated entity states, the type of entity interactions that take place in a DIS exercise, and data for management and control of a DIS exercise. This standard also specifies the communication services to be used with each of the PDUs.

G.4.2 IEEE 1278.3-1995: DIS Exercise Management and Feedback

SCOPE: This standard addresses the exercise control and feedback stations connected into DIS networks. IEEE Standard 1278.3, currently in revision prior to balloting recirculation, provides a recommended practice for Distributed Interactive Simulation exercise management and feedback

PURPOSE: Exercise management and feedback stations are not currently covered by standards. In fulfilling this need, the working group will define the functions that must be implemented in Exercise Management and Feedback Stations. These functions will allow the exercise manager to control exercise participants and to provide feedback of exercise results to participants; both groups distributed geographically.

The recommended practice provides procedures and guidelines used to plan, set up, execute, manage and assess a DIS exercise. It provides guidelines for sponsors, providers and supporters of DIS compliant systems and exercises. It provides functional requirements for developers of DIS exercise management and feed back stations. It specifies the functions of the organizations involved in a DIS exercise and the top level process recommended to accomplish those functions. Special attention is paid to the elements of this process that support verification, validation, and accreditation of the DIS exercise.

G.5 HUMAN-COMPUTER INTERFACES

There are no exceptions to the standards in the main body of the ATA.

G.6 INFORMATION SECURITY

There are no exceptions to the standards in the main body of the ATA.

APPENDIX H - ATA VERSION CHANGE MATRIX

A summary of the changes between ATA Version 4.0 and this version is listed in the tables below.

TABLE H-1 SECTION 1, TECHNICAL ARCHITECTURE OVERVIEW CHANGES

Section	Item	ATA 4.0	ATA 4.5	Remarks
1.1.2.1 1.1.2.2 1.1.2.3	Architecture definitions	TA, OA, SA	Changed to JTA definitions	JTA
1.1.3	ADO RAMP process, “Mark-On-The-Wall”	None	Added	Updated
1.1.3	HQDA systems	None	Apply to HQDA and HQDA FOAs	Updated
1.1.3 Figure 1-2	Joint Vision 2010	None	Rebased on Joint Vision 2010	Updated
1.1.4	ATA implements JTA	None	Army implements JTA standards through the ATA	JTA
1.1.5	JTA	None	JTA 1.0 is one of 5 primary sources, remove TAFIM discussion	JTA
1.1.6	ATA Change Matrix	None	Appendix H, ATA 4.0 to 4.5 changes	Updated
1.2	Standards profiles	Included	Some removed and replaced with actual modifications	JTA
1.2.1	DII COE	GCCS	DII	JTA

TABLE H-2 SECTION 2, INFORMATION PROCESSING STANDARDS CHANGES

Section	Item	ATA 4.0	ATA 4.5	Remarks
2.1	COE	Concept & GCCS 2.0 APIs	Concept & DII COE 2.0 APIs	JTA (Lacking of API References)
2.2.1	Application Software Entity	GCCS COE Spt Applications & Application Platform Applications	DII COE Spt Apps TA compliant Platform Apps Follow DII COE IR&TS Segmentation rules	JTA
2.2.2.1.1.1	Programming Languages	Ada 95	Ada 95	JTA - DODD 3405.1
2.2.2.1.2	User Interface Svs	CDE - Emerging	CDE - Mandated	JTA (Ties to Motif 1.2)
2.2.2.1.3	Data Mgmt Svs	FIPS 127-2 & ISO 12227	FIPS 127-2 - Deleted ISO 12227	JTA & Lack of market support
2.2.2.1.4.1	Data Interchg Svs	HTML 3.0	HTML 2.0 mandated HTML 3.2 emerging	JTA - HTML 3.0 abandoned
2.2.2.1.4.1	Data Interchg Svs	Table 2-1 Emerging	JTA Table 2-1 - Mandated	JTA - Minimal set
2.2.2.1.4.2	Graphics Data Interchg	DMA Geo Data Stds JPEG	New section + WGS 84 JPEG File Interchange Format	JTA
2.2.2.1.4.3	Imagery Data Interchg	NITFS - Except TACO2	NITFS - Broken out w/o TACO2	JTA
2.2.2.1.4.7	Video Data Interchg	MPEG-1 Mandated MPEG-2 Emerging	MPEG-1 & 2 Mandated	JTA
2.2.2.1.4.8	Atmos Data Interchng	None	Mandated	JTA
2.2.2.1.4.9	Ocean Data Interchg	None	Mandated	JTA
2.2.2.1.7	Operating Sys Svs	POSIX suite (-)	POSIX suite + updated 1003.1	JTA * Updated
2.2.2.2.4	Distrib Comp Svs	X/Open XFN CORBA Emerging	XFN Deleted CORBA Emerging	JTA JTA - CORBA Mandated

TABLE H-3 SECTION 3, INFORMATION TRANSFER STANDARDS CHANGES

Section	Item	ATA 4.0	ATA 4.5	Remarks
3.2.1.3	BOOTP	Included	Added RFC-1533	JTA
3.2.1.3	Connectionless application layer for transfer of VMF msgs	3.2.1.3	Moved to 4.2.4.2	More applicable in Data Exchange
3.2.1.5	VTC	Mandated ITU H.320, H.324 and Industry VTC profile	Mandated VTC001-Rev1 & H.324 (H.320 in VTC001-Rev1)	JTA
3.2.2	BGP V4	Mandated RFC 1654	Replaced RFC 1654 w/ RFCs 1771 & 1772	JTA
3.2.2	BOOTP	Mandated	Added RFCs mandates	JTA
3.2.2	OSPF	Multicast OSPF (RFC 1584)emerging	Mandated RFC 1584	JTA
3.2.2	Trivial FTP protocol	None	STD-33	JTA
3.2.3.1	Serial Lines	PPP and LAPB	Dropped LAPB for routers	JTA
3.2.3.2	JTF LAN	None	IEEE 802.3, 10Base-T	JTA
3.2.3.4, 3.3.2	Local Area Network (LAN) Emulation over ATM, and PNNI	PNNI and LANE emerging	Mandated PNNI and LANE	Standard matured and products available
3.2.3.5	X.25	MIL-STD 188-114A, MIL-STD-200, MIL-STD 2045-14502-3	Dropped MIL-STD-188-114A, MIL-STD-188-200, and MIL-STD 2045-14502-3: Added X3.100.	Not in JTA/ Commercial Stds
3.2.3.6	ISDN	International	Same	Different from JTA
3.3.1	IPv6	Emerging	Added emerging RFCs	JTA
3.3.2	MIL-STD-188-176	Emerging	Deleted	Removed profile
3.3.2	PCS/Mobile Cellular	None	Added emerging standards	New emerging Stds

TABLE H-4 SECTION 4, INFORMATION MODELING AND DATA EXCHANGE STANDARDS CHANGES

Section	Item	ATA 4.0	ATA 4.5	Remarks
4.2.2	Data Model	Enterp Data Model	Def Data Model	JTA - Updated
4.2.2	Data model development	DOD 8320.1-M-X	DOD 8320.1-M-1	Update
4.2.4.6 4.2.5	Data Exch Emerging Stds & Mod & Simulation	Separate paragraphs	4.3 Emerging Std updated Removed Mod & Sim	JTA and updated emerging stds
4.2.4.1	Data Exch	msg sets - "interim"	msg sets - "current"	Editorial
4.2.4.2	VMF	TF XXI	VMF TIDP & MIL-STD-2045-47001	JTA and correctness
4.2.4.4	TADIL Msgs	TADIL J Series...	J-Series of TDLs: Added JTIDS TIDP-TE, and STANAG 5516 - Link 16	JTA * (between systems that use a Joint Tactical Data Link)
4.3.3	MIDS	Emerging	Removed	Updated

TABLE H-5 SECTION 5, HUMAN-COMPUTER INTERFACES CHANGES

Section	Item	ATA 4.0	ATA 4.5	Remarks
5.2.1.3	Common Fighting Symbology	2525 Version 1 mandated Version 2525A - Emerging	2525A mandated	Updated - DCSOPS Concurrence
5.2.1.3	FM 101-5-1 in symbology	None	Added for doctrinal meaning and use of military symbology	Updated
5.2.2.3	Domain-level Style Guides	GCCS User Interface Spec	DII User Interface Spec, and Army WSHCI Style Guide	JTA and updated
5.3	Emerging Stds	DII UI Spec &	CDENext Style Guide & Wpn Sys Style Guide	JTA and updated

TABLE H-6 SECTION 6, INFORMATION SECURITY CHANGES

Section	Item	ATA 4.0	ATA 4.5	Remarks
6.2.1.1	App SW Entity -	FORTEZZA Plus ICD	FORTEZZA Crypto Interface Programmer's Guide	JTA
6.2.1.1 6.3.1.1	App SW Entity - Info Transfer Sec Stds	DoD mandated use of MISSI products	DOD mandates use of FORTEZZA for email for all systems	Army position
6.2.1.2	Appl Platform Entity	POSIX 1003.6	Deleted	JTA
6.2.1.2	Appl Platform Entity	DCE Security - Emerging	Kerberos - RFC 1510 - for use w/ DCE 1.1	JTA
6.2.1.2 6.3.1.1.2	Security labels	6.2.1.2 mandated DNSIX	6.2.1.2 removed DNSIX, 6.3.1.1.2 added MIL-STD-2045-48501	JTA
6.2.2.1	Emerging Stds - App. Sw Entity	ISO/IEC DII 10181 OSI	Deleted	JTA
6.2.2.2	Emerging Stds - App Platform SW	SOCKS	Deleted	JTA
6.2.2.4	Security Extension	FTP Security Extn	Deleted	JTA
6.3.1.1.2	MISSI Security Protocols	FIPS Pub JJJ, ID & Authentication	FIPS Pub 196	Updated

TABLE H-7 APPENDIX D, SUSTAINING BASE/OFFICE AUTOMATION DOMAIN EXCEPTIONS AND EXTENSIONS CHANGES

Section	Item	ATA 4.0	ATA 4.5	Remarks
App. D				No significant changes

TABLE H-8 APPENDIX E, C3I DOMAIN EXCEPTIONS AND EXTENSIONS CHANGES

Section	Item	ATA 4.0	ATA 4.5	Remarks
E.2.2	CDE	Emerging	Mandated in 2.2.2.1.2	JTA
E.5	HCI User Interface Specification	GCCS	DII User Interface Specification includes CDE	JTA - Updated

TABLE H-9 APPENDIX F, WEAPONS SYSTEM DOMAIN EXCEPTIONS AND EXTENSIONS CHANGES

Section	Item	ATA 4.0	ATA 4.5	Remarks
F.2.2	SAE Generic Open Architecture (GOA)	None	Emerging, draft GOA	New emerging standard
F.5.1.1	Human-computer Interfaces Extensions	None	Mandates MIL-STD 1477B as supplement to MIL-STD 2525A	For Air Defense Sub-domain

TABLE H-10 APPENDIX G, MODELING & SIMULATION DOMAIN EXCEPTIONS AND EXTENSIONS CHANGES

Section	Item	ATA 4.0	ATA 4.5	Remarks
G.1, G.2.1.1	HLA	Emerging	Mandated	Update, DOD mandated
G.2.2	SEDRIS	None	Emerging	New emerging specification, DMSO plans