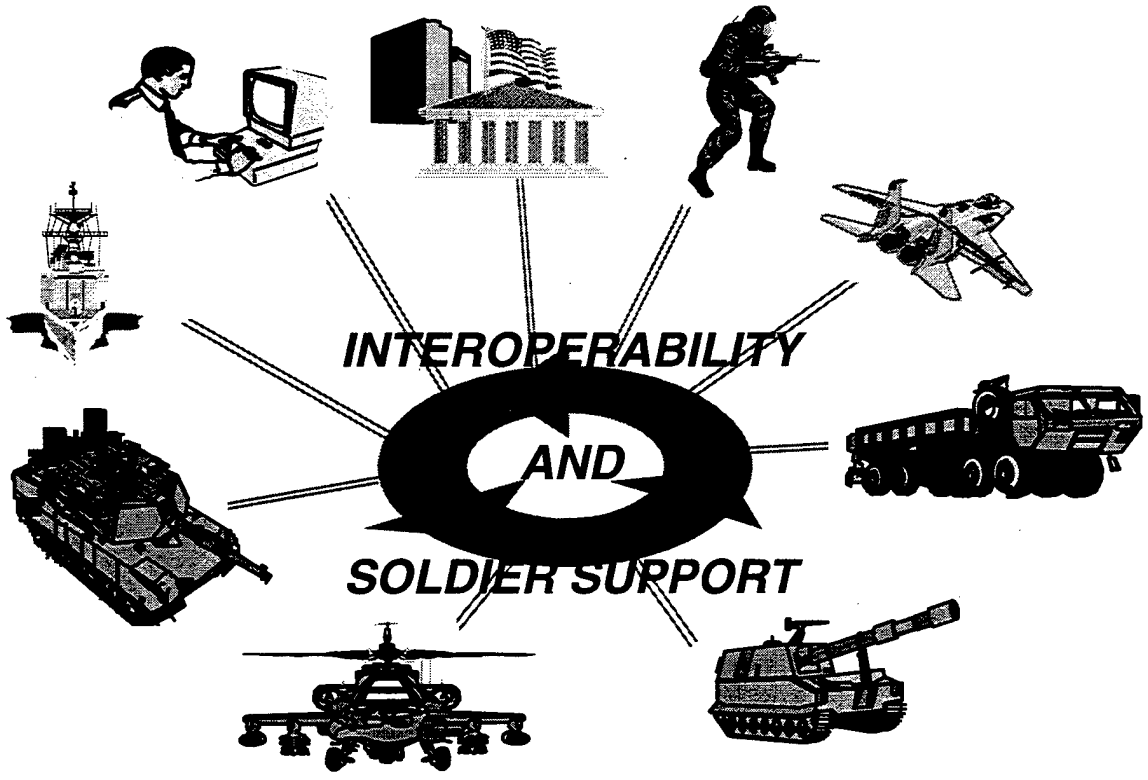
Enterprise

Joint Technical Architecture - Army



DTIC QUALITY INSPECTED 4

19980212 031

Department of the Army

Version 5.0
11 September 1997

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

ffice. Director of Information
ystems for Command, Control,
ommunications, & Computers

11 SEP 1997

SAIS-PAA

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Implementation of the Joint Technical Architecture-Army, Version 5.0 (Formerly the Army Technical Architecture (ATA))

References [1]:

a. Memorandum, SAIS-ADM, 30 Jan 96, Subject: Implementation of the Army Technical Architecture.

b. DACS-ZB message, 29 May 96, Subject: Army Technical Architecture Implementation.

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

d. Memorandum, SAIS-ADM, 12 Nov 96, Subject: Implementation of the Army Technical Architecture, Version 4.5.

e. Memorandum, SAIS-ADM, 06 Dec 96, Subject: Implementation of the Department of Defense (DOD) Joint Technical Architecture.

The Joint Technical Architecture-Army (JTA-Army), Version 5.0 [2], formerly titled the Army Technical Architecture (ATA), has completed the configuration management process, and is mandatory for all systems that produce, use, or exchange information electronically. This version extends the minimum set of interoperability standards [3], for the Chief of Staff's FY2000 "Mark on the Wall" for interoperability of Division XXI systems (reference b.). The timeline contained in reference b still holds. JTA-Army compliance is the method by which the Army implements compliance with the Joint Technical Architecture (JTA).

The JTA-Army is also the Army's mechanism for meeting compliance with a number of DOD mandated architectures: Joint Technical Architecture (JTA) for C4I systems, High Level Architecture (HLA) for modeling and simulation systems, and the Open Electronic Standards (OES) for weapons systems. Compliance with the JTA-Army is the means by which Army organizations will meet these DOD mandates (reference e).

---

[1] References are available on a Website at "http://www.hqda.army.mil/techarch/".
[2] Attachment: Joint Technical Architecture - Army, Version 5.0.
[3] Attachment: Set of Critical Interoperability Standards.

Printed on Recycled Paper

This JTA-Army version updates existing standards, mandates selected emerging standards that have sufficiently matured, and provides additional standards in areas not covered by previous versions (references a and d). A detailed summary of JTA-Army changes from Version 4.0 to Version 5.0 is in Appendix H. All non-commercial standards mandated in the JTA-Army have met the DOD Commercial Standards Policy and are waived. A request for waiver or exception to policy is not required.

This version supersedes previous versions (references a for Version 4.0, and d for Version 4.5). The effective date of JTA-Army 5.0 is 60 days after signature of this letter. Procurements currently underway may continue to use previous versions, unless systems must be modified in order to maintain interoperability. New procurements, Requests for Proposal, and new Migration Plans will be based on JTA-Army Version 5.0. Reference c [4] provides procedures for the submission and approval of JTA-Army Migration Plans.

JTA-Army Version 5.0 includes significant changes as compared to previous versions, and as a result, all systems developers are required to review the changes, including the Joint Variable Message Format (Joint VMF) and the Calendar Date Data Format for Y2K compliance [5]. Another major change is the extension of Win32 APIs for operating systems (OS) and corresponding Human Computer Interfaces (HCI) to the Modeling and Simulation Domain. Win32 APIs have been in the Sustainment Domain since Version 4.0.

JTA-Army Version 5.0, as well as other JTA-Army documentation, is available for viewing and downloading on the World Wide Web at URL "http://www.hqda.army.mil/techarch/". Technical questions regarding JTA-Army Version 5.0 should be referred to the Army Systems Engineering Office (ASEO), Mr. Paul Manz, DSN 987-3309, Commercial (732) 427-3309, "manz@doim6.monmouth.army.mil". All other questions about the JTA-Army should be referred to the Office, Director of Information Systems for Command, Control, Communications, and Computers (DISC4), Mrs. E. Jean Gilleo, DSN 227-4189, Commercial (703) 697-4189, E-mail: "gilleej@hqda.army.mil".

RONALD H. GRIFFITH
General, United States Army
Vice Chief of Staff

ROBERT M. WALKER
Army Acquisition Executive

2 Attachments

[4] This document will be revised to reflect the pending assumption of migration planning oversight for MACOM, Agency, and Installation systems by the Director of Information Systems for Command, Control, Communications, and Computers. At that time, a separate set of procedures covering migration planning for these systems will be published.

[5] See JTA-Army Version 5.0 sections 4.2.4.2 and 4.2.6.

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 (RDA), 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, SAIS-2A, 107 Army Pentagon, Washington, DC 20310-0107

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

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

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 20310-1007

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, 5109 Leesburg Pike, Room 672, Falls Church, VA 22041-3258

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

Commanding General, U.S. Army Aviation and Missile Command, ATTN AMSAM-CG, Redstone Arsenal, AL 35898

U.S. Army Tank-Automotive and Armaments Command, Commander, Warren, MI 48397-5000

Director, U.S. Army Aviation Research Development Center, ATTN AMSAT-R-Z, 4300 Goodfellow Blvd, St. Louis, MO 63120-1798
Army Digitization Office (ADO), ATTN DACS-ADO, 201 Army Pentagon, Room 2B679
Army Systems Engineering Office (ASEO), ATTN AMSEL-RD-ASE (Mr. Herrick), Myer Center Room 2700, Fort Monmouth, NJ 07703-5201

COMMANDER-IN-CHIEF
US Army Europe and Seventh Army, Commander-in-Chief, ATTN AEAIM, Unit 29351, APO, AE 09014

COMMANDER
US Army Communications-Electronics Command and Fort Monmouth, Commander, ATTN AMSEL-CG, Fort Monmouth, NJ 07703-5000
US Army Corps of Engineers, Commander, ATTN CECG, 20 Massachusetts Ave NW, Washington, DC 20314-1000
US Army Forces Command, Commander, ATTN DCG, Fort McPherson, GA 30330
US Army Health Services Command, Commander, ATTN HSIM, Fort Sam Houston, TX 78234-6000
US Army Information Systems Command, Commander, ATTN ASCG, Fort Huachuca, AZ 85613-5000
US Army Information Systems Engineering Command, Commander, ATTN ASQB-OCG, Fort Huachuca, AZ 85613-5000
US Army Intelligence and Security Command, Commander, ATTN IACG, Fort Belvoir, VA 22060-7040
US Army Materiel Command, Commander, ATTN AMCDCG, 5001 Eisenhower Ave, Alexandria, VA 22333-0001
US Army Medical Command, Commander, ATTN MCCG, Fort Sam Houston, TX 78234-6000
US Army Medical Research and Materiel Command and Fort Detrick, Commander, ATTN MCMR-ZA, Fort Detrick, MD 21702-5012
US Army Military Traffic Management Command, Commander, ATTN MTCG, 5611 Columbia Pike, Falls Church, VA 22041-5050
US Army Operational Test and Evaluation Command, Commander, ATTN CSTE-ZA, 4501 Ford Ave Park Center IV, Alexandria, VA 22302-1458
US Army Signal Center and Fort Gordon, Commander, ATTN ATZH-CG, Fort Gordon, GA 30905-5000
US Army Simulations, Training and Instrumentation Command, Commander, ATTN AMSTI-CG, 12350 Research Parkway, Orlando, FL 32826-3276
US Army Space and Strategic Defense Command, Commander, 1941 Jefferson Davis Highway, Suite 900, Arlington, VA 22215-0280
US Army Special Operations Command, Commander, ATTN AOCG, Fort Bragg, NC 28307-5200
US Army Test and Evaluation Command, Commander, ATTN AMCG, Aberdeen Proving Ground, MD 21005-5055
US Army Training and Doctrine Command, Commander, ATTN ATDC, Fort Monroe, VA 23651-5000

US Forces Korea, Commander, APO, AP 96205-0010
US Military District of Washington, Commander, 103 3d Street, Fort Lesley J McNair, Washington, DC 20319-5058

DIRECTOR
Army Research Laboratory, Director, ATTN AMSRL-HR-MB (Mr. McCommons), Aberdeen Proving Ground, MD 21005-5425
Strategic Logistics Agency, Director, ATTN LOSA, 5001 Eisenhower Ave, Alexandria, VA 22333
US Army Materiel Systems Analysis Activity, Director, ATTN AMXSY-CR, Aberdeen Proving Ground, MD 21005

PROGRAM EXECUTIVE OFFICER
Armored Systems Modernization, US Army TACOM, Program Executive Officer, ATTN SFAE-ASM, Warren, MI 48397-5000
Aviation, Program Executive Officer, ATTN SFAE-AV, 4300 Goodfellow Blvd, St. Louis, MO 63120-1798
Command Control and Communications Systems, Program Executive Officer, ATTN SFAE-C3S, Fort Monmouth, NJ 07703-5000
Field Artillery Systems, Program Executive Officer, ATTN SFAE-FAS, Picatinny Arsenal, NJ 07806-5000
Intelligence and Electronic Warfare, Program Executive Officer, ATTN SFAE-IEW, Fort Monmouth, NJ 07703-5000
Missile Defense, Program Executive Officer, ATTN SFAE-MD-HSV, PO Box 1500, Huntsville, AL 35807-3801
Standard Army Management Information Systems, Program Executive Officer, ATTN SFAE-PS, 9350 Hall Road Suite 142, Fort Belvoir, VA 22060-5526
Tactical Missiles, Program Executive Officer, ATTN SFAE-MSL, Redstone Arsenal, AL 35898-8000
Tactical Wheeled Vehicles, Program Executive Officer, ATTN SFAE-TWV, Warren, MI 48397-5000

PROGRAM MANAGER
Chemical Demilitarization, Program Manager, ATTN SFAE-CD-Z, Bldg E4585, Aberdeen Proving Ground, MD 21010-5401
Joint Program Management Office for Biological Defense, Program Manager, ATTN SFAE-BD, 5201 Leesburg Pike, Skyline 3 Room 1200, Falls Church, VA 22041-3203
Reserve Component Automation System (RCAS), Program Manager, 8510 Cinder Bed Road, Suite 1000, Newington, VA 22122-8510

SET OF CRITICAL INTEROPERABILITY STANDARDS

The set of critical interoperability standards to which the Chief of Staff's FY 2000 "Mark on the Wall" for Division XXI systems applies are contained in the Joint Technical Architecture-Army (JTA-Army), Version 5.0, within the sections listed in Table 1.

The set of critical interoperability standards listed in the "Army Technical Architecture Migration Planning, Guidance and Procedures", 17 October 1996, Section 5.3.1 - Division XXI Systems (referring to the Army Technical Architecture Version 4.0), remains in effect. The list in Table 1 below relates these standards to JTA-Army Version 5.0. JTA-Army Version 5.0 was re-organized and expanded. Therefore, Table 1 is the JTA-Army Version 5.0 set of critical interoperability standards.

Table 1 - Set of Critical Interoperability Standards

JTA-Army V5.0 Section	Title
INFORMATION PROCESSING STANDARDS	
2.2.2.1.4	Data Interchange Services
2.2.2.2.1	Internationalization Services
2.2.2.2.4	Distributed Computing Services
INFORMATION TRANSFER STANDARDS	
3.2	MANDATES (INFORMATION TRANSFER STANDARDS)
INFORMATION MODELING AND DATA EXCHANGE STANDARDS	
4.2.3	Data Definitions
4.2.4	Data Exchange
4.2.6	Calendar Date Data Format
HUMAN-COMPUTER INTERFACES	
5.2.1.3	Symbology
INFORMATION SECURITY	
6.3.1	MANDATES (INFORMATION TRANSFER SECURITY STANDARDS)
SUSTAINMENT DOMAIN EXCEPTIONS AND EXTENSIONS	
D.2.2.2	Extensions, Reference section 2.2.2.1.4.3 Geospatial Data Interchange
D.3.2.2	Extensions (INFORMATION TRANSFER STANDARDS)
C3I DOMAIN EXCEPTIONS AND EXTENSIONS	
E.3	INFORMATION TRANSFER STANDARDS
WEAPON SYSTEMS DOMAIN EXCEPTIONS AND EXTENSIONS	
F.5.2.2.1	Symbology (Reference section 5.2.1.3)

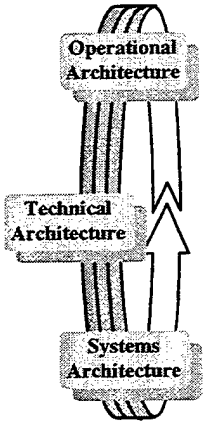
Joint Technical Architecture - Army, Version 5.0

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.

A Technical Architecture (TA) 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 fosters interoperability between systems, as well dramatically reducing 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

The name of the Army Technical Architecture (ATA) has changed to the Joint Technical Architecture - Army (JTA-Army). The first reason for the change is that the Joint Technical Architecture (JTA), Version 2.0, is expanding its breadth of scope to include the Sustainment, Weapons, and Modeling and Simulation Domains. JTA Version 2.0 is scheduled to be published in December 1997, and contain the first expansion into the new domains. Second, the JTA-Army, as it now stands, is the comprehensive set of standards required for Army and Joint interoperability. The Army responded to an Office of the Secretary of Defense (OSD) request by stating that the Army will implement the JTA

---

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

through the implementation of the ATA. Renaming the document to JTA-Army will lessen confusion on the part of Army developers that have to comply with the JTA. Third, there is a perception at certain levels that the ATA is different from the JTA. This is not true. As stated, the ATA, or now JTA-Army, is a comprehensive set of standards for Army and Joint interoperability which is compliant with the JTA. This gives Army systems developers a single technical standards document to go to for the standards that need to be followed at all levels.

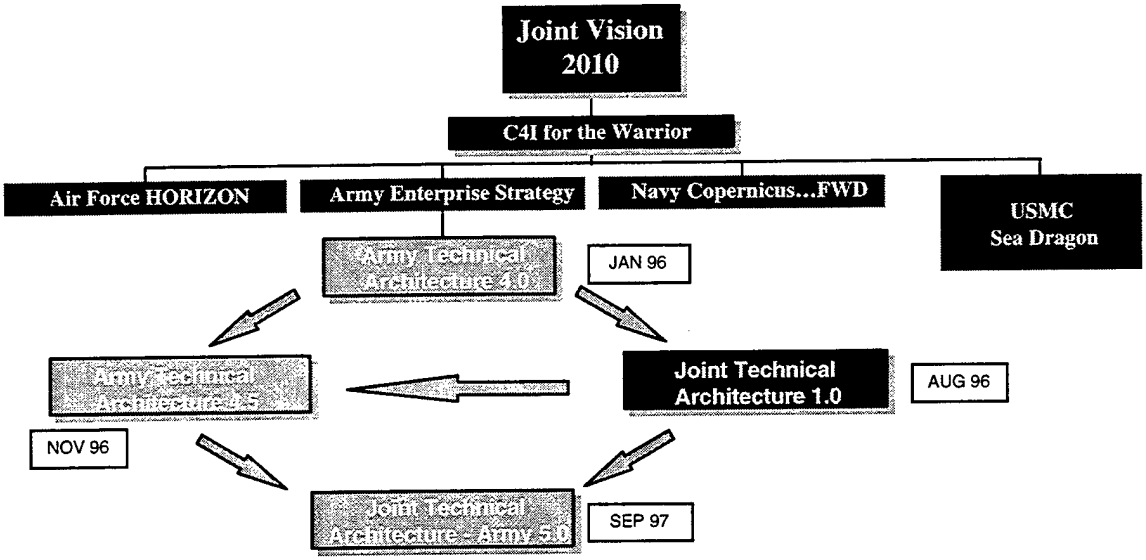
SCOPE

The Joint Technical Architecture - Army (JTA-Army) applies to all systems that produce, use, or exchange information electronically. The JTA-Army 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 JTA-Army. System developers will comply with the JTA-Army in order to ensure that products meet interoperability, performance, and sustainment criteria. Combat developers will use the JTA-Army in developing requirements and functional descriptions. Battle Labs will use the JTA-Army to ensure that the fielding of their "good ideas" is not unduly delayed by the cost and time required for wholesale re-engineering to meet interoperability standards. Compliance with JTA-Army 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 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 version. In order to be more discriminating in the applicability of standards and to extend the TA 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. Version 4.5 built upon the expanded groundwork of Version 4.0, updated evolving mandated and emerging standards, and aligned existing C4I-oriented mandates with the Joint Technical Architecture (JTA), Version 1.0. Version 5.0 updates evolving mandated and emerging standards, includes C and Ada 95 as acceptable programming languages, adds SMTP for non-DMS electronic mail, and adds network system management standards. Version 5.0

will continue to be the central source of Technical Architecture guidance for Army systems.



WHAT'S NEW IN VERSION 5.0

This version updates existing JTA-Army standards and makes selected emerging standards that have sufficiently matured mandatory. It also includes the interoperability standards for both the Army unique and the joint environments. Changes include:

- Updated the public DII COE APIs from 2.0 to 3.1.
- Included C with previously mandated Ada 95 as acceptable programming languages, and added C++ as emerging.
- Added audio MPEG-1 Layer 3 for audio interchange.
- Added GZIP for file compression standard.
- Added SMTP for non-DMS electronic mail.
- Added video teleconference standards.
- Added facsimile standards.
- Added 100Base-T and 100Base-F Ethernet.
- Added ATM standards.
- Added SONET.
- Updated network system management standards for data communications and added telecommunications management standards.
- Added Joint VMF TIDP-TE for message exchange.
- Included calendar date data format mandate from Version 4.5 Urgent Change #1 related to the Y2K problem.

- Mandated MIL-STD-1472E style guide.
- Added security password usage, security protocols and DMS security interface mandates.
- For the Sustainment Domain, added spatial data standard for USACE systems and added medical community standards.
- For the C3I Domain, TACO2, SATCOM and radio communications standards.
- For the Weapons System Domain, added symbology, bus interface and general hardware interface standards.
- For the Modeling & Simulation Domain (M&S), defined the scope to exclude embedded M&S and added the simulator database interchange format standard.
- For the M&S Domain, added Win32 APIs with previously mandated POSIX for user interfaces, operating system services and commercial style guide.

A more comprehensive catalogue of changes made to JTA-Army, Version 5.0 is contained in Appendix H of the JTA-Army, with respect to Version 4.0 to 4.5 and to Version 4.5 to 5.0. Appendix I is similar comparison of JTA Version 1.0. and JTA-Army Version 5.0. JTA-Army is available on-line at a World Wide Web address, Uniform Resource Locator (URL), of "http://www.hqda.army.mil/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.

INTERNET AVAILABILITY

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

COMMENTS ON THE JOINT TECHNICAL ARCHITECTURE - ARMY

To speed processing and consideration, comments and suggested changes should be submitted electronically via Email. Submit your comment on the Joint Technical Architecture - Army (JTA-Army) Comment Form. The Comment Form is available on the WWW at URL: "http://www.hqda.army.mil/techarch/comform.htm". Fill in the comment form and E-mail to: "armyta@HQDA.ARMY.MIL". Each comment will receive a unique Army Reference Number for tracking purposes. Receiving comments via E-mail and using this Comment Form allows us to distribute your comment to the Army Technical Architecture Configuration Management Board (CMB) and the appropriate working groups so we can 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 can be found on the WWW at URL "http://www.hqda.army.mil/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**

INTERNET AVAILABILITY ..... **i**

COMMENTS ON THE JOINT TECHNICAL ARCHITECTURE - ARMY ..... **ii**

TRADEMARKS AND REFERENCES ..... **iii**

TECHNICAL ARCHITECTURE OVERVIEW **1**

1.1 INTRODUCTION 1
1.1.1 Purpose *1*
1.1.2 Architectures Defined *1*
1.1.2.1 Technical Architecture 1
1.1.2.2 Operational Architecture 2
1.1.2.3 Systems Architecture 2
1.1.3 Scope *2*
1.1.4 Background *3*
1.1.5 Basis for the JTA-Army *5*
1.2 TECHNICAL ARCHITECTURE 5
1.2.1 COMMON OPERATING ENVIRONMENT/ DOMAINS *6*
1.2.2 DOCUMENT ORGANIZATION *7*
1.2.2.1 Information Processing Standards 8
1.2.2.2 Information Transfer Standards 8
1.2.2.3 Information Modeling and Data Exchange Standards 8
1.2.2.4 Human-Computer Interfaces 9
1.2.2.5 Information Security 9

INFORMATION PROCESSING STANDARDS **11**

2.1 INTRODUCTION 11
2.1.1 Purpose *11*
2.1.2 Scope *11*
2.1.3 Background *12*
2.2 MANDATES 12
2.2.1 Application Software Entity *13*
2.2.2 Application Platform Entity *14*
2.2.2.1 Service Areas 14
2.2.2.2 Application Platform Cross-Area Services 22
2.3 EMERGING STANDARDS 24
2.3.1 DII COE *24*
2.3.2 Service Area Standards *24*

INFORMATION TRANSFER STANDARDS **27**

3.1 INTRODUCTION 27
3.1.1 Purpose *27*

3.1.2 Scope *27*
3.1.3 Background *27*
3.1.3.1 Communications Framework 27
3.1.3.2 Protocol Standards 28
3.1.3.3 Protocol Profiles 28
3.2 MANDATES 28
3.2.1 End System Standards *28*
3.2.1.1 Host Standards 28
3.2.1.2 Video Teleconferencing (VTC) Standards 32
3.2.1.3 Facsimile Standards 33
3.2.1.4 Secondary Imagery Dissemination Standards 33
3.2.1.5 Global Position System (GPS) Standards 33
3.2.2 Network Standards *34*
3.2.2.1 Router Standards 34
3.2.2.2 Subnetworks 35
3.2.3 Transmission media *41*
3.2.3.1 Military Satellite Communications (MILSATCOM) 41
3.2.3.2 Radio Communications 41
3.2.3.3 Synchronous Optical Network (SONET) Transmission Facilities 41
3.2.4 Summary of Packet Standards *41*
3.2.5 Network and Systems Management *42*
3.2.5.1 Data Communications 42
3.2.5.2 Telecommunications 43
3.3 EMERGING STANDARDS 43
3.3.1 Emerging Host Standards *43*
3.3.2 Emerging Network Standards *44*

INFORMATION MODELING AND DATA EXCHANGE STANDARDS 47

4.1 INTRODUCTION 47
4.1.1 Purpose *47*
4.1.2 Scope *47*
4.1.3 Background *47*
4.2 MANDATES 50
4.2.1 Activity Model *50*
4.2.2 Data Model *51*
4.2.3 Data Definitions *52*
4.2.4 Data Exchange *52*
4.2.4.1 Data Exchange Applicability 52
4.2.4.2 Connectionless Data Transfer 53
4.2.4.3 US Message Text Format (USMTF) Messages 53
4.2.4.4 Tactical Digital Information Link (J Series) Messages 53
4.2.4.5 Remote Procedure Calls 54
4.2.4.6 Database to Database Exchange 54
4.2.5 Modeling and Simulation Information and Data Exchange Standards *54*
4.2.6 Calendar Date Data Format *54*
4.3 EMERGING STANDARDS 54
4.3.1 Activity Modeling *54*
4.3.2 Data Modeling *55*
4.3.3 Data Exchange *55*

HUMAN-COMPUTER INTERFACES **57**

5.1 INTRODUCTION 57
5.1.1 Purpose *57*
5.1.2 Scope *57*
5.1.3 Background *57*
5.2 MANDATES 58
5.2.1 General *58*
5.2.1.1 Graphical User Interfaces 58
5.2.1.2 Character-based Interfaces 58
5.2.1.3 Symbology 59
5.2.1.4 Security 59
5.2.2 Style Guides *59*
5.2.2.1 Commercial Style Guides 60
5.2.2.2 DOD HCI Style Guide 60
5.2.2.3 Domain-level Style Guides 61
5.2.2.4 System-level Style Guides 61
5.3 EMERGING STANDARDS 62

INFORMATION SECURITY **63**

6.1 INTRODUCTION 63
6.1.1 Purpose *63*
6.1.2 Scope *63*
6.1.3 Background *63*
6.2 INFORMATION PROCESSING SECURITY STANDARDS 64
6.2.1 Mandated Standards *64*
6.2.1.1 Application Software Entity 65
6.2.1.2 Application Platform Entity 65
6.2.2 Emerging Standards *65*
6.2.2.1 Application Software Entity 65
6.2.2.2 Application Platform Entity 66
6.2.2.3 Authentication Security Standards 66
6.2.2.4 Generic Security Service Application Program Interface (GSS API) 66
6.2.2.5 Security Management Protocols 67
6.3 INFORMATION TRANSFER SECURITY STANDARDS 67
6.3.1 MANDATES *67*
6.3.1.1 Security Protocols 67
6.3.1.2 DMS Interface 68
6.3.1.3 MISSI Cryptographic Algorithms 68
6.3.1.4 MISSI Digital Signature Infrastructure 69
6.3.1.5 Transport Mechanisms 69
6.3.2 Emerging Standards *69*
6.3.2.1 Security Association Management 69
6.3.2.2 Secure World Wide Web (WWW) Transactions 69
6.3.2.3 Networking Security Standards 69
6.3.2.4 Security Protocols 70
6.3.2.5 Other 70
6.3.3 Summary of Standards *70*
6.4 INFORMATION MODELING AND DATA EXCHANGE SECURITY STANDARDS 70
6.4.1 Mandated Standards *72*

6.4.2 Emerging Standards 72
6.5 HUMAN-COMPUTER INTERFACE SECURITY STANDARDS 72
6.5.1 Mandated Standards 72
6.5.1.1 Security Banners and Screen Labels 72
6.5.2 Emerging Standards 72
6.5.2.1 Entity Authentication 72
6.5.2.2 Personal Authentication 73
6.6 SECURITY RELATED DOCUMENTS 73

APPENDIX A - ACRONYMS 75

APPENDIX B - LIST OF REFERENCES 85

B.1 MILITARY 85
B.1.1 DOD References *85*
B.1.2 Army References *89*
B.1.3 Other Government Agency References *89*
B.2 COMMERCIAL REFERENCES 90

APPENDIX C - GLOSSARY 101

APPENDIX D - SUSTAINMENT DOMAIN EXCEPTIONS AND EXTENSIONS 109

D.1 INTRODUCTION 109
D.1.1 Purpose *109*
D.1.2 Scope *109*
D.1.3 Background *109*
D.2 INFORMATION PROCESSING STANDARDS 110
D.2.1 Scope *110*
D.2.2 Mandates *110*
D.2.2.1 Exceptions 110
D.2.2.2 Extensions 110
D.2.3 Emerging Standards *111*
D.3 INFORMATION TRANSFER STANDARDS 111
D.3.1 Scope *111*
D.3.2 Mandates *111*
D.3.2.1 Exceptions 111
D.3.2.2 Extensions 111
D.3.3 Emerging Standards *112*
D.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS 113
D.5 HUMAN-COMPUTER INTERFACES 113
D.5.1 Scope *113*
D.5.2 Mandates *113*
D.5.2.1 Exceptions 113
D.5.2.2 Extensions 113
D.5.3 Emerging Standards *113*
D.6 INFORMATION SECURITY 113

APPENDIX E - C3I DOMAIN EXCEPTIONS AND EXTENSIONS 115

E.1 INTRODUCTION 115

E.1.1 Scope *115*
E.1.2 Background *115*
E.1.3 Appendix Organization *115*
E.2 INFORMATION PROCESSING STANDARDS 115
E.2.1 Scope *115*
E.2.2 Mandates *115*
E.3 INFORMATION TRANSFER STANDARDS 115
E.3.1 Scope *115*
E.3.2 Mandates *115*
E.3.2.1 Exceptions 115
E.3.2.2 Extensions 116
E.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS 119
E.5 HUMAN-COMPUTER INTERFACES 119
E.5.1 Scope *119*
E.5.2 Mandates *119*
E.5.2.1 Exceptions 119
E.5.2.2 Extensions 119
E.5.2.2.1 Domain-level Style Guides (Reference Section 5.2.2.3) 119
E.5.3 Emerging Standards *119*
E.6 INFORMATION SECURITY 119

APPENDIX F - WEAPON SYSTEMS DOMAIN EXCEPTIONS AND EXTENSIONS 121

F.1 INTRODUCTION 121
F.1.1 Scope *121*
F.1.2 Appendix Structure *121*
F.2 INFORMATION PROCESSING STANDARDS 122
F.2.1 Scope *122*
F.2.1.1 Top Level Extensions 122
F.2.1.2 Hierarchy of TRMs 123
F.2.2 MANDATES *124*
F.2.2.1 Exceptions 124
F.2.2.2 Extensions 124
F.2.3 EMERGING STANDARDS *124*
F.2.3.1 Emerging General Standards 124
F.2.3.2 Emerging Service Area Standards 125
F.3 INFORMATION TRANSFER STANDARDS 126
F.3.1 Scope *126*
F.3.2 MANDATES *126*
F.3.2.1 Exceptions 126
F.3.2.2 Extensions 126
F.3.3 EMERGING STANDARDS *126*
F.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS 126
F.4.1 Scope *126*
F.4.2 MANDATES *127*
F.4.3 EMERGING STANDARDS *128*
F.5 HUMAN-COMPUTER INTERFACE STANDARDS 128
F.5.1 Scope *128*
F.5.1.1 Definition 128
F.5.1.2 HCI Hierarchy 128

F.5.2 MANDATES *129*
F.5.2.1 Exceptions 129
F.5.2.2 Extensions 129
F.5.3 EMERGING STANDARDS *130*
F.5.3.1 Aviation Subdomain Style Guide 130
F.5.3.2 Ground Vehicle Subdomain Style Guide 130
F.5.3.3 Missile Subdomain Style Guide 130
F.5.3.4 Soldier Systems Subdomain Style Guide 130
F.6 INFORMATION SECURITY STANDARDS 130
F.7 APPLICATION HARDWARE STANDARDS 130
F.7.1 Scope *130*
F.7.2 MANDATES *131*
F.7.2.1 Exceptions 131
F.7.2.2 Extensions 131
F.7.3 EMERGING STANDARDS *132*
F.7.3.1 Emerging General Standards 132
APPENDIX G - MODELING & SIMULATION DOMAIN EXCEPTIONS AND EXTENSIONS .. 133
G.1 INTRODUCTION 133
G.1.1 Purpose *133*
G.1.2 Scope *133*
G.1.3 Background *133*
G.2 INFORMATION PROCESSING STANDARDS 135
G.2.1 Scope *135*
G.2.2 Mandates *135*
G.2.2.1 Exceptions 135
G.2.2.2 Extensions 135
G.2.3 Emerging Standards *137*
G.3 INFORMATION TRANSPORT STANDARDS 137
G.3.1 Scope *137*
G.3.2 Mandates *137*
G.3.2.1 Exceptions 137
G.3.2.2 Extensions (Reference Section 3.2) 137
G.3.3 Emerging Standard *138*
G.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS 138
G.4.1 Scope *138*
G.4.2 Mandates *138*
G.4.2.1 Exceptions 138
G.4.2.2 Extensions 138
G.4.3 Emerging Standards *139*
G.5 HUMAN-COMPUTER INTERFACES 139
G.5.1 Scope *139*
G.5.2 Mandates *139*
G.5.2.1 Exceptions 139
G.5.2.2 Extensions 140
G.5.3 Emerging Standards *140*
G.6 INFORMATION SECURITY 140
APPENDIX H - JTA-ARMY VERSION CHANGE MATRIX 141

H.1 ATA 4.0 TO ATA 4.5 CHANGE MATRIX 141
H.2 ATA 4.5 TO JTA-ARMY 5.0 CHANGE MATRIX 145

APPENDIX I - JTA-ARMY VERSION 5.0 COMPARISON TO JTA 1.0 MATRIX 153

This page was intentionally left blank.

SECTION 1
TECHNICAL ARCHITECTURE OVERVIEW

1.1 INTRODUCTION

The Joint Technical Architecture - Army (JTA-Army) has three mutually supporting objectives. The first and foremost objective is 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. The second objective is to provide guidelines and standards for system development and acquisition that will dramatically reduce cost, development time, and fielding time for improved systems. The third objective is 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.

1.1.1 Purpose

The purpose of this section is to provide an overview of the JTA-Army. It describes the purpose, scope, and background of the JTA-Army, 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. The Department of Defense (DOD) has implemented this by defining an interrelated set of architectures: Operational, Systems, and Technical. The diagram, 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 JTA-Army 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.

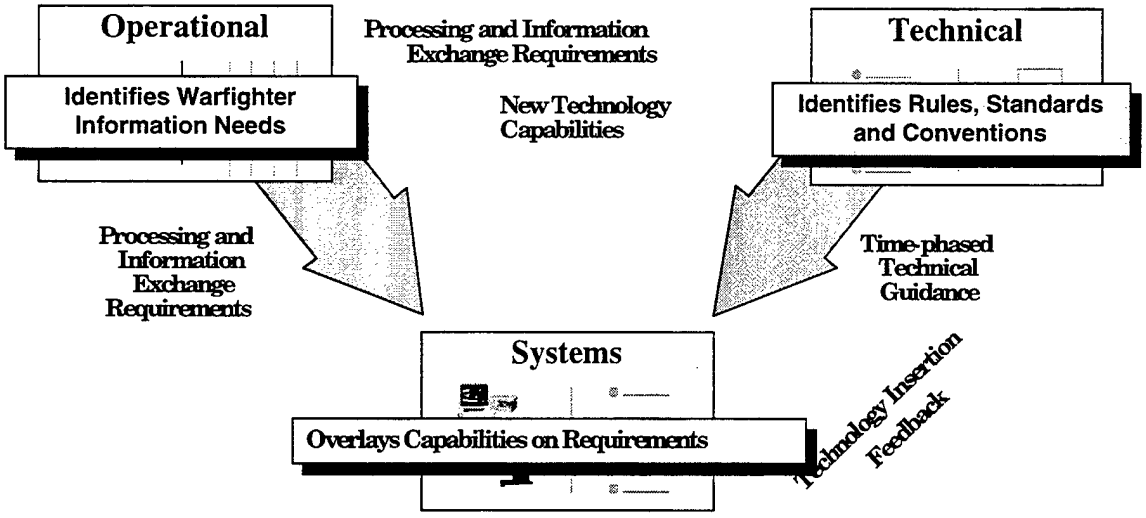


FIGURE 1-1. THE DIFFERENT ARCHITECTURES

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.

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 per 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 JTA-Army applies to all systems that produce, use, or exchange information electronically. The JTA-Army 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 JTA-Army. System developers will comply with the

JTA-Army in order to ensure that products meet interoperability, performance, and sustainment criteria. Combat developers will use the JTA-Army in developing requirements and functional descriptions. Battle Labs will use the JTA-Army to ensure that the fielding of their "good ideas" is not unduly delayed by the cost and time required for wholesale re-engineering 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 JTA-Army.

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 weapon systems, sensors and shooters -- tanks, aircraft, Unmanned Aerial Vehicles (UAVs);

2 Among Command, Control, Communications, and Intelligence (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), Joint Chiefs of Staff (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.

JTA-Army Version 5.0 supports the Army's needs over all these dimensions.

Compliance is enumerated in an implementation/migration plan. A system is compliant with the JTA-Army if it meets, or is implementing an approved plan to meet, all applicable JTA-Army 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 JTA-Army. They have mandated that by the end of 2000 all Division XXI systems must meet the critical interoperability standards identified in their migration plans and by the end of 2006 ALL systems must meet ALL applicable JTA-Army standards. The Army Digitization Office (ADO) (http://www.ado.army.mil/) has the lead for monitoring progress toward compliance with the JTA-Army.

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 (ATA), with the support of various organizations. The relationship of the ATA to DOD and other Service Architectures is shown in Figure 1-2. After the development of ATA Version 4.5 and the Joint Technical Architecture Version 1.0, the title of the ATA was changed to the Joint Technical Architecture - Army Version 5.0.

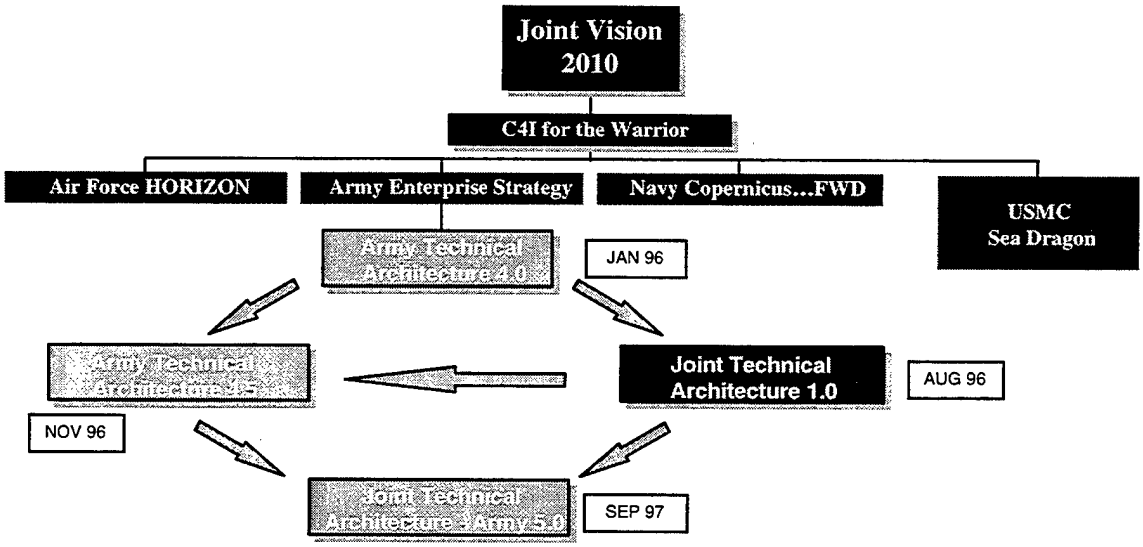


FIGURE 1-2. JTA-ARMY LINEAGE

The JTA-Army follows a direction 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 JTA-Army is fully responsive to all these mandates.

The first Army C4I 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 Weapon Systems, Sustaining Base Systems, and Information Security. Since information exchanged between weapon systems often travels via C3I systems, the standards in ATA Version 3.1 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" - Sustainment/Office Automation, C3I, Weapons, and Modeling & Simulation. ATA Version 4.5, published on 12 November 1996, built upon the expanded groundwork of ATA Version 4.0. JTA-Army Version 5.0 updates evolving mandated and emerging standards, completes the alignnment of Army Technical Architecture mandates with JTA Version 1.0, completes the minimal interoperability standards for all domains, and starts expanding the scope to include open information electronic hardware standards. Appendix H contains the list of changes in JTA-Army Version 5.0 with respect to Version 4.5. JTA-Army Version 5.0 encompasses and extends the scope of other related DOD efforts, and remains the central source of Technical Architecture guidance for Army systems. Appendix I contains the list of differences between JTA 1.0 and JTA-Army 5.0.

1.1.5 Basis for the JTA-Army

The JTA-Army 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 JTA-Army. 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 JTA-Army 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 JTA-Army 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, which was based on the Global Command and Control System (GCCS) COE. The GCCS COE was referenced for use in Version 3.1 of the ATA. 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 JTA-Army emphasizes using the COE concept, its software architecture, reusing as many

software components as possible, and building to a standard set of APIs. The JTA-Army 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.

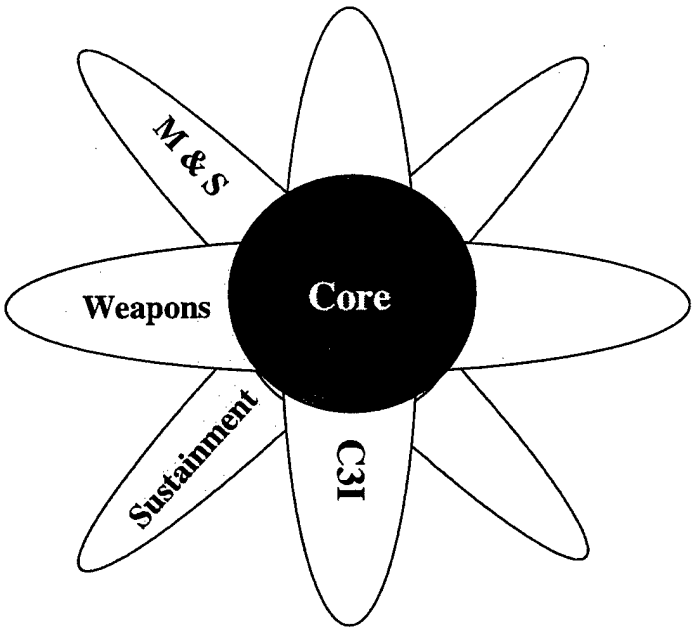


FIGURE 1-3 ARMY SYSTEM DOMAINS

There is only one DII COE. However, one specific COE implementation of software components and infrastructure cannot satisfy the requirements of all systems. The JTA-Army 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 (adds a domain standard to the main body set of standards). If a system relates to a domain, then **both** the core **and** domain

standards apply to that system. A lead agency for each domain, shown in parentheses below, has been designated to further develop each domain appendix.

1 Appendix D - Sustainment. (PEO-Standard Army Management Information System (STAMIS)).

2 Appendix E - C3I. (PEO-Command, Control, and Communications Systems (C3S)).

3 Appendix F - Weapons. (Weapon Systems Technical Architecture Working Group).

4 Appendix G - Modeling and Simulation. (Army Modeling and Simulation Office (AMSO)).

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

1 *Introduction* - This subsection is for information only. It provides background descriptions and definitions that are unique to the section.

2 *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 JTA-Army 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.

3 *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. This section also identifies areas where standards are still evolving or do not exist, but are critically needed.

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 and data links 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 JTA-Army. 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 JTA-Army. Therefore this section is structured to shadow the overall organization of the JTA-Army in order that readers can easily link security topics with the related subject area in the core sections of the JTA-Army.

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 JTA-Army 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 JTA-Army 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 Section 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 Environmant 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

Section 2 of the DII COE Version 3.1 Baseline Specification, describes the COE concept 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. Fundamental to the concept are segmentation and the use of public APIs. All systems that must be integrated into the DII shall implement the COE concept, segment their applications in accordance with the DII COE Integration, Runtime Specification Version 2.0, and use the DII COE 3.1 public APIs. The following standards are mandated:

- DII COE 3.1 Baseline Specification, 29 April 1997.
- DII COE Integration and Runtime Specification (I&RTS), Version 2.0, 23 October 1995.

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.

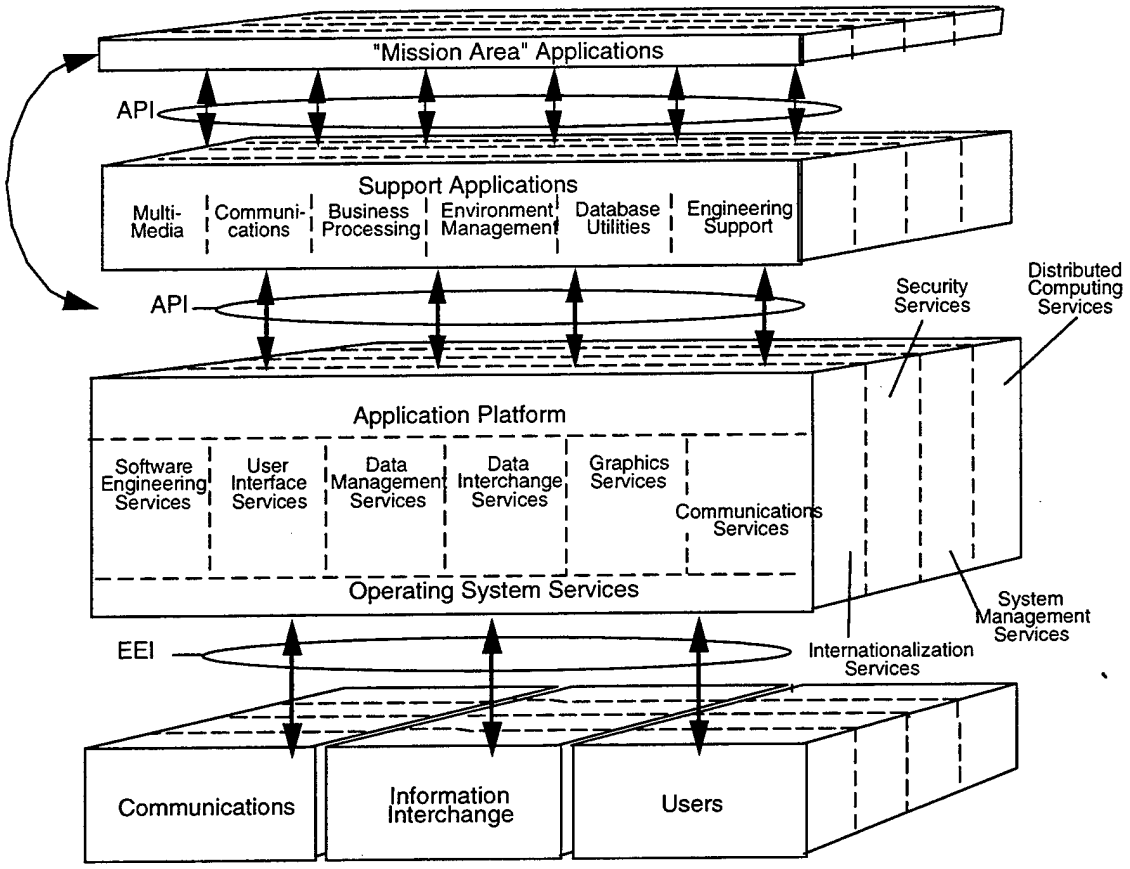


FIGURE 2-1 TAFIM TRM, VERSION 2.0

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.

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 system developers shall identify their common support applications and mission applications. Mission area applications shall transition to the DII COE common support applications to the maximum extent possible. The following mandates apply:

- DII COE 3.1 Baseline Specification, 29 April 1997.
- DII COE Integration and Runtime Specification (I&RTS), Version 2.0, 23 October 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.

According to DOD 5000.2-R, it is DOD policy to design and develop software based on software engineering principles. When selecting a third generation language (3GL) for custom development, developers should consider life cycle costs, code reuse and commercial software integration in conjunction with the specific software requirements of the system or application being developed. All 3GL coding shall adhere to the applicable language standard and avoid vendor extensions to the programming language. The mandated 3GL programming languages are Ada 95 and C. The following standards are mandated:

- ISO/International Electrotechnical Commission (IEC) 8652:1995 (Ada95), Ada Reference Manual, Language and Standard Libraries.

- ISO/International Electrotechnical Commission (IEC) 9899:1990, Programming languages -- C.
- ISO/IEC 9899/Cor. 1: 1994, Programming languages -- C, Technical Corrigendum 1.
- ISO/IEC 9899/Cor. 2: 1996, Programming languages -- C, Technical Corrigendum 2.
- ISO/IEC 9899/Amd. 1: 1995, Programming languages -- C, Amendment 1, C Integrity.

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. For applications developed in Ada, 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 JTA-Army 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 Common Desktop Environment (CDE) provides a common set of desktop applications and management capabilities for Unix user environments similar to the Microsoft Windows' 3.x Program Manager. CDE supports Open Software Foundation (OSF) Motif based application execution. Both CDE and Motif applications use the X Window System. Applications that require user interaction shall use Motif /X Window APIs and be capable of executing in the CDE. The following standards are mandated:

- 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 system (DBMS) services. DBMS services support the definition, storage,

and retrieval of data elements from monolithic and distributed DBMSs. Application code using Relational Database Management System (RDBMS) resources and COTS RDBMSs shall conform to the requirements of Entry Level SQL. For any system required to use a Relational Database Management System, the following standards are mandated:

- ISO/IEC 9075:1992 'Information Technology - Database Language - SQL' as modified by FIPS Pub 127-2:1993, Database Language for relational DBMSs. (Entry Level SQL).

In addition, the SQL/Call Level Interface (CLI) addendum to the SQL standard provides a standard CLI between database application clients and database servers. For both database application clients and database servers, the following standard is mandated:

- ISO/IEC 9075-3:1995 Information Technology - Database Languages - SQL - Part 3: Call Level Interface (SQL/CLI).

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 commerce data, video data, atmospheric data, and oceanographic data interchange services.

Message interchange standards are covered in Section 4.

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. The Standard Generalized Markup Language (SGML) format supports the production of documents which are intended for long-term storage and electronic dissemination for viewing in multiple formats. SGML formalizes document mark-up, making the document independent of the production and/or publishing system. SGML is an architecture-free and application-free language for managing structures and is designed for full multi-media database document publishing. The following standard is mandated:

- ISO 8879: 1986, Standard Generalized Markup Language (SGML).

For documents intended to be interchanged via the Worldwide Web (WWW), the following standard is mandated:

- Request For Comment (RFC)-1866: 1995, Hypertext Mark-up Language (HTML), Internet Version 2.0.

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 companies' 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 in Table 2-1 for the appropriate document type.

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.

2.2.2.1.4.2 Graphics Data Interchange

These services are supported by device-independent descriptions of picture element raster and vector graphics. Computer graphics are primarily either vector or raster based. The Computer Graphics Metafile format supports vector graphics. The ISO Joint Photographic Expert Group (JPEG) standard describes several alternative algorithms for the representation and compression of raster images, particularly for photographs. The JPEG standard does not specify an interchange format for JPEG images, which led to the development of the JPEG File Interchange Format (JFIF). CGM shall be used to

interchange vector graphics. JPEG and JFIF shall be used to interchange photographic images over the internet. The following standards are mandated:

- FIPS Pub 128-1, Computer Graphics Metafile (CGM).
- JPEG File Interchange Format (JFIF), Version 1.02, C-Cube Microsystems.
- ISO 10918-1: 1994, Joint Picture Expert Group (JPEG).

2.2.2.1.4.3 Geospatial Data Interchange

Geospatial services include mapping, charting, and geodesy information and services. The National Imagery and Mapping Agency (NIMA) (formally the Defense Mapping Agency (DMA) and the Central Imagery Office(CIO)) establish formats and produce raster-based digital products, such as Compressed Arc Digitized Raster Graphics (CADRG), Controlled Image Base (CIB), and Digital Point Positioning Data Base (DPPDB). NIMA is also responsible for vector-based products such as, 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+). The NIMA topographic Digital Terrain Elevation Data (DTED) level 1 and 2 data as well as other products such as the Digital Bathymetric Database (DBDB) are also provided by NIMA and are listed in Defense Mapping Agency List (DMAL) 805-1A. Fundamental to the interchange of military geographic location information is the use of the standard global reference system, World Geodetic System 84 (WGS-84). WGS-84 is employed by the NAVSTAR Global Positioning System (GPS) and modern weapons and systems. Latitude and longitude location data shall use WGS-84. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3900.01 provides guidance on the use of WGS-84. The following standards are mandated :

- MIL-STD-2411, Raster Product Format (RPF).
- MIL-STD-2407, Vector Product Format (VPF).
- MIL-D-89020, Digital Terrain Elevation Data (DTED).
- MIL-STD-2401, World Geodetic System 84 (WGS-84), 21 March 1994.

2.2.2.1.4.4 Imagery Data Interchange

The National Imagery Transmission Format Standard (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. For secondary imagery dissemination, the following standards are mandated:

- 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.
- American National Standards Institute (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. The Initial Graphics Exchange Specification (IGES) shall be used to interchange computer-aided design (CAD) data, such as technical illustrations and engineering drawings. The following standard is mandated:

- MIL-PRF-28000A, Initial Graphics Exchange Specification (IGES), Amendment 1, 14 December 1992.

2.2.2.1.4.6 Audio Data Interchange

Effective compression of audio data depends not only upon data compression techniques but also upon the application of a psycho-acoustic model that predicts which sounds humans are likely to be able to hear or not hear in given situations. The sounds selected for elimination depend on the bit rate available for streaming the audio data when the file is decoded and played. Therefore, the best selection of a file format depends upon the bandwidth assumed to be available on the platform that will decode the file. For audio files intended to be decoded in an environment with a target bit rate of about 56 to 64 kilobits per second (kbps) per audio channel, the following format is mandated.

- ISO/IEC 11172-3: 1993, Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Megabits per second (Mbits/s) --Part 3 (Audio Layer-3 only).
- ISO/IEC 11172-3/Cor. 1: 1996, Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s --Part 3: Audio Technical Corrigendum (Audio Layer-3 only).

[Note: Despite the title of the standard, the standard specified is for audio without associated video.]

2.2.2.1.4.7 Video Data Interchange

Video data interchange services provide combined audio and video services. The Motion Pictures Expert Group (MPEG), developed MPEG-1. 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 Megabits per second (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 audio portion of the MPEG-1 standard is not a single compression algorithm, but a family of three audio encoding and compression schemes called MPEG-Audio Layer-2, and Layer-3 which are all hierarchically compatible. The audio compression schemes are lossy, but they can achieve perceptually lossless quality. 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.
- ISO/IEC 11172-3: 1993 - Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s --Part 3: Audio.
- ISO/IEC 11172-3/Cor. 1: 1995 - Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s --Part 3: Audio Technical Corrigendum.

MPEG-2 is designed for the encoding, compression, and storage of studio-quality motion video and multiple CD-quality audio channels (up to five full bandwidth channels (left, right, center, and two surround sound), an additional low-frequency enhancement channel, and up to seven commentary or multilingual 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.
- ISO 13818-3: 1995 - Generic Coding of Moving Pictures and Associated Audio Information - Part 3: Audio.

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. Gridded Binary (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.

Besides being used for the transfer of data, Binary Universal Format for Representation (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. 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.
- FM 94-X-BUFR - The WMO Binary Universal Format for Representation (BUFR) of meteorological data.
- Data Exchange Format (DEF) - Appendix 30 to the Tactical Automated Weather Distribution System (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 standard is mandated:

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

2.2.2.1.4.10 File Compression

Compression of files is a method of reducing files thereby reducing file storage and transfer resource consumption. For general purpose interchange of files among different platforms and organizations, a platform-independent file compression format is useful. Unless another more specific mandated compression format is used (e.g. JIFF), the following compressed file format is mandated.

- RFC-1952, GZIP File Format Specification, Version 4.3, 23 May 1996.

2.2.2.1.4.11 Electronic Commerce Data Interchange

These services are used to create an electronic environment (paperless) for the interchange of data with commercial industry during electronic commerce/ electronic data interchange operations (EC/EDI). FIPS Pub 161-1, defines the interchange format for

documents that are highly structured (e.g., consisting of a sequence of numeric or alphanumeric fields rather than free-form text). The following standard is mandated:

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

Refer to Section 4.2.4 for additional requirements on message standards.

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 Graphics Kernel System (GKS) provides 2-D graphics services. The Programmers Hierarchical Interactive Graphics System (PHIGS) provides 3-D graphics services. The following standards are mandated:

- ISO 7942:1991, Graphics Kernel System (GKS), as profiled by FIPS Pub 120-1 (change notice 1).
- ISO 9592: 1989, Programmers Hierarchical Interactive Graphics Systems (PHIGS), as profiled by FIPS Pub 153.

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 the 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. See Section 2.2.2.1.1.2 for language bindings to the operating system. The following standards are mandated:

- ISO/IEC 9945-1:1996, Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 1: System Application Program Interface (API), (as profiled by FIPS PUB 151-2: 1994).
- ISO 9945-2: 1993, Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 2: Shell and Utilities, (as profiled by FIPS Pub 189-1).
- IEEE 1003.2d:1994, Information Technology--Portable Operating System Interface for Computer Environments (POSIX)-Part 2: Shell and Utilities - Amendment 1: Batch Environment.

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 JTA-Army. 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.

2.2.2.2.4 Distributed Computing Services

These services allow various tasks, operations, and information transfers to occur on multiple, physically or logically-dispersed, computer platforms. These services include, but are not limited to, global time; data, file, and name services; thread services; and remote process services. There are two categories of Distributed Computing Services, Remote Procedure Computing, and Distributed Object Computing.

2.2.2.2.4.1 Remote Procedure Computing

The mandated standards for remote procedure computing are the Distributed Computing Environment (DCE) version 1.1 standards promulgated by the Open Group. The use of DCE Interface Definition Language (IDL) (included in the cited Open Group standards) is also mandated to specify public, DCE-based, Application Programming Interfaces (APIs).

- Open Group CAE Specification C309, DCE: Remote Procedure Call which includes DCE IDL, August 1994.

- Open Group CAE Specification C310, DCE 1.1: Time Services Specification, November 1994.
- Open Group CAE Specification C312, DCE: Directory Services, December 1994.

2.3 EMERGING STANDARDS

2.3.1 DII COE

The Army is committed to the COE concept and will mandate DII COE 4.0 APIs as they become stable. Draft I&RTS Version 3.0 is an emerging standard for code segmentation rules.

2.3.2 Service Area Standards

Within the Software Engineering Services area, the Draft ISO WG21/ANSI X3J16 "Programming Language C++", 2 December 1996 is an emerging standard.

Within the User Interface Services area, Common Desktop Environment (CDE) version 2.1 is an emerging standard.

Within Data Interchange Services, HTML 3.2 for the interchange of Hyper-text electronic documents and associated embedded navigational links via the World Wide Web is expected to be mandated once approved by the Internet Engineering Task Force (IETF), and implemented in commercial and free-ware products. For the interchange of line-art graphic files, the Portable Network Graphics (PNG) Specification, Version 1.0, World Wide Web Consortium, 1 October 1996 is an emerging standard awaiting wider spread implementation in commercial products. In the area of image data interchange, wavelet image compression techniques are still being reviewed for inclusion in the NITFS imaging standard. For the interchange of full motion video and associated audio at data rates of 1.5Mbps - 6.0 Mbps, ISO 13818-4, MPEG-2 is an emerging standard. For the interchange of Audio at low bit rates, MPEG-4 is an emerging standard.

Within Operating System Services, it is expected that the following draft POSIX standards will be adopted once they become final and products are available. IEEE P1003.5B Ada Bindings for Real-Time Extensions, P1003.1D Real-Time Extensions, P1003.1H Services for Reliable, Available, Serviceable Systems, P1003.1G Protocol Independent Interfaces, P1003.2L Real-Time Distributed Systems Communication, and P1003.1J Advanced Real-Time Extensions. In addition, the X/Open Single UNIX Specification (SUS) (previously referred to as Specification 1170) is an emerging standard.

Within the User Interfaces Services and the Operating System Services, the Win32 APIs are emerging standards that allow use/reuse of COTS/GOTS products on X86 platforms.

Within Distributed Computing Services' Distributed Object Computing service area, the emerging Object Management Group (OMG) standards include the Common Object Request Broker Architecture (CORBA) 2.0 and associated CORBA Facilities and

Services specifications. OMG is awaiting the approval and release of a branding test suite.

Within Data Management Services, the emerging standard is the draft DIS 9075-4, Database Language SQL, Part 4: Persistent Stored Modules (SQL/PSM). For object oriented database services, SQL3 under development by the ANSI X3H2 committee and the ODMG-9x standard being developed by the Object Database Management Group (ODMG) are emerging standards.

This page was intentionally left blank.

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 JTA-Army 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 3.2.1.1. Router standards are specified in Section 3.2.2.1. Within the Open Systems Interconnection (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 OSI reference model. Network standards are specified in Section 3.2.2.

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 JTA-Army uses the STD nomenclature.

The JTA-Army 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 End System Standards

This subsection addresses standards for the following types of end systems: host, Video Teleconferencing (VTC), facsimile, and secondary imagery dissemination.

3.2.1.1 Host Standards

Internet Architecture Board (IAB) Standard-3 is an umbrella standard that references other documents and corrects errors in some of the referenced documents. Standard-3 also adds additional discussion and guidance for implementors. The following standard is mandated:

- IAB Standard 3/RFC-1122/RFC-1123, Host Requirements, October 1989.

3.2.1.1.1 Application Support Services

3.2.1.1.1.1 Electronic Mail

The standard for electronic mail is the Defense Message System (DMS)'s X.400-based suite of military messaging standards as defined in Allied Communication Publication (ACP) 123, and the U.S. Supplement No. 1. The U.S. Supplement annexes contain standards profiles for the definition of the DMS "Business Class Messaging" (P772) capability and the Message Security Protocol (MSP). See Section 6 for security standards. Since X.400 is not an internet standard, see 3.2.1.1.2.2 for operation over Internet Protocol (IP) based networks. The following standard is mandated:

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

For interoperability with non-DMS electronic mail, the following standards are also mandated:

- RFC-821, Simple Mail Transfer Protocol, 1 August 1982.
- RFC-822, Standard for the format of ARPA Internet text messages, 13 August 1982.

3.2.1.1.1.2 Directory Services

X.500 and Domain Name System (DNS) provide complimentary directory services. The X.500 protocol provides individual and organizational directory services and is mandated for use with DMS. The DNS provides computer addressing services and is mandated for Internet Protocol (IP)-based services.

3.2.1.1.1.2.1 X.500 Directory Services

International Telecommunications Union (ITU) X.500 provides directory services that may be used by users or host applications to locate other users and resources on the network. X.500 also provides security services used by DMS-compliant X.400 implementations. See Section 6 for security standards. Since X.500 is not an internet standard, see Section 3.2.1.1.2.2 for operation over Internet Protocol (IP) based networks. The following standard is mandated:

- ITU-T X.500, The Directory - Overview of Concepts, Models, and Services - Data Communication Networks Directory, 1993.

3.2.1.1.1.2.2 Domain Name System (DNS)

The DNS provides the service of translating between host names and IP addresses. DNS uses Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) as a transport service when used in conjunction with other services. The following standard is mandated:

- IAB Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987.

3.2.1.1.1.3 File Transfer

Basic file transfer shall be accomplished using File Transfer Protocol (FTP). FTP provides a reliable, file transfer service for text or binary files. FTP uses TCP as a transport service. The following standard is mandated:

- IAB Standard 9/RFC-959, File Transfer Protocol, October 1985, with the following FTP commands mandated for reception: Store unique (STOU) and Abort (ABOR).

3.2.1.1.1.4 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. The following standard is mandated:

- IAB Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983.

3.2.1.1.1.5 Network and Systems Management

Refer to Section 3.2.5.

3.2.1.1.1.6 Network Time

Network Time Protocol (NTP) provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet. The following standard is mandated:

- RFC-1305, Network Time Protocol (V3), 9 April 1992.

3.2.1.1.1.7 Bootstrap Protocol (BOOTP)

BOOTP assigns an IP address to workstations with no IP address. The following standards are mandated:

- RFC-951, Bootstrap Protocol, September 1, 1985.
- RFC-1533, Dynamic Host Configuration Protocol (DHCP) Options and BOOTP Vendor Extensions, October 8, 1993.
- RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, October 27, 1993.

3.2.1.1.1.8 Dynamic Host Configuration Protocol (DHCP)

DHCP provides an extension of BOOTP to support the passing of configuration information to Internet hosts. DHCP consists of two parts, a protocol for delivering host-specific configuration parameters from a DHCP server to a host, and a mechanism for automatically allocating IP addresses to hosts. DHCP uses UDP as a transport service. The following standard is mandated:

- RFC-1541, Dynamic Host Configuration Protocol, October 27, 1993.

3.2.1.1.1.9 World Wide Web (WWW) Services

3.2.1.1.1.9.1 Hypertext Transfer Protocol (HTTP)

HTTP is used for search and retrieval within the WWW. HTTP uses TCP as a transport service. The following standard is mandated:

- RFC-1945, Hypertext Transfer Protocol -- HTTP/1.0, May 17, 1996.

3.2.1.1.1.9.2 Uniform Resource Locator (URL)

A URL specifies the location of and access methods for resources on an internet. The following standards are mandated:

- RFC-1738, Uniform Resource Locators, December 20, 1994
- RFC-1808, Relative Uniform Resource Locators, June 14, 1995.

3.2.1.1.2 Transport Services

The transport services provide host-to-host communications capability for application support services. The following sections define the requirements for this service.

3.2.1.1.2.1 Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) over Internet Protocol (IP)

3.2.1.1.2.1.1 Transmission Control Protocol (TCP)

TCP provides a reliable connection-oriented transport service. The following standard is mandated:

- IAB Standard 7/RFC-793, Transmission Control Protocol, September 1981. In addition, TCP shall implement the PUSH flag and the Nagle Algorithm, as defined in IAB Standard 3.

3.2.1.1.2.1.2 User Datagram Protocol (UDP)

UDP provides an unacknowledged, connectionless, datagram transport service. The following standard is mandated:

- IAB Standard 6/RFC-768, User Datagram Protocol, August 1980.

3.2.1.1.2.1.3 Internet Protocol (IP)

IP is a basic connectionless datagram service. All protocols within the IP suite use the IP datagram as the basic data transport mechanism. The following standard is mandated:

- IAB Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112, Internet Protocol, September 1981. In addition, all implementations of IP must pass received Type-of-Service (TOS) values up to the transport layer. Two other protocols are considered integral parts of IP: the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP). ICMP is used to provide error reporting, flow control, and route redirection. IGMP provides multicast extensions for hosts to report their group membership to multicast routers.

3.2.1.1.2.2 Open Systems Interconnection (OSI)/Internet Interworking Protocol

This protocol provides the interworking between Transport Protocol Class 0 (TP0) and TCP transport service necessary for OSI applications to operate over IP-based networks. The following standard is mandated:

- IAB Standard 35/RFC-1006, ISO Transport Service on top of the TCP, May 1978.

3.2.1.2 Video Teleconferencing (VTC) Standards

VTC terminals operating at data rates of 56-1,920 kilobits per second (kb/s) 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 for telephony applications. Additional ITU-T ratified standards, which supplement and/or displace the standards in VTC001-Rev1, are mandated for those VTC systems implementing the multimedia applications.

The following is mandated for VTC terminals operating at data rates of 56-1,920 kb/s:

- VTC001-Rev1, Industry Profile for Video Teleconferencing, Revision 1, 25 April 1995.
- ITU-T H.221, Frame Structure for a 64 to 1,920 kbit/s Channel in Audiovisual teleservices, July 1995.
- ITU-T H.321, Adaptation of H.320 Visual Telephone Terminals to B-ISDN Environments, March 1996.
- ITU-T H.224, A Real Time Control Protocol for Simplex Applications using the H.221 LSD/HSD/MLP channels , November 1994.
- ITU-T H.281, A Far-End Camera Protocol for Videoconferences Using H.224, November 1994.
- ITU-T H.244, Synchronized Aggregation of Multiple 64 or 56 kb/s channels, July 1995.

For VTC terminals operating at low bit rates (9.6-28.8 kbps) the following is mandated:

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

For VTC applications implementing the features of audiographic conferencing, facsimile, still image transfer, annotation, pointing, shared whiteboard, file transfer, and audio-visual control, the following standards are mandated:

- ITU-T T.120, Data Protocols for Multimedia Conferencing, July 1996.
- ITU-T T.122, Multipoint Communication Service for Audiographics and Audiovisual Conferencing Service Definition, March 1993.
- ITU-T T.123, Protocol Stacks for Audiographic and Audiovisual Teleconference Applications November 1994.
- ITU-T T.124, Generic Conference Control, August 1995.
- ITU-T T.125, Multipoint Communication Service Protocol Specification, April 1994.
- ITU-T T.126, Multipoint Still Image and Annotation Protocol, August 1995.

- ITU-T T.127, Multipoint Binary File Transfer Protocol, August 1995.

For Picture Format Resolution, the video CODEC shall provide full-color operation using at least the Quarter Common Intermediate Format (QCIF) in accordance with ITU H.261. If a resolution of 325 (horizontal) by 228 (vertical) or higher is required for motion video, the standard algorithm of ITU-T H.261 shall be supported at Full Common Intermediate Format (FCIF) resolution. The following standard is mandated:

- ITU-T H.261, Video CODEC for Audiovisual Services at p x 64 kbit/s, March 1993.

To support the coding and decoding of audio, the following standards are mandated:

- ITU-T G.711, Pulse Code Modulation (PCM) of Voice Frequencies, 1988.
- ITU-T G.728, Coding of Speech at 16 kbits/s Using Low-Delay Code Excited Linear Prediction (LD-CELP), September 1992.

3.2.1.3 Facsimile Standards

3.2.1.3.1 Analog Facsimile Standard

Facsimile requirements for analog output shall comply with ITU-T Group 3 specifications. The following standards are mandated:

- Telecommunications Industry Association (TIA)/Electronics Industries Association (EIA)-465-A, Group 3 Facsimile Apparatus for Document Transmission, 21 March 1995.
- TIA/EIA 466, Procedures for Document Facsimile Transmission, May 1981.

3.2.1.3.2 Digital Facsimile Standard

Digital facsimile terminals operating in tactical, high Bit Error Rate (BER) environments shall implement digital facsimile equipment standards for Type I and/or Type II mode. Also, facsimile transmissions requiring encryption, or interoperability with NATO countries, shall use the digital facsimile standard. All secure facsimile transmissions shall use MIL-STD-188-161D. MIL-STD-188-161D is currently the minimum essential standard for secure facsimile transmissions for joint and NATO interoperability. The following standard is mandated:

- MIL-STD-188-161D, Interoperability and Performance Standards for Digital Facsimile Equipment, 10 January 1995.

3.2.1.4 Secondary Imagery Dissemination Standards

Refer to Appendix E.3.2.2.1.1.

3.2.1.5 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. The following standard is mandated:

- ASD Memorandum Development, Procurement, and Employment of DoD Global Position System User Equipment, 30 April 1992.

3.2.2 Network Standards

3.2.2.1 Router Standards

Routers are used to interconnect various subnetworks and end systems. Protocols necessary to provide this service are specified below. RFC-1812 is an umbrella standard that references other documents and corrects errors in some of the reference documents. In addition, some of the standards that were mandated for hosts in Section 3.2.1.1 also apply to routers. The following standards are mandated:

- RFC-1812, Requirements for IP Version 4 Routers, June 22, 1995.
- IAB Standard 6/RFC-768, User Datagram Protocol, August 1980.
- IAB Standard 7/RFC-793, Transmission Control Protocol, September 1981.
- IAB Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983.
- IAB Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987.
- IAB Standard 15/RFC-1157, Simple Network Management Protocol, May 1990.
- IAB Standard 16/RFC-1155/RFC-1212, Structure of Management Information, May 1990.
- IAB Standard 17/RFC-1213, Management Information Base, March 1991.
- RFC-951, Bootstrap Protocol, September 1, 1985.
- RFC-1533, DHCP Options and BOOTP Vendor Extensions, October 8, 1993.
- RFC-1541, DHCP, October 27, 1993.
- RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, October 27, 1993.
- IAB Standard 33/RFC-1350, Trivial FTP (TFTP), July 1992, to be used for initialization only.

Security requirements are addressed in Section 6.

3.2.2.1.1 Internet Protocol (IP)

IP 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. The following standard is mandated:

- IAB Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112, Internet Protocol, September 1981. Two other protocols are considered integral parts of IP, the Internet Control Message

Protocol (ICMP) and the Internet Group Management Protocol (IGMP). ICMP is used to provide error reporting, flow control, and route redirection. IGMP provides multicast extensions for hosts to report their group membership to multicast routers.

3.2.2.1.2 IP Routing

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

3.2.2.1.2.1 Interior Routers

Routes within an autonomous system 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 unicast interior gateway routing and Multicast OSPF (MOSPF) for multicast interior gateway routing. The following standards are mandated:

- RFC-1583, Open Shortest Path First Routing Version 2, March 23, 1994, for unicast routing.
- RFC-1584, Multicast Extensions to OSPF, March 24, 1994, for multicast routing.

3.2.2.1.2.2. Exterior Routers

Exterior gateway protocols are used to specify routes between autonomous systems. Routers shall use the Border Gateway Protocol 4 (BGP-4) for exterior gateway routing. BGP-4 uses TCP as a transport service. The following standards are mandated:

- RFC-1771, Border Gateway Protocol 4, March 21, 1995.
- RFC-1772, Application of BGP-4 In the Internet, March 21, 1995.

3.2.2.2 Subnetworks

3.2.2.2.1 Ethernet

Ethernet is the most common network technology available. Data is transmitted at 10 Mbps (or 100 Mbps for higher speed requirements) over a cable that 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 six different types of cable.

Ethernet's physical layer and CSMA/CD access scheme are specified in the following mandated standard:

- ISO/IEC 8802-3: 1996 (E) (ANSI/IEEE Std 802.3, 1996 edition) Local Area Network (LAN)/MAN CSMA/CD Access Method Standards Package, which includes 10Base-5 (Thick Coaxial), 10Base-2 (Thin Coaxial), 10Base-T (Unshielded Twisted Pair), 10Base-F (Fiber-Optic Cable), 100Base-T, and 100Base-F.
- Ethernet V2 framing shall be used instead of 802.2 framing on Ethernet LANs.

Bridging (or switching) among Ethernet LAN segments shall comply with the following mandated standard:

- ISO/IEC 10038: 1993 (ANSI/IEEE Std 802.1D, 1993 Edition) Information technology-Telecommunications and information exchange between systems-Local area networks-Media access control (MAC) bridges.

The interface between Ethernet and IP shall be in accordance with the following mandated standards:

- IAB STD 37/RFC-826, An Ethernet Address Resolution Protocol, November 1982.
- IAB STD 41/RFC-894, Standard for the Transmission of IP Datagrams Over Ethernet Networks, April 1984.

Platforms that must physically connect to a Joint Task Force Local Area Network shall, at a minimum, support ISO/IEC 8802-3 using a 10Base-T connection, IAB STD 37 and IAB STD 41.

Ethernet management shall be in accordance with the following mandated standard:

- ISO/IEC 15802-2 : 1995 (ANSI/IEEE Std 802.1B, 1995 Edition) Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks - Common specifications-Part 2: LAN/MAN management (ANSI).

3.2.2.2.2 Point to Point Standards

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-1989, PPP Link Quality Monitoring, August 1996.
- RFC-1994, PPP Challenge Handshake Authentication Protocol (CHAP), August 1996.
- RFC-1570, PPP Link Control Protocol (LCP) Extensions, January 11, 1994.
- RFC-1990, The PPP Multilink Protocol, August 96.

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

- Electronics Industries Association's (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.)

3.2.2.2.3 Combat Net Radio (CNR) Networking

CNRs are a family of radios that allow voice or data communications for mobile users. These radios provide a half-duplex, broadcast transmission media with potentially high BERs. The method by which IP packets are encapsulated and transmitted is specified in MIL-STD-188-220A. 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 following standard is mandated:

- MIL-STD-188-220A, Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, July 27, 1995.

3.2.2.2.4 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 following standards are mandated:

For the BRI Physical Layer:

- ANSI T1.601 ISDN Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT (Layer 1 Specification), 1992.

For the PRI Physical Layer:

- ANSI T1.408, ISDN Primary Rate - Customer Installation Metallic Interfaces (Layer 1 Specification), 1990.

For the Data Link Layer:

- ANSI T1.602, Data Link Signaling Specification for Application at the User Network Interface, 1996.

For Signaling at the User-Network Interface:

- ANSI T1.607, Digital Subscriber Signaling System No. 1 - Layer 3 Signaling Specification for Circuit Switched Bearer Service, 1990.
- ANSI T1.607a, Supplement, 1996.
- ANSI T1.610, DSS1 - Generic Procedures for the Control of ISDN Supplementary Services, 1994.
- ANSI T1.619, Multi-Level Precedence and Preemption (MLPP) Service, ISDN Supplementary Service Description, 1992.
- ANSI T1.619a, Supplement, 1994.

The above Signaling at the User-Network Interface ANSI mandates shall be as profiled by the following National ISDN documents as adopted by the North American ISDN Users' Forum (NIUF):

- SR-3875, National ISDN 1995, 1996, and 1997, Bellcore.

- SR-3888, 1997 Version of National ISDN Basic Rate Interface Customer Premise Equipment Generic Guidelines, Bellcore.
- SR-3887, 1997 Version of National ISDN Primary Rate Interface Customer Premise Equipment Generic Guidelines, Bellcore.

For transmitting IP packets using Point-to-Point Protocol (PPP) over ISDN:

- RFC-1618, PPP over ISDN, May 94.

Note: It should be recognized that deployable systems might be required to additionally support other non-North American ISDN standards when accessing region-specific international infrastructure for ISDN services.

3.2.2.2.5 Asynchronous Transfer Mode (ATM)

ATM is a high speed switched data transport technology that takes advantage of primarily low bit error rate transmission media to accommodate intelligent multiplexing of voice, data, video, imagery, and composite inputs over high-speed trunks and dedicated user links.

ATM is a layered type of transfer protocol with the individual layers consisting of an ATM Adaptation Layer (AAL), the ATM layer, and the Physical Layer. The function of the AAL layer is to segment variable length data units into 48-octet cells, reassemble the data units, and perform error checking. The ATM Layer adds the necessary header information to allow for recovery of the data at the receiver end. The Physical Layer converts the cell information to the appropriate electrical/optical signals for the given transmission medium. AAL5 shall be used to support variable rate service. AAL1 shall be used to support constant bit rate service, which is sensitive to cell delay, but not cell loss. IP packets shall be transported over AAL5 in accordance with Lane 1.0.

The ATM Forum's User-Network Interface (UNI) Specification 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.

The Private Network-Network Interface (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.

Ethernet can be emulated by ATM Networks allowing ATM Networks to be deployed without disruption of host network protocols and applications.

The following standards are mandated:

For the Physical Layer:

- ATM Forum's 25.6 Mb/s Over Twisted Pair Cable Physical Interface, af-phy-0040.000.
- Physical Interface Specifications found in Section 2 of ATM Forum's User-Network Interface (UNI) Specification, Version 3.1, af-uni-0010.002, September 94.

- ATM Forum's DS1 Physical Layer Specification, af-phy-0016.000.
- ATM Forum's DS3 Physical Layer Interface Specification, af-phy-0054.000.

For the User to Network Interface:

- ATM Forum's User-Network Interface (UNI) Specification, Version 3.1, af-uni-0010.002, September 94.
- ATM Forum's Integrated Local Management Interface (ILMI) Specification, Version 4.0, af-ilmi-0065.000, September 96.
- ATM Forum's ILMI Management Information Base (MIB) for UNI 3.1, af-uni-0011.001.
- ATM Forum's UNI Signaling Specification, Version 4.0, af-sig-0061.000, July 96.
- ATM Forum's Traffic Management Specification, Version 4.0, af-tm-0056.000, April 96.
- ANSI T1.630 ATM Adaptation Layer for Constant Bit Rate (CBR) Services Functional and Specification, (i.e. AAL1), 1993.
- ANSI T1.635 ATM Adaptation Layer Type 5, Common Part Functions and Specifications, 1994 which adopts ITU-T I.363 Section 6 (i.e. AAL5).

For Private Network to Network Interfaces:

- ATM Forum's Private Network to Network Interface (PNNI) Specification, Version 1.0, af-pnni-0055.000, March 1996.
- ATM Forum's PNNI V1.0 Addendum, af-pnni-0066.000.

For Local Area Network Emulation and IP Over ATM:

- ATM Forum's Local Area Network Emulation (LANE) Over ATM, Version 1.0., af-lane-0021.000.
- ATM Forum's LAN Emulation Client Management Specification, af-lane-0038.000.
- ATM Forum's LANE 1.0 Addendum, af-lane-0050.000.
- ATM Forum's LANE Servers Management Spec v1.0, af-lane-0057.000.

3.2.2.2.6 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. The following standards are mandated

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

For DTEs, ISO 7776 shall be used at the data link layer and ISO 8208 shall be used at the packet layer. The following standards are mandated:

- 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.

At the physical layer, the X.25 interface shall comply with one of the following mandated standards. The following standards are mandated:

- 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.)

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. The following standards are mandated:

- RFC-1356, Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode, August 1992.
- ACCS-A3-407-008D, Interface Specification for the Army Data Distribution System (ADDS) Interface.
- ANSI X3.100, Interface between DTE and DCE for Operation with PSDN, or between Two DTEs, by Dedicated Circuit, 1989.
- ANSI X3.100a, Supplement to ANSI X3.100, 1991.

3.2.2.2.7 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 following standards are mandated:

- ISO 9314-1, Fibre Distributed Data Interface (FDDI) - Pt 1: Token Ring Physical Layer (PHY).
- ISO 9314-2 (media access control), 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).
- ANSI X3.229, Fibre Distributed Data Interface (FDDI) - Station Management (SMT).

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. The following standards are mandated

- IEEE 802.2, Local and Metropolitan Area Networks, Part 2: Logical Link Control, 1994.
- STD-36/RFC-1390. Transmission of IP and ARP over FDDI Networks, January 1993.

3.2.3 Transmission media

3.2.3.1 Military Satellite Communications (MILSATCOM)

Refer to Appendix E.3.2.2.3.1.

3.2.3.2 Radio Communications

Refer to Appendix E.3.2.2.3.2.

3.2.3.3 Synchronous Optical Network (SONET) Transmission Facilities

The Synchronous Optical Network (SONET) is a telecommunications transmission standard for use over fiber-optic cable. SONET is the North American subset of the ITU standardized interfaces, and includes a hierarchical multiple structure, optical parameters, and service mapping. When utilizing SONET Transmission Facilities, the following standards are mandated:

- ANSI T1.105, Telecommunications - Synchronous Optical Network (SONET) Basic Description Including Multiplex Structure, Rates, and Formats (ATIS) (Revision and Consolidation of ANSI T1.105-1991 and ANSI T1.105A-1991), 1995.
- ANSI T1.107, Digital Hierarchy - Formats Specifications, 1995.
- ANSI T1.117, Digital Hierarchy - Optical Interface Specifications (SONET) (Single Mode - Short Reach), 1991.
- ANSI T1.101, Telecommunications - Synchronization Interface Standard, 1994.

Note: It should be recognized that deployable systems may be required to support, in addition to SONET, other non-SONET telecommunications transmission standards when accessing region-specific international infrastructure.

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 JTA-Army.

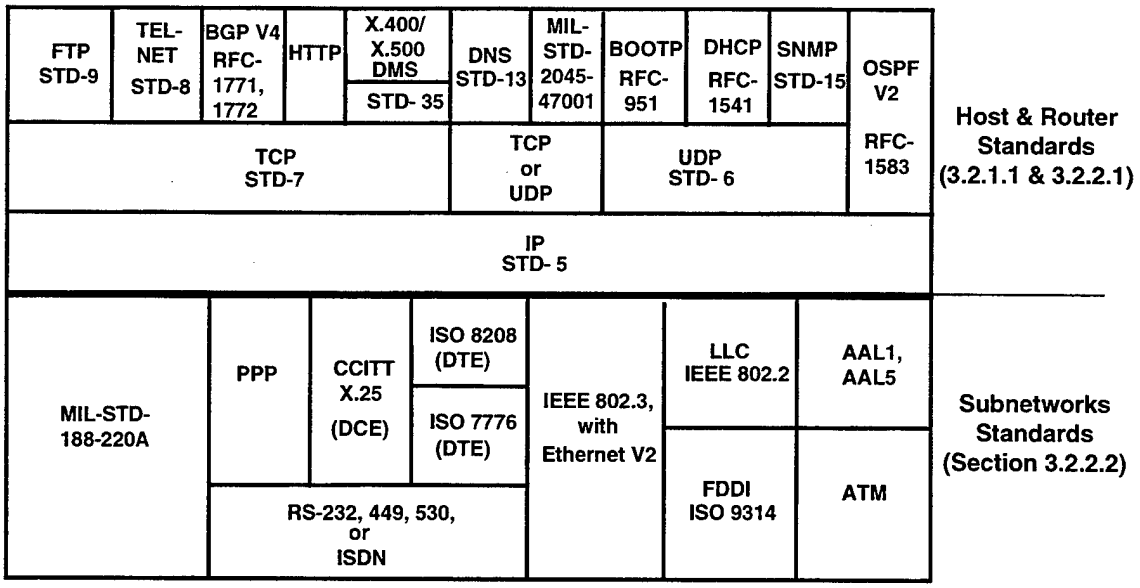


FIGURE 3-1. SUMMARY OF THE PACKET-SWITCHED TRANSFER STANDARDS

3.2.5 Network and Systems Management

Network and Systems Management (NSM) provides the capability to manage designated networks, systems, and information services. This includes controlling the network's topology; dynamically segmenting the network into multiple logical domains; maintaining network routing tables; monitoring the network load; and making routing adjustments to optimize throughput. NSM also provides the capability to review and publish addresses of network and system objects; monitor the status of objects; start, restart, reconfigure, or terminate network or system services; and detect loss of network or system objects in order to support automated fault recovery. A management system has four essential elements: management stations; management agents; management information bases (MIBs); and management protocols, to which these standards apply.

3.2.5.1 Data Communications

Management stations and management agents (in end systems and networked elements) shall support the Simple Network Management Protocol (SNMP). The following SNMP-related standard is mandated:

- IAB Standard 15/RFC-1157, Simple Network Management Protocol (SNMP), May 1990.

To standardize the management scope and view of end systems and networks, the following standards for MIB modules of the management information base are mandated:

- IAB Standard 16/ /RFC-1212, Structure of Management Information, May 1990.
- IAB Standard 17/RFC-1155/RFC-1213, Management Information Base, March 1991.

- RFC-1514, Host Resources MIB, September 1993.
- STD-50/RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994.
- RFC-1757, Remote Network Monitoring Management Information Base, (RMON Version 1), February 1995.
- RFC-1850, Open Shortest Path First (OSPF) Version 2 Management Information Base, November 1995.

3.2.5.2 Telecommunications

Management systems for telecommunications voice switches will implement the Telecommunications Management Network (TMN) framework. To perform information exchange within a voice telephony network, the following Telecommunications Management Network framework standards are mandated:

- ANSI T1.204, OAM&P - Lower Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements, 1993.
- ANSI T1.208, OAM&P - Upper Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements, 1993.
- ITU-T M.3207.1, TMN management service: maintenance aspects of B-ISDN management, 1996.
- ITU-T M.3211.1, TMN management service: Fault and performance management of the ISDN access, 1996.
- ITU-T M.3400, TMN Management Functions, 1992.
- ISO/IEC 9595 Information Technology-Open Systems Interconnection Common Management Information Services, December 1991.
- ISO/IEC 9596-1:1991 Information technology -- Open Systems Interconnection -- Common Management Information Protocol (CMIP) -- Part 1: Specification.
- ISO/IEC 9596-2:1993 Information technology -- Open Systems Interconnection -- Common Management Information Protocol: Protocol Implementation Conformance Statement (PICS) proforma.

3.3 EMERGING STANDARDS

Commercial communications standards and products will evolve over time. The JTA-Army 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 JTA-Army, but are expected to be adopted in the near future.

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 - Draft VTC001-Rev2 is updated by Draft FIPS Pub 178-1 and its Appendix A. T.128, Audio Visual Control for Multipoint Multimedia Systems, and T.130, High Level Audio Visual Control are draft standards pending approval. While approved in November 1996 by the ITU, H.323 is not yet mandated for VTC terminals employed in a LAN environment.

ITU-T Recommendation H.310, " Broadband Audiovisual Communication Systems and Terminals", ratified November 1996, is an umbrella standard for video-conferencing over high bandwidth (ATM) communication links. H.310 includes underlying standards for: video (MPEG1 and MPEG2, refer to Section 2.2.2.1.4.7), multiplexing (H.222/0 and H.222/1, still under development), and control/signaling (H.245 still under development). It is expected that, when the underlying standards are completed, H.310 will be mandated for VTC requiring > 2 Mbps infrastructure.

Hypertext Transfer Protocol (HTTP/1.1) - HTTP/1.1 is specified by Proposed Standard RFC-2068. This protocol includes more stringent requirements than in the mandated RFC-1945 for HTTP/1.0, to improve reliability. Several open issues need to be resolved before it becomes a Draft Standard.

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.

Network Management Systems for Data Communications - The following SNMP MIB modules are identified as emerging standards for implementation within systems that manage data communications networks:

(1) Asynchronous Transfer Mode (ATM) MIB, RFC-1695 - defines a set of standard objects for managing ATM switches.

(2) Border Gateway Protocol version 4 (BGP-4) MIB, RFC-1657 - defines a set of standard objects for managing this internetwork routing protocol.

(3) Domain Name Service (DNS) MIBs, RFCs 1611 and 1612 - define a set of standard objects for managing this name server and name resolver services.

(4) Fiber-optic Data Distribution Interface (FDDI) MIBs, RFCs 1285 and 1512 - define a set of standard objects for managing FDDI rings.

(5) Internetwork Protocol (IP) MIBs, RFCs 2006 and 2011 - define a set of standard objects for managing this traditional static IP and emerging mobile IP services.

(6) Point-to-Point Protocol (PPP) MIBs, RFCs 1471 through 1474 - define a set of standard objects for managing PPP links, security, IP network level, and bridge level services.

(7) Remote Network Management Monitoring Version 2 (RMON2) MIB, RFC-2021 - defines a set of standard objects for monitoring protocol communications services across a subnetwork of all seven layers of the OSI model.

(8) Transmission Control Protocol (TCP) MIB, RFC-2012 - defines a set of standard objects for managing a systems TCP services.

(9) User Datagram Protocol (UDP) MIB, RFC-2013 - defines a set of standard objects for managing a systems UDP services.

(10) X.25 MIBs, RFCs 1381, 1382, and 1461 - define a set of standard objects for managing network layer and data link layer services.

(11) X.500 MIB, RFC-1567 - defines a set of standard objects for monitoring X.500 directory services.

ATM Standards - (1) BTD-VTOA-LLT-01 - *Voice and Telephone over ATM - ATM Trunking for Narrow Band Services* (March 1997). This specification is currently out for

a letter ballot. It is expected to be published in the summer of 1997. (2) STR-MPOA-MPOA-01.00 - *Multiprotocol over ATM* (February 1997). The specification should have a letter ballot by the end of 1997.

ATM Conformance Testing - ATM Forum's conformance test suites, Protocol Information Conformance Statement (PICS) pro forma and the Protocol Implementation Extra Information for Testing (Pixit) pro forma, are available to demonstrate interoperability between vendor products.

Ethernet Virtual LANs (VLANs) - The draft IEEE 802.1Q specifies multi-switch Ethernet VLANs and will allow the Army to deploy multi-switch VLANs in a non-proprietary manner. In the Ethernet switching context, a VLAN is a bridging domain created by Ethernet switches connecting Ethernet segments.

Secondary Imagery Dissemination - In Section 2.2.2.1.4.4, the NITFS suite of standards is mandated for the exchange, storage, and transmission of digital imagery products. For secondary imagery dissemination, the NITFS suite also includes the Tactical Communications protocol 2 (TACO2) for use when native transfer protocols do not exist or are too inefficient. TACO2 is currently used for NITFS transfer across half-duplex and simplex, point-to-point, tactical radio circuits, but is incompatible with IP router-based networks that adhere to the mandated standards in Section 3. Tactical Communications protocol 3 (TACO3), a new tactical bulk transfer protocol stack based on TACO2 technology but compatible with the mandated standards, has been developed and tested, and is currently available as sample software from the National Imagery and Mapping Agency (NIMA). TACO3 will permit the transmission of imagery (or other large files) over bandwidth limited networks. TACO3 uses a variant of the same key protocol, NETwork BLock Transfer (NETBLT), that controls TACO2. A draft RFC for this version of NETBLT was prepared and submitted by NIMA in May 1997, to the Internet Engineering Steering Group/Internet Engineering Task Force (IESG/IETF) as an internet draft.

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 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. Activity 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 activities, products, and interfaces. A function (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 activity and data models. Interface models are customized to fit a particular project; hence system developers should create and use interface models as necessary.

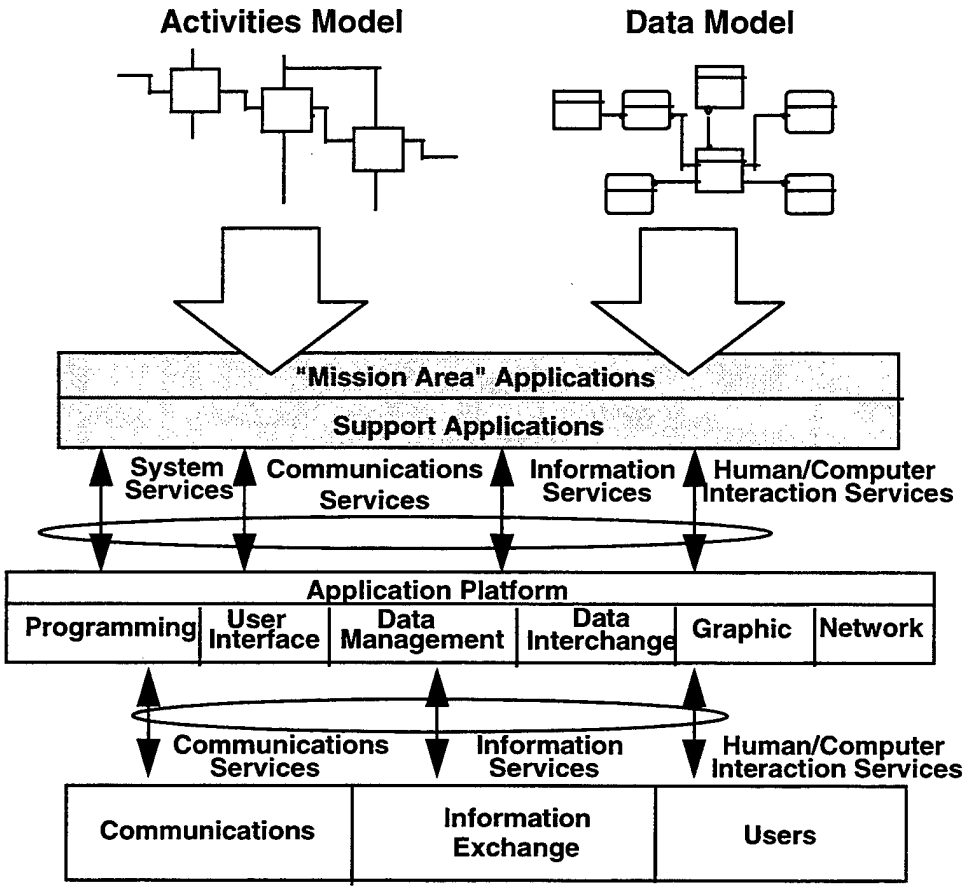


FIGURE 4-1. RELATIONSHIP OF TAFIM TO INFORMATION STANDARDS

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 Activity 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 activities 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 primarily 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), that 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 activity 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.

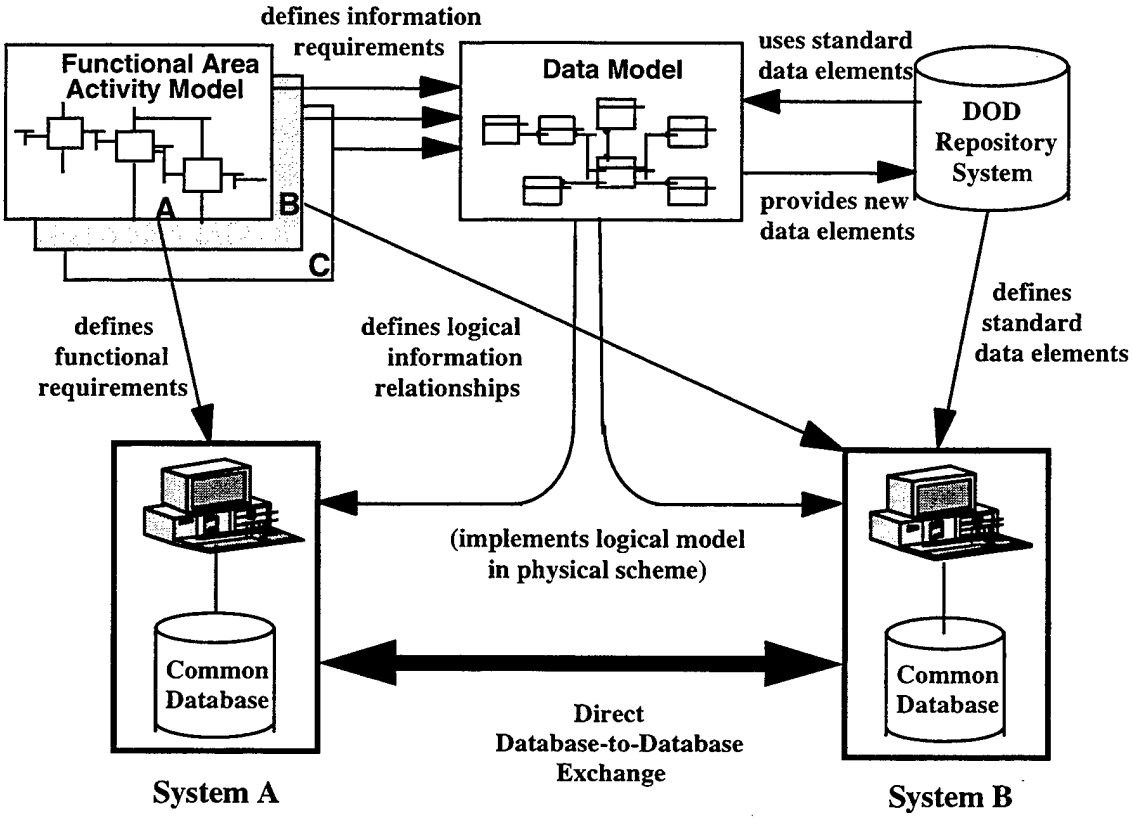


FIGURE 4-2. OBJECTIVE INFORMATION EXCHANGE ARCHITECTURE

4.2 MANDATES

4.2.1 Activity 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 all data entities. 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 Interim IDEF Repository (currently managed by DISA) shall be used as a reference for extending activity models for specific programs. The following standard is mandated:

- FIPS Pub 183, Integration Definition for Function Modeling (IDEF0).

The doctrinally based activity 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 activity models. The activity model will be enhanced and refined to accommodate the increased knowledge inherent in system development. An approved activity model, created by the materiel developer and coordinated with the combat developer, can support criteria for Milestone II and III decisions.

As activity models are developed, security levels shall be considered. Most activity models are unclassified even if the content of one or more activity characteristics (see inputs, controls, outputs, and mechanisms (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 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 meta data and modeling elements for all DOD. New information requirements are derived by using information from both the data models and activity models. The new information requirements are then approved through the use of the DOD Data Standardization Program (Department of Defense Directive (DODD) 8320 Series) and will then be used to extend the DDM and C2CDM. The C2 Core Data Model can be down loaded from the DDDS server. Message format will be in Section 4 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 following standards are mandated:

- FIPS Pub 184, Integration Definition For Information Modeling (IDEF1X), December 1993.

- DOD Defense Data Model (DDM).
- C2 Core Data Model (C2CDM) - tactical systems.
- DODD 8320 Series, DOD Data Standardization Program.

The data models, and associated activity models which provide context information, shall be used in software requirement 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 and a fully attributed data model will be prepared prior to Milestone II or equivalent decision. 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 (DODD) 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. The following references and standards are mandated:

- DDDS.
- DODD 8320.1, Data Administration.
- DOD 8320.1-M-1, DOD Data Standardization Procedures.

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 function 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 Connectionless Data Transfer

Variable Message Format (VMF) Messages shall use a connectionless application layer. The following standard is mandated:

- MIL-STD-2045-47001, Connectionless Data Transfer Application Layer Standard, July 27,1995.

4.2.4.3 US Message Text Format (USMTF) Messages

USMTF messages are jointly agreed, fixed-format, character-oriented messages that are man-readable and machine-processable. 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). The following standard is mandated:

- MIL-STD-6040, United States Message Text Format (USMTF) (formerly JCS Publication 6-04).

4.2.4.4 Tactical Digital Information Link (J Series) Messages

The J-Series Family of TDLs allows 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 includes LINK 16, 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. For information exchange, the following standards are mandated:

- MIL-STD-6016 - Joint Tactical Information Distribution System (JTIDS) Technical Interface Design Plan - (TIDP).

- STANAG 5516, Edition 1, Tactical Data Exchange - LINK 16, Ratified 2 March 1990.
- VMF Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 1 February 1995.

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.

4.2.4.6 Database to Database Exchange

The following is mandated:

- Database to Database Exchange shall use standard data elements from the DDDS.

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).

4.2.6 Calendar Date Data Format

In order to ensure the unambiguous exchange of date data between systems before, during, and past the year 2000, database design and data modeling shall adhere to the DOD Classword value structure and specifications for the term "Date". In addition, system developers shall ensure that this standard data structure is incorporated into all external interfaces of their systems where there is a requirement to exchange calendar date information. For external exchange of character calendar dates by systems not using a standardized message (i.e. USMTF) or transaction (i.e. EC/EDI) format, the following standard is mandated.

- YYYYMMDD (from the CLASS Word "DATE" in the DDDS, and ISO 8601, Date/Time Representations).

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 that 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 that represents the 1995 baseline version to which all non-standard joint interoperability messages are to adhere. (An emerging 1998 version is expected to replace the 1995 version.)

The Joint VMF Technical Interface Design Plan, Reissue 3, which includes additions required by the Fire Support and the Force XXI Battle Command Brigade and Below (FBCB2) communities, is currently under development at JIEO and is scheduled for release in 2Q98.

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 Section 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 HCIs used by different applications and systems 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 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. In order to present a consistent interface to the user, graphical and character-based application user interface styles should not be mixed within an application.

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 Section 5.2.2.1. Hybrid GUIs shall not be created. A hybrid GUI is a GUI that is composed of tool kit components from more than one user interface style. An example of a hybrid GUI would be one that uses tool kit components from both Motif TM and Windows. When selecting Commercial Off-The-Shelf (COTS)/Government Off-The-Shelf (GOTS) applications for integration with previously developed automated systems, maintaining consistency in the user interface is highly recommended.

- Mandates as stated above are contained in Section 5.2.2.1, D.5.2.2.1 and G.5.2.2.1.

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*. The following standard is mandated:

- 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

The following standard is mandated:

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

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

- Refer to Section 6 for HCI security standards.

5.2.2 Style Guides

An HCI style guide is a document that specifies design rules and guidelines for the look and behavior of the user interaction with a software application or a family of software applications. The goal of a style guide is to improve human performance and reduce operator training requirements by ensuring consistent and useable design of the HCI across software modules, applications, and systems. The style guide represents "what" user interfaces should do in terms of appearance and behavior, and can be used to derive HCI design specifications which define "how" the rules are implemented in HCI application code.

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 interactive prototype-based HCI development. The process starts with top-level general guidance and uses prototyping activities to develop system-specific design rules.

The interface developer shall use the following documents as well as input from human factors specialists, to create the system-specific HCI.

- MIL-STD-1472E, Human Engineering Design Criteria for Military Systems, Equipment and Facilities, 31 October 1996.
- DOD HCI Style Guide.
- Selected commercial GUI style guide.
- Appropriate domain-level style guide.

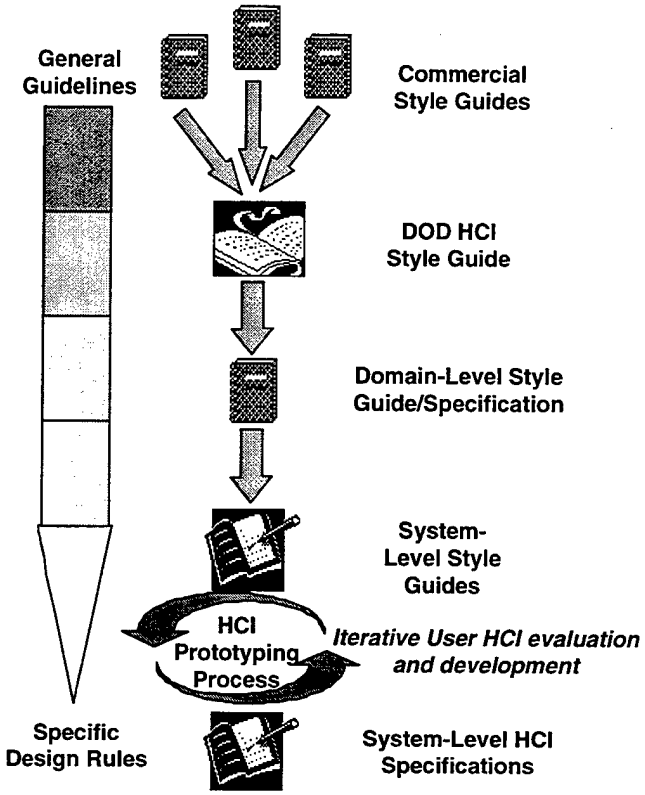


FIGURE 5-1. HIERARCHY OF STYLE GUIDES

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).

For Motif TM based systems, the following standard is mandated:

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

OSF/Motif TM is a non-proprietary interface style that supports the DOD goal for an open systems environment.

When Common Desktop Environment (CDE) is used for desktop management, the user interface "look and feel" shall be based on and consistent with the CDE version of Motif TM. The CDE version of Motif TM provides significant convergence in "look and feel" with Microsoft Windows.

Use of non-commercial GUI styles is addressed in Section 5.2.1.1.

5.2.2.2 DOD HCI Style Guide

The DOD HCI Style Guide, is a high-level document that allows consistency across DOD Systems without undue constraint on domain and system-level implementation. Volume 8

of the TAFIM, the *DOD HCI Style Guide* 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.*

The following standard is mandated:

- DOD HCI Style Guide, TAFIM Version 3.0, Volume 8, 30 April 1996.

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 hand-held devices or 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. For example, the C3I domain has adopted the *User Interface Specifications for the Defense Information Infrastructure (DII)* and 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 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.

Until a domain develops its domain-level style guide the following are mandated:

- DOD HCI Style Guide, TAFIM Version 3.0, Volume 8, 30 April 1996.
- 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 STANDARDS

The JTA-Army 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-1472E is being revised to incorporate extensive technical updates and is expected to be reissued as MIL-STD-1472F in 1998.

Common Desktop Environment (CDE) 2.1 incorporates the Motif 2.1 Graphical User Interface. The Motif 2.1 style guide will be mandated when CDE 2.1 is mandated.

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.

Related to Commercial Style Guides, the emerging Windows interface guidelines would allow use/reuse of COTS/GOTS products on X86 platforms.

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 JTA-Army. Therefore this section is structured to mirror the structure of the JTA-Army itself with security standards organized corresponding to each JTA-Army 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 JTA-Army. 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.

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.

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 JTA-Army, 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 JTA-Army 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 JTA-Army can also be used to assess the relevance of standards that can be met with evaluated commercial and government-provided components and protocols. The JTA-Army 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

This section contains the information systems security standards and protocols that shall be implemented in systems that have a need for the corresponding interoperability-related services. If a service is to be implemented in a C4I system, then it shall be implemented at the required level of protection using the associated security standards in this section. If a service is provided by more than one standard, the appropriate standard should be selected based on system requirements.

6.2.1 Mandated Standards

Technical evaluation criteria to support information system security policy, and evaluation and approval, disapproval, and accreditation responsibilities are promulgated

by DOD Directive (DODD) 5200.28. Based on the required level of trust, the following information processing security standards are mandated.

6.2.1.1 Application Software Entity

The following standards are mandated for the development and acquisition of application software consistent with the required level of trust:

- DOD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985.
- NCSC-TG-021, Version 1, Trusted Database Management System Interpretation, April 1991.

If DMS services are used, the following are mandated:

- MD4002101-1.52, FORTEZZA Application Implementors' Guide, 5 March 1996.
- MD4000501-1.52, FORTEZZA Cryptologic Interface Programmers' Guide, 30 January 1996.

6.2.1.2 Application Platform Entity

For security auditing or alarm reporting, the following standard is mandated:

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

Authentication supports tracing security-relevant events to individual users. The following standard is mandated:

- FIPS PUB 112, Password Usage, National Institute of Standards and Technology (NIST), 30 May 1985.

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

Host end system security standards include security algorithms, security protocols, and evaluation criteria. The first generation FORTEZZA Cryptographic Card and its successor the Type I Card (formerly known as FORTEZZA Plus) are designed for protection of information in messaging and other applications. 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.

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 [C Language], Draft 15 (reballot March 1996) and IEEE P1003.2c, POSIX Part 2: Shell and Utilities - Protection and Control Interfaces, Draft 15 (reballot March 1996). These draft standards define security interfaces to open systems for access control lists, audit, privilege, mandatory access control, and information label mechanisms and are stated in terms of their C bindings.

6.2.2.2.1 Security Alarm Reporting:

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 for 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 Authentication Security Standards

RFC-1938, A One-Time Password System, provides authentication for system access (login) and other applications requiring authentication that is secure against passive attacks based on replaying captured reusable passwords. The One-Time Password System evolved from the S/KEY One-Time Password System that was released by Bellcore.

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. The Internet Draft "GSS-API, Version 2," J. Linn, 20 February 1996, draft-ietf-cat-gssv2-05.txt revises RFC-1508, making specific, incremental changes in response to implementation experience and liaison requests.

The Internet Draft, "Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)," C. Adams, 18 February 1996, draft-ietf-cat-idup-gss-04.txt, 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. An example application is secure electronic mail where data needs to be protected without any on-line connection with the intended recipient(s) of that data. Subsequent to being protected, the data unit

can be transferred to the recipient(s) - or to an archive - perhaps to be processed as unprotected only days or years later.

6.2.2.5 Security Management Protocols

Progress toward approval of SNMP V2 has been slow and not likely to be adopted. SNMP V3 is not yet mature enough to be considered as an emerging standard. In the meantime CMIP has been adopted by many developers for the management of circuit-switched systems. Information concerning the CMIP can be found in: 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). It is envisioned that a future Network and System Management standard will incorporate features of both SNMP and CMIP for packet-switched and circuit-switched environments respectively. A key management protocol standard can be found in: 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 Multilevel Information System Security Initiative (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 emerging standard may be appropriate: 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 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). For messaging, key management, and security protocols, the following standards are mandated:

- MIL-STD-2045-18500, Message Handling System (MHS) Message Security Protocol(MSP) Profile, Parts 1-5, October 1993.

- SDN.903, revision 3.2, Secure Data Network System (SDNS) Key Management Protocol (KMP), 1 August 1989.
- SDN.301, revision 1.5, Secure Data Network System (SDNS) Security Protocol 3 (SP3), 1989.

Additionally, MISSI recently added the following as its identification and authentication (I&A) protocol. The following standard is mandated:

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

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

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

6.3.1.2 DMS Interface

If FORTEZZA services are used due to an interface with the Defense Message System (DMS),the following standards apply:

- MD4002101-1.52, FORTEZZA Application Implementor's Guide, 5 March 1996.
- MD4000501-1.52, FORTEZZA Cryptologic Interface Programmer's Guide, 30 January 1996.

6.3.1.3 MISSI Cryptographic Algorithms

The FORTEZZA Card includes a CAPSTONE chip containing a time stamping capability and four algorithms. For these algorithms, the following standards are mandated:

- FIPS PUB 180-1, Secure Hash Algorithm, 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).
- R21-Tech-23-94, NSA-developed Type II Key Exchange Algorithm (KEA), NSA, 12 July 1994.

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). The following standards are mandated:

- FORTEZZA Crypto Card ICD, Version P1.5, 22 December 1994.
- FORTEZZA Plus Crypto Card ICD, Release 3.0, 01 June 1995.

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

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

6.3.1.4 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. The following standards are mandated:

- ITU-T Rec. X.500 (ISO/IEC 9594-1) Directory Infrastructure that is DMS compliant.
- ITU-T Rec. X.509 Version 3 (ISO/IEC 9594-8.2), The Directory: Authentication Framework, 1993, that is DMS compliant.

6.3.1.5 Transport Mechanisms

For interpretations of network standards and criteria, the following standard is mandated:

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

6.3.2 Emerging Standards

6.3.2.1 Security Association Management

The following Integrated Services Digital Network (ISDN) security protocol is emerging: ISDN Security Program (ISP)-421, Revision 1.0: The ISP Security Association Management Protocol (SAMP), 15 May 1994.

6.3.2.2 Secure World Wide Web (WWW) Transactions

The draft IETF Transport Layer Security Protocol (TLSP) V1, dated 24 March 1997 incorporates the Netscape proprietary Secure Sockets Layer (SSL) protocol V3.0, dated 18 November 1996. The TLSP provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

6.3.2.3 Networking Security Standards

The following emerging standards are being considered for standardization: (1) Security Architecture for the Internet Protocol (RFC-1825), (2) IP Authentication Header (RFC-1826), with IP Authentication using Keyed MD5 (RFC-1828), (3) IP Encapsulating Security Payload (ESP) (RFC-1827), with The ESP DES-CBC Transform (RFC-1829), (4) IEEE 802.10, IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS), IEEE, 1992, (5) IEEE 802.10a, Standard for Interoperable LAN Security-The Model, IEEE, Draft Jan 1989, and (6) IEEE 802.10b, Standard for Interoperable LAN Security-Part B: Secure Data Exchange, IEEE, 1992.

The following ATM specification, BTD-Security-01, ATM Security Specification (April 1997), is emerging as the only possibility for an ATM security standard at this time. The

specification is not complete (due September 1997) and has not been studied by the security working group due to its immaturity.

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

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.

Extensions for interpersonal messaging can be found in the following ISO: 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.

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.

TABLE 6-1 NOTIONAL MAPPING OF PROTOCOLS AND SECURITY STANDARDS

Layer	Common Protocols		Security Standards/Protocols
Application Presentation Session	Interactive Session: Connection Oriented dialup FTP PPP/SLIP Setup rlogin Telnet	M	DOD 5200.28-STD (Orange Book)
		M	FIPS PUB 180-1 (Secure Hash Standard)
		M	FIPS PUB 185 (Escrowed Encryption Standard)
		M	FIPS PUB 186 (Digital Signature Standard)
		M	FIPS PUB 196 (Entity Auth. Using Public Key Crypto.)
		M	ITU X.509 v3 (Directory Auth. Framework)
		M	KMP (Key Management Protocol)
		M	RFC 1510 (Kerberos)
		E	GSS API (Generic Security Services API, RFC 1508)
		E	IEEE 802.10C (SILS Part c-Key Management)
		E	ISP-421/94.05.15 rev 1 (Sec Assoc Mgmt Protocol)
		E	RFC 1938 (One-Time Password System)
		E	TLSP "formerly SSL (Secure Socket Layer)"
	Non-Session: Connectionless Dir Server Access E-Mail EDI WWW	M	DOD 5200.28-STD (Orange Book)
		M	FIPS PUB 180-1 (Secure Hash Standard)
		M	FIPS PUB 185 (Escrowed Encryption Standard)
		M	FIPS PUB 186 (Digital Signature Standard)
		M	FIPS PUB 196 (Entity Auth. Using Public Key Crypto.)
		M	FORTEZZA (Interface Control Document)
		M	FORTEZZA Plus (Interface Control Document)
		M	ITU X.509 v3 (Directory Auth. Framework)
		M	KMP (Key Management Protocol)
		M	MD4000501-1.52 (FORTEZZA Crypto. Prog. Guide)
		M	MD4002101-1.52 (FORTEZZA Appl. Imple. Guide)
		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	TLSP "formerly SSL (Secure Socket Layer)"
		E	TSIX(RE) 1.1 (Trstd Sec Info Ex Restricted Envir.)
Transport Network	ATM TCP/IP UDP X.25	E	ISP-421/94.05.15 rev 1 (Sec Assoc Mgmt Protocol)
		E	NLSP (SP3) (Network Layer Security Protocol)
		E	RFC 1825 (IP Security Architecture)
		E	RFC 1826 (IP Authentication Header)
		E	RFC 1827 (IP Encapsulating Security Payload)
		E	RFC 1828 (IP Authentication using Keyed MD5)
		E	RFC 1829 (ESP DES-CBC Transform)
		E	SILS (Standards for Interoperable LAN Security)
		E	TLSP (SP4) (Transport Layer Security Protocol)
		E	BTD Security-01-ATM (ATM Security Spec.)
Data Link Physical	ATM Ethernet FDDI IEEE 802.3 X.25	E	ISP-421/94.05.15 rev 1 (Sec Assoc Mgmt Protocol)
		E	SDE (Secure Data Exchange)
		E	SILS (Standards for Interoperable LAN Security)
		E	SP2 (Security Protocol Layer 2)
Media	ATM RF		No current security standards

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

6.4.1 Mandated Standards

None mandated at this time.

6.4.2 Emerging Standards

Emerging standards are: (1) ISO/IEC 10165 Series, Information Technology - Open Systems Interconnection- Structure of Management Information - Parts 1- 4, 1993 - 1994, and (2) 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

For security banners and screen labels, the following standard is mandated:

- Department of Defense (DOD), 1994b, Department of Defense Human-Computer Interface Style Guide, TAFIM (Version 3.0), Volume 8, 30 April 1996.

6.5.2 Emerging Standards

6.5.2.1 Entity Authentication

An entity authentication emerging standard is: 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

A personal authentication emerging standard is 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 following standard applies as stated above:

- 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.

This page was intentionally left blank.

APPENDIX A - ACRONYMS

AAE	Army Acquisition Executive
AAL	ATM Adaptation Layer
ABOR	Abort
ACP	Allied Communication Publication
ACR	American College of Radiology
ACT	Advanced Concept and Technology
ACTD	Advanced Concept Technology Demonstration
ADDS	Army Data Distribution System
ADO	Army Digitization Office
ADPCM	Adaptive Differential Pulse Code Modulation
AEP	Application Environment Support
AIS	Automated Information Systems
AJ	Anti-Jam
ALSP	Aggregate Level Simulation Protocol
AMC	Army Materiel Command
AMSO	Army Modeling and Simulation Office
ANSI	American National Standards Institute
API	Application Programming Interface
AR	Army Regulation
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
BER	Bit Error Rate
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
bps	bits per second
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

CBR	Constant Bit Rate
CBS	Commission for Basic Systems
CCITT	International Telephone and Telegraph Consultative Committee (now ITU-T)
CDE	Common Desktop Environment
CDMA	Code Division Multiple Access
CFS	Center for Standards
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
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CLI	Call Level Interface
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
COS	Corporation for Open Systems
COTS	Commercial Off-The-Shelf
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
DAA	Designated Approving Authority
DAMA	Demand Assigned Multiple Access
DBDB	Digital Bathymetric Database
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
DICOM	Digital Imaging and Communication in Medicine
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
DMAL	Defense Mapping Agency List
DMS	Defense Message System
DMTD	Digital Message Transfer Device
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
EC	Electronic Commerce
EDI	Electronic Data Interchange
EEI	External Environment Interface
EHF	Extremely High Frequency
EIA	Electronics Industries Association
ESC	Electronic Systems Command
ESP	Encapsulating Security Payload
FBCB2	Force XXI Battle Command Brigade and Below
FCIF	Full Common Intermediate Format
FDDI	Fiber Distributed Data Interface
FDB	Functional Description of the Battlespace
FDMA	Frequency Division Multiple Access
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
HL7	Health Level 7
HQDA	Headquarters Department of the Army
HRI	Human readable interpretation
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
ICC	Integrated Circuit Chip
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
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IGES	Initial Graphics Exchange Specification
IGMP	Internet Group Management Protocol
ILMI	Integrated Local Management Interface
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
JTA-Army Joint Technical Architecture - Army
JTDLMP Joint Tactical Data Link Management Plan
JTIDS Joint Tactical Information Distribution System

kbits kilobits
kbps kilobits per second
kb/s kilobits per second
KEA Key Exchange Algorithm
kHz kilo-Hertz
KMP Key Management Protocol

LAN Local Area Network
LCP Link Control Protocol
LD-CELP Low-Delay Code Excited Linear Prediction
LDR Low Data Rate
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
MDR Medium Data Rate
MHS Message Handling System
Mhz Megahertz
MIB Management Information Base
MIDS Multifunctional Information Distribution System
MIL-HDBK Military Handbook
MILSATCOM Military Satellite Communications
MIL-STD Military Standard
MISSI Multilevel Information System Security Initiative
MLPP Multi-Level Precedence and Preemption
MMP MISSI Management Protocol
MOSPF Multicast OSPF
MPEG Motion Pictures Expert Group
MSMP Modeling and Simulation Master Plan
MSP Message Security Protocol

NCSC	National Computer Security Center (see NSA)
NEMA	National Electrical Manufacturers Association
NES	Network Encryption System
NETBLT	NETwork BLock Transfer
NIMA	National Imagery and Mapping Agency
NIST	National Institute of Standards and Technology
NITF	National Imagery Transmission Format
NITFS	National Imagery Transmission Format Standard
NIUF	North American ISDN Users' Forum
NLSP	Network Layer Security Protocol
NSA	National Security Agency
NSM	Network and Systems Management
NTP	Network Time Protocol
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
OMCSR	Object Model Content Standards Repository
OMG	Object Management Group
OML	Object Model Library
OOA	Object Oriented Analysis
OOM	Object-oriented methods (OOM
OOP	Object Oriented Programming
OOT	Object Oriented Technology
OOTW	Operations-Other-Than-War
ORD	Operational Requirements Document
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OSJTF	Open Systems Joint Task Force
OSPF	Open Shortest Path First
PC	Personal Computer
PCM	Pulse Code Modulation
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Services
PDF	Portable Data File
PDU	Protocol Data Unit
PEO	Program Executive Office
PHIGS	Programmers Hierarchical Interactive Graphics System
PHY	Physical Layer
PICMG	PCI Industrial Computer Manufacturer's Group

PICS	Protocol Implementation Conformance Statement
Pixit	Protocol Implementation Extra Information for Testing
PM	Program/Product Manager
PMD	Physical Layer Medium Dependent
PNG	Portable Network Graphics
PNNI	Private Network-Network Interface
POSIX	Portable Operating System Interface
PPP	Point-to-Point Protocol
PPS	Precise Position Service
PRI	Primary Rate Interface
PSK	Phase Shift Keying
PSM	Persistent Stored Modules
PSTN	Public Switched Telephone Network
PTTI	Precise Time and Time Interval
QCIF	Quarter Common Intermediate Format
RDBMS	Relational Database Management System
RDT&E	Research, Development, Test & Evaluation
RF	Radio Frequency
RFC	Request for Comment
RMON	Remote Network Management Monitoring
RPC	Remote Procedure Calls
RPF	Raster Product Format
RS	Recommended Standard
RT/NRT	Real-Time/Near-Real-Time
SA	Systems Architecture
SAE	Society of Automotive Engineers
SAMP	Security Association Management Protocol
SATCOM	Satellite Communications
SCQL	Structured Card Query Language
SCSI	Small Computer Systems Interface
SDNS	Secure Data Network System
SDTS	Spatial Data Transfer Standard
SEA	Strategic Enterprise Architecture
SEDRIS	Synthetic Environment Data Representation Interchange Specification
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SHF	Super High Frequency
SIF	Standard Simulator Data Base (SSDB) Interchange Format
SILS	Standard for Interoperable LAN Security
SISO	Simulation Interoperability Standards Organization
SME	Standard Electronic Module

SMIB	Security Management Information Base
SMP	Symmetrical Multi-processing
SMT	Station Management
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SP3	Security Protocol at Layer 3
SQL	Structured Query Language
SSDB	Standard Simulator Data Base
SSL	Secure Sockets Layer (of HTTP)
STAMIS	Standard Army Management Information System
STANAG	Standardization Agreement
STD	Standard
STOU	Store Unique
SUS	Single UNIX Specification
TA	Technical Architecture
TACO2	Tactical Communications Protocol 2
TACO3	Tactical Communications Protocol 3
TAFIM	Technical Architecture Framework for Information Management
TAWDS	Tactical Automated Weather Distribution System
TCP	Transmission Control Protocol
TCSEC	Trusted Computer Security Evaluation Criteria
TDMA	Time Division Multiple Access
TEED	Tactical End-to-End Encryption Device
TELNET	Telecommunications Network
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TIDP	Technical Interface Design Plan
TIDP-TE	Technical Interface Design Plan - Test Edition
TIS	Technical Interface Specifications
TLSP	Transport Layer Security Protocol
TMN	Telecommunications Management Network
TOS	Type-of-Service
TP0	Transport Protocol Class 0
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
UHF	Ultra High Frequency

UNI	User-Network Interface
URL	Uniform Resource Locator
USACE	Army Corps of Engineers
USD A&T	Under Secretary of Defense for Acquisition and Technology
USMC	United States Marine Corps
USMTF	United States Message Text Format
USS	Uniform Symbology Specification
UVMap	Urban Vector Map
VHDL	VHSIC Hardware Description Language
VITD	Vector Interim Terrain Data
VLAN	Virtual LANs
VMap	Vector Map
VMap AD	VMap Aeronautical Data
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
WWSS	Warfare and Warfare Support System
WWW	World Wide Web
3GL	Third Generation Language

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

DMAL 805-1A, DMA List of Products and Services, March 1994

DOD 5000.37H, Buying Commercial & Nondevelopmental Items: A DRAFT Handbook, April 1996

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

DODD 5000.59, DoD Modeling and Simulation Management, 4 January 1994

DODD 8320 Series, DOD Data Standardization Program

DODD 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), Amendment 1, 14 December 1992

MIL-STD-1295, Vertical Situation Displays And Electronic Attitude Director Indicators For Rotary-Wing Aircraft

MIL-STD-1389D, Standard Electronic Module (SME)

MIL-STD-1472E, Human Engineering Design Criteria for Military Systems, Equipment and Facilities, 31 October 1996

MIL-STD-1553B, Standard for Medium Speed System Network Bus

MIL-STD-1582, EHF LDR Uplinks and Downlinks, 10 December 1992

MIL-STD-1787, Aircraft Display Symbology

MIL-STD-1821, Standard Simulator Data Base (SSDB) Interchange Format (SIF) Design Standard

MIL-STD-188-110A, Data Modems, Interoperability and Performance Standards, 30 September 1991

MIL-STD-188-136, EHF MDR Uplinks and Downlinks, 26 August 1995

MIL-STD-188-141A, Medium and High Frequency Radio Equipment Standard, 10 September 1993

MIL-STD-188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment, 28 July 1992

MIL-STD-188-148A, Interoperability Standard Anti-Jam (AJ) Communication HF Band (2-30 Mhz), 18 March 1992

MIL-STD-188-161D, Interoperability and Performance Standards for Digital Facsimile Equipment, 10 January 1995

MIL-STD-188-182, Interoperability Standard for 5 kHz UHF DAMA Terminal Waveform, 18 September 1992

MIL-STD-188-183, Interoperability Standard for 25 kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992

MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993

MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995

MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995

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-188-242, Tactical Single Channel (VHF) Radio Equipment, 20 June 1985

MIL-STD-188-243, Tactical Single Channel (UHF) Radio Communications, 15 March 1989

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

MIL-STD-1773, Fiber Optics Mechanization of an Aircraft Internal Time Division Command/Response Multiplex Data Bus

MIL-STD-2045-18500, Message Handling System Message Security Protocol (MSP) Profile, Parts 1-5, October 1993

MIL-STD-2045-44500, National Imagery Transmission Format Standard (NITFS) Tactical Communications Protocol 2 (TACO2), 18 June 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-6016 - Joint Tactical Information Distribution System (JTIDS) Technical Interface Design Plan - (TIDP)

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

SSDCB79S4000 - JTIDS System Segment Specification (Class 2 Terminal) (SECRET)

STANAG 4175, Edition 1, 29 August 91 - Technical Characteristics of the Multifunctional Information Distribution System (MIDS)

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

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

(No Number) Defense Data Dictionary System (DDDS)

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

(No Number) DII COE Version 3.1 Baseline Specification, 29 April 1997

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

(No Number) DOD Defense Data Model (DDM)

(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 3.0, Defense Information Systems Agency Center for Standards, 30 April 1996

(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) GLOSSARY: Defense Acquisition Acronyms and Terms, 1996

(No Number) HLA Management Plan, Version 1.6, 17 July 1995

(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) 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 Department of Defense (DOD) Modeling and Simulation Master Plan (MSMP)

(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

(No Number) VMF Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 1 February 1995

B.1.2 Army References

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

AR 5-11, Management of Army Models and Simulations (draft), December 1996

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

FM 101-5-1, Operational Terms and Graphics

(No Number) Army Model and Simulation Master Plan

(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) Department of the Army Technical Architecture, Version 4.5, 12 November 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 112, Password Usage, National Institute of Standards and Technology (NIST), 30 May 1985

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 151-2, Portable Operating System Interface (POSIX) - System Application Program Interface [C Language], 12 May 1993

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 173, Spatial Data Transfer Standard (SDTS), 10 June 1994

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, Portable Operating System Interface (POSIX) -- Part 2: Shell and Utilities, 11 October 1994

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 T1.101-1994, Telecommunications - Synchronization Interface Standard

ANSI T1.105, Telecommunications - Synchronous Optical Network (SONET) Basic Description Including Multiplex Structure, Rates, and Formats (ATIS) (Revision and Consolidation of ANSI T1.105-1991 and ANSI T1.105A-1991), 1995

ANSI T1.107, Digital Hierarchy - Formats Specifications, 1995

ANSI T1.117, Digital Hierarchy - Optical Interface Specifications (SONET) (Single Mode - Short Reach), 1991

ANSI T1.204, OAM&P - Lower Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements, 1993

ANSI T1.208, OAM&P - Upper Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements, 1993

ANSI T1.408, ISDN Primary Rate - Customer Installation Metallic Interfaces (Layer 1 Specification), 1990

ANSI T1.601 ISDN Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT (Layer 1 Specification), 1992

ANSI T1.602, Data Link Signaling Specification for Application at the User Network Interface, 1996

ANSI T1.607, Digital Subscriber Signaling System No. 1 - Layer 3 Signaling Specification for Circuit Switched Bearer Service, 1990

ANSI T1.607a, Supplement, 1996

ANSI T1.610, DSS1 - Generic Procedures for the Control of ISDN Supplementary Services, 1994

ANSI T1.619, Multi-Level Precedence and Preemption (MLPP) Service, ISDN Supplementary Service Description, 1992

ANSI T1.619a, Supplement, 1994

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 X3.100a, Supplement to ANSI X3.100, 1991

ANSI X3.131, Information Systems - Small Computer Systems Interface - 2 (SCSI-2), 1994

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

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

ANSI/VITA 1, VME64 Specification, 1994

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

EIA 170, Electrical Performance Standards - Monochrome Television Studio Facilities, November 1957

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

EIA 330, Electrical Performance Standards for Closed Circuit Television Camera 525/60 Interlaced 2:1 (ANSI/EIA 330-68), November 1966

EIA 343-A, Electrical Performance Standard for High Resolution Monochrome Closed Circuit Television Camera (November 1966), September 1969

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 802.10, 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 1003.2d, POSIX: Shell and Utilities - Batch Environment

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

IEEE 1003.5b, POSIX, Ada Bindings for Real-Time Extensions (Draft)

IEEE 1101.2, Standard for Mechanical Core Specifications for Conduction-Cooled Eurocards (ANSI), 1992

IEEE 1278.1, DIS Application Protocols, 1995

IEEE 1278.2, DIS Communication Services and Profiles, 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 7942:1991, Graphics Kernel System (GKS), as profiled by FIPS Pub 120-1 (change notice 1)

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

ISO 8601, Date/Time Representations

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

ISO 8879: 1986, Standard Generalized Markup Language (SGML)

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 9592: 1989, Programmers Hierarchical Interactive Graphics Systems (PHIGS)

ISO 9945-2: 1993, Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 2: Shell and Utilities

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

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 13818-3: 1995 - Generic Coding of Moving Pictures and Associated Audio Information - Part 3: Audio

ISO/IEC 8802-3: 1996 (E) (ANSI/IEEE Std 802.3, 1996 edition) Local Area Network (LAN)/MAN CSMA/CD Access Method Standards Package

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

ISO/IEC 9075:1992 Information Technology - Database Language - SQL

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

ISO/IEC 9595 Information Technology-Open Systems Interconnection Common Management Information Services, December 1991

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 9596-2:1993 Information technology -- Open Systems Interconnection -- Common Management Information Protocol: Protocol Implementation Conformance Statement (PICS) proforma

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 9899, Programming languages -- C, 1990

ISO/IEC 9899/Amd. 1: 1995, Programming languages -- C, Amendment 1, C Integrity

ISO/IEC 9899/Cor. 1: 1994, Programming languages -- C, Technical Corrigendum 1

ISO/IEC 9899/Cor. 2: 1996, Programming languages -- C, Technical Corrigendum 2

ISO/IEC 9945-1:1996, Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 1: System Application Program Interface (API)

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 10038: 1993 (ANSI/IEEE Std 802.1D, 1993 Edition) Information technology-Telecommunications and information exchange between systems-Local area networks-Media access control (MAC) bridges

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

ISO/IEC 11172-3: 1993, Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Megabits per second (Mbits/s) --Part 3 (Audio Layer-3 only)

ISO/IEC 11172-3/Cor. 1: 1996, Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s --Part 3: Audio Technical Corrigendum (Audio Layer-3 only)

ISO/IEC 15802-2 : 1995 (ANSI/IEEE Std 802.1B, 1995 Edition) Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks - Common specifications-Part 2: LAN/MAN management (ANSI)

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-T G.711, Pulse Code Modulation (PCM) of Voice Frequencies, 1988

ITU-T G.728, Coding of Speech at 16 kbits/s Using Low-Delay Code Excited Linear Prediction (LD-CELP), September 1992

ITU-T H.221, Frame Structure for a 64 to 1,920 kbit/s Channel in Audiovisual teleservices, July 1995

ITU-T H.224, A Real Time Control Protocol for Simplex Applications using the H.221 LSD/HSD/MLP channels , November 1994

ITU-T H.244, Synchronized Aggregation of Multiple 64 or 56 kb/s channels, July 1995

ITU-T H.261, Video CODEC for Audiovisual Services at p x 64 kbit/s, March 1993

ITU-T H.281, A Far-End Camera Protocol for Videoconferences Using H.224, November 1994

ITU-T H.321, Adaptation of H.320 Visual Telephone Terminals to B-ISDN Environments, March 1996

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

ITU-T T.120, Data Protocols for Multimedia Conferencing, July 1996

ITU-T T.122, Multipoint Communication Service for Audiographics and Audiovisual Conferencing Service Definition, March 1993

ITU-T T.123, Protocol Stacks for Audiographic and Audiovisual Teleconference Applications November 1994

ITU-T T.124, Generic Conference Control, August 1995

ITU-T T.125, Multipoint Communication Service Protocol Specification, April 1994

ITU-T T.126, Multipoint Still Image and Annotation Protocol, August 1995

ITU-T T.127, Multipoint Binary File Transfer Protocol, August 1995

ITU-T M.3207.1, TMN management service: maintenance aspects of B-ISDN management, 1996

ITU-T M.3211.1, TMN management service: Fault and performance management of the ISDN access, 1996

ITU-T M.3400, TMN Management Functions, 1992

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

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)

Open Group CAE Specification C309, DCE: Remote Procedure Call which includes DCE IDL, August 1994

Open Group CAE Specification C310, DCE 1.1: Time Services Specification, November 1994

Open Group CAE Specification C312, DCE: Directory Services, December 1994

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

RFC-821, Simple Mail Transfer Protocol, 1 August 1982

RFC-822, Standard for the format of ARPA Internet text messages, 13 August 1982

RFC-951, Bootstrap Protocol, September 1985

RFC-1305, Network Time Protocol (V3), 9 April 1992

RFC-1332, The PPP Internet Protocol Control Protocol (IPCP), May 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-1514, Host Resources MIB, 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-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-1757, Remote Network Monitoring Management Information Base, (RMON Version 1), February 1995

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-1850, Open Shortest Path First (OSPF) Version 2 Management Information Base, November 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

RFC-1952, GZIP File Format Specification, Version 4.3, 23 May 1996

RFC-1989, PPP Link Quality Monitoring, August 1996

RFC-1990, The PPP Multilink Protocol, August 96

RFC-1994, PPP Challenge Handshake Authentication Protocol (CHAP), August 1996

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

SAE J 1850, Class B Data Communication Network Interface, 1 July 1995

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

SDN.903, revision 3.2, Secure Data Network System (SDNS) Key Management Protocol (KMP), 1 August 1989

SDN.301, revision 1.5, Secure Data Network System (SDNS) Security Protocol 3 (SP3), 1989

SMPTE 170M, Television - Composite Analog Video Signal - NTSC for Studio Applications, 1994

SR-3875, National ISDN 1995, 1996, and 1997, Bellcore

SR-3887, 1997 Version of National ISDN Primary Rate Interface Customer Premise Equipment Generic Guidelines, Bellcore

SR-3888, 1997 Version of National ISDN Basic Rate Interface Customer Premise Equipment Generic Guidelines, Bellcore

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-50/RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994

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

TIA/EIA 465-A, Group 3 Facsimile Apparatus for Document Transmission, 21 March 1995

TIA/EIA 466, Procedures for Document Facsimile Transmission, May 1981

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

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

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

(No Number) ATM Forum's DS1 Physical Layer Specification, af-phy-0016.000

(No Number) ATM Forum's DS3 Physical Layer Interface Specification, af-phy-0054.000

(No Number) ATM Forum's ILMI Management Information Base (MIB) for UNI 3.1, af-uni-0011.001

(No Number) ATM Forum's Integrated Local Management Interface (ILMI) Specification, Version 4.0, af-ilmi-0065.000, September 96

(No Number) ATM Forum's LAN Emulation Client Management Specification, af-lane-0038.000

(No Number) ATM Forum's LANE 1.0 Addendum, af-lane-0050.000

(No Number) ATM Forum's LANE Servers Management Spec v1.0, af-lane-0057.000

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

(No Number) ATM Forum's PNNI V1.0 Addendum, af-pnni-0066.000

(No Number) ATM Forum's Private Network to Network Interface (PNNI) Specification, Version 1.0, af-pnni-0055.000, March 1996

(No Number) ATM Forum's Traffic Management Specification, Version 4.0, af-tm-0056.000, April 96

(No Number) ATM Forum's UNI Signaling Specification, Version 4.0, af-sig-0061.000, July 96

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

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

Digital Imaging and Communication in Medicine (DICOM V3.0), American College of Radiology (ACR) and National Electrical Manufacturers Association (NEMA), parts 1-12, 1993

(No Number) Health Level 7 (HL7) V.2.2, 1 December 1994

(No Number) IP Mobility Support

(No Number) JPEG File Interchange Format (JFIF), Version 1.02, C-Cube Microsystems

(No Number) Microsoft Developer Network Win32 Software Development Kit (SDK), Microsoft

(No Number) Open Data Base Connectivity (ODBC), ODBC 3.0

(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) Personal Computer Memory Card International Association (PCMCIA), PC Card Standard, March 1997

(No Number) PCI Industrial Computer Manufacturer's Group (PICMG): Compact PCI Specification, 1 November 1995

(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 Guidelines for Software Design, Microsoft, 1995

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

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

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., Trusted Computer Security Evaluation Criteria (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). (OSJTF)

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, other than real property, that is of a type customarily used for nongovernmental purposes and that -- has been sold, leased, or licensed to the general public, or has been offered for sale, lease, or license to the general public.

(2) Any item that evolved from an item described in paragraph 1, above, through advances in technology or performance that is not yet available in the commercial market, but will be available in the commercial market 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 paragraph 1 or 2, above.

(4) Any combination of items meeting the requirements of paragraph 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 an 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 Federal Government simultaneously and under similar terms and conditions, and

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

(6) Services of a type offered and sold compet--itively, in substantial quantities, in the commer- cial market-place based on established catalog or market prices for specific tasks per-formed 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, combination of items, or ser- vice is transferred between or among separate divisions, subsidiaries, or affiliates of a contractor.

(8) A nondevelopmental item, if the procuring agency determines the item was developed exclusively at private expense and sold in substantial quantities, on a competitive basis, to multiple State and local governments.

(DRAFT DOD 5000.37H, Buying Commercial & Nondevelopmental Items: A DRAFT Handbook, April 1996)

Commercial Off-The-Shelf (COTS)

COTS is defined as commercial items that require no unique government modifications or maintenance over the life cycle of the product to meet the needs of the procuring agency.

(GLOSSARY: Defense Acquisition Acronyms and Terms, 1996)

Compliance

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

Exceptions

In the JTA-Army, exceptions are mandates for a given domain that replace a specific mandate in the main body of the JTA-Army.

Extensions

In the JTA-Army, extensions are additional mandates for a given domain that add to the mandates in the main body of the JTA-Army.

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

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 DOD 5000.37H, Buying Commercial & Nondevelopmental Items: A DRAFT Handbook, April 1996)

Mandates

Mandatory standards shall be implemented by systems that have a need for the corresponding interoperability-related services. In the JTA-Army, 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 JTA-Army 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.

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.

Nondevelopmental Item (NDI)

Nondevelopmental means "not requiring development."

(1) Any previously developed item used exclusively for governmental purposes by a Federal agency, a State or local government, or a foreign government with which the U.S. has a mutual defense cooperation agreement.

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

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

(DRAFT DOD 5000.37H, Buying Commercial & Nondevelopmental Items: A DRAFT Handbook, April 1996)

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. (OSJTF)

Operational Architecture (OA)

An Operational Architecture 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. (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. (OSJTF)

Real Time Systems

Systems which provide a deterministic response to asynchronous inputs. (OSJTF)

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. (OSJTF)

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. (OSJTF)

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 JTA-Army, 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 JTA-Army 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 JTA-Army is an important design consideration.

Systems Architecture (SA)

A **Systems Architecture** 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. (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/OSJTF)

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 - SUSTAINMENT DOMAIN EXCEPTIONS AND EXTENSIONS

D.1 INTRODUCTION

The Sustainment Domain consists of automated systems that perform combat service support and administrative business functions. These functions include all Army systems not specifically included in the Domains identified as C3I, Weapons Systems, or Modeling & Simulation.

D.1.1 Purpose

To denote differences (exceptions and extensions) employed in the Sustainment Domain that are required to implement needed application/system functionality and still support the JTA-Army philosophy of interoperability and integration (where required).

D.1.2 Scope

This domain includes all Army Sustainment Systems. Sustainment System examples include but are not limited to: Personnel; Legal; Logistics; Financial; Medical; Security; Supply; Maintenance; Engineering; Training and Education; Morale, Welfare, and Recreation; Acquisition; and Installation Management systems. The Army Information Mission Area has always addressed three environments: Theater/Tactical, Strategic, and what AR25-1 refers to as Sustaining Base. To name these specific environments does not imply any real or artificial boundaries. Many Sustainment Systems are indeed located and exist in more than one environment. The term "Base" has been eliminated from this domain title since some have erroneously taken the "Base" terminology to imply that its boundary is the installation - rather than it being the base or foundation of a system. Many Sustainment systems do indeed deploy (both during transition to/from and to war) either in total or as an extension (Split-Based or Power Projection are terms that are commonly applied).

D.1.3 Background

Office Automation was also initially in this domain's name but is, in itself, not a separate domain and not just associated with Sustainment.

The Army Medical Community is fundamentally a segment of the Joint Service Medical Community. As such, Army Medical places primary emphasis in being interoperable and integratible within that environment. As an area of Joint Service, the Medical Community has recommended to the JTA working Group that a separate Medical supplement (domain) be added to the JTA.

D.2 INFORMATION PROCESSING STANDARDS

D.2.1 Scope

Same scope as Section 2.1 of the document main body.

D.2.2 Mandates

D.2.2.1 Exceptions

There are no Exceptions to the Standards in the main body of the JTA-Army.

D.2.2.2 Extensions

D.2.2.2.1 User Interface Services (Reference Section 2.2.2.1.2)

As an extension to the mandates in Section 2.2.2.1.2, domain applications that require user interaction shall use Motif/X Windows APIs and be capable of executing in the CDE, or the applicable native windowing Win32 APIs. The Motif/X Window APIs should be used for systems requiring high multi-user performance, or when required for reuse of existing POSIX/Unix software. The Win32 APIs are more appropriate for systems requiring substantial use/reuse of COTS/GOTS products on X86 platforms. The following standard is mandated and noted as an extension:

- Microsoft Developer Network Win32 Software Development Kit (SDK), Microsoft.

D.2.2.2.2 Data Management Services (Reference Section 2.2.2.1.3)

This domain may develop or acquire client applications that use Microsoft data management services. In those instances, the following standard may be applied:

- Open Data Base Connectivity (ODBC), ODBC 3.0: Provides standard call level APIs between database application clients and the database server. It is noted that use of this standard is an extension to the standard as defined in the body of the JTA-Army. This ODBC standard is contained in the WIN 32 Software Development Kit referenced in Section D.2.2.2.1.

D.2.2.2.3 Geospatial Data Interchange (Reference Section 2.2.2.1.4.3)

In addition to tactical missions, the Army Corps of Engineers (USACE) has major projects in the Civil Works area and for Army Installations in the facilities engineering and environmental restoration arena. For both the Civil and Army Installation sectors, interpretation of a Presidential Executive Order 12906 (dated April 1994) stipulates the use of FIPS 173-1 versus MIL-STD-2407 & 2411 as defined in the JTA-Army. For civil, facilities engineering, and environmental restoration missions, the following standard is mandated and noted as an extension:

- FIPS Pub 173, Spatial Data Transfer Standard (SDTS), 10 June 1994.

D.2.2.2.4 Operating System Services (Reference Section 2.2.2.1.7)

As an extension to the mandates in Section 2.2.2.1.7, services shall be accessed by applications through either the applicable standard POSIX APIs or Win32 APIs. The POSIX APIs should be used for systems requiring high multi-user performance, or when required for reuse of existing POSIX/Unix software. The Win32 APIs are more appropriate for systems requiring substantial use/reuse of COTS/GOTS products on X86 platforms. The following standard is mandated and noted as an extension:

- Microsoft Developer Network Win32 Software Development Kit (SDK), Microsoft.

D.2.3 Emerging Standards

There are no additions to the standards referenced in the main body of the document.

D.3 INFORMATION TRANSFER STANDARDS

D.3.1 Scope

Same scope as Section 3 of the main body of the JTA-Army. Additionally, the Smart Card Technology is being developed for a variety of potential applications within the Sustainment domain. As this technology matures, it is expected to become available for use in other Army domains.

D.3.2 Mandates

D.3.2.1 Exceptions

There are no exceptions to the standards in the main body of the JTA-Army.

D.3.2.2 Extensions

D.3.2.2.1 Mandates (Reference Section 3.2)

In defining the standards for communicating medical information between nodes internal to the Medical Community, the key extensions required and mandated are:

- Health Level 7 (HL7) V.2.2, 1 December 1994.
- Digital Imaging and Communication in Medicine (DICOM V3.0), American College of Radiology (ACR) and National Electrical Manufacturers Association (NEMA), parts 1-12, 1993.

It is noted that the DICOM standard does not apply to communications which would be conducted over common tactical Army communication networks such as SINCGARS or EPLRS.

D.3.3 Emerging Standards

Smart Card technology is a burgeoning area with numerous existing and potential applications. These Smart Cards incorporate one or more technologies used to store information which is both updatable and static. They include use of magnetic stripe, bar code, and integrated circuit chip (ICC) and optical (embossed and printed) media.

Physical Standards - Physical characteristics such as card dimensions, construction, materials and characteristics are provided in ISO/IEC 7810, Identification Cards-Physical Characteristics, 15 August 1995.

Magnetic Stripe Standards - Magnetic stripe requirements (three track) are covered in the ISO/IEC 7811 series, Identification Cards - Recording Techniques, 15 August 1995.

Bar Code Standards - One dimensional bar codes (commonly called 3 of 9) are covered by ANSI/AIM BC-1-1995 Uniform Symbology Specification Code 39 (USS-39) and ANSI x3.182- 1992 with the USS-39 standard having precedence. Human readable interpretation (HRI) as defined in USS-39 will not be used. Two Dimensional bar codes will comply with requirements in Uniform Symbology Specification (USS) Portable Data File (PDF) 417. Neither truncated USS PDF 417 nor Macro PDF 417 will be used.

ICC Standards - The ISO/IEC 7816 series of standards (Identification Cards - Integrated Circuits with Contacts, 1995), which cover the basic characteristics of integrated circuit chips (ICC) with contacts, has achieved near-universal marketplace acceptance. The ISO/IEC 10536 series of standards similarly covers contactless IC cards. It should be noted that ISO/IEC 7816-7 standard covers a promising set of inter-industry commands for Structured Card Query Language (SCQL) to support vendor-independent data management. The 7816 series of standards describes the basic ICC physical and electrical characteristics, interface protocols, and data and file conventions for IC cards with contacts, and has achieved near-universal acceptance across industry and DOD sponsored smart card projects. The 10536 series parallels the 7816 series of standards for contactless cards (i.e. cards the communicate with the reader device via conductive or capacitive coupling, radio frequency (RF) transmission, etc. vice requiring physical contact with the reader).

Financial Transaction Card Standards - Financial transaction card messages between the IC card and the card accepting device are covered by ISO 9992-1 (1990) and ISO/DIS 9992-1 (No- Date). Additionally, Financial transaction card security architectural issues are addressed in ISO 10202.

Although many of these individual standards have been in place since the mid-1980s, implementation of combinations of Smart Card features will undoubtedly force changes to be incorporated. DOD (DISA JIEO Center for Standards (CFS)) has published a Military Handbook (MIL-HDBK-0348) entitled Portable Information Carrier - Standards and Guidance dated 15 April 1997.

D.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS

There are no exceptions or extensions to the standards in the main body of the JTA-Army.

D.5 HUMAN-COMPUTER INTERFACES

D.5.1 Scope

Same as Section 5 of the main body of the JTA-Army.

D.5.2 Mandates

D.5.2.1 Exceptions

There are no exceptions to the standards in the main body of the JTA-Army.

D.5.2.2 Extensions

D.5.2.2.1 Commercial Style Guides (Reference Section 5.2.2.1)

As an extension to the mandate in Section 5.2.2.1 and for Windows based systems, the following standard is mandated:

- The Windows Interface Guidelines for Software Design, Microsoft, 1995.

D.5.3 Emerging Standards

There are no additions to the standards referenced in the main body of the document.

D.6 INFORMATION SECURITY

There are no exceptions or extensions to the standards in the main body of the JTA-Army.

This page was intentionally left blank.

APPENDIX E - C3I DOMAIN EXCEPTIONS AND EXTENSIONS

E.1 INTRODUCTION

E.1.1 Scope

The C3I Domain consists of command and control, communications, intelligence, and electronic warfare systems. There are three sub-domains: Command and Control, Communications, and Intelligence and Electronic Warfare.

E.1.2 Background

E.1.3 Appendix Organization

E.2 INFORMATION PROCESSING STANDARDS

E.2.1 Scope

E.2.2 Mandates

There are no exceptions or extensions to the standards in the main body of the JTA-Army.

E.3 INFORMATION TRANSFER STANDARDS

E.3.1 Scope

The scope is the same as Section 3 of the main body of the JTA-Army.

E.3.2 Mandates

E.3.2.1 Exceptions

There are no exceptions to the standards in the main body of the JTA-Army.

E.3.2.2 Extensions

E.3.2.2.1 End System Standards

E.3.2.2.1.1 Secondary Imagery Dissemination Standards (Reference Section 3.2.1.4)

The Tactical Communications Protocol 2 (TACO2) is the communications component of the National Imagery Transmission Standard (NITFS) suite of standards used to disseminate secondary imagery. TACO2 shall be used over point-to-point tactical data links in high BER disadvantaged communications environments. TACO2 is used to transfer secondary imagery and related products where transfer protocols in Section 3.2.1.1.2 fail. TACO2 only applies to users having simplex and half duplex links as their only means of communications. MIL-HDBK-1300A, NITFS, provides guidance to implement various Technical Interface Specifications (TIS) to connect the TACO2 host to specific cryptographic equipment. The following standard is mandated:

- MIL-STD-2045-44500, National Imagery Transmission Format Standard (NITFS) Tactical Communications Protocol 2 (TACO2), 18 June 1993.

E.3.2.2.2 Network Standards

There are no extensions to the standards in the main body of the JTA-Army.

E.3.2.2.3 Transmission media (Reference Section 3.2.3)

E.3.2.2.3.1 Military Satellite Communications (MILSATCOM)

MILSATCOM systems include those systems owned or leased and operated by the DOD and those commercial Satellite Communications (SATCOM) services used by the DOD. The basic elements of satellite communications consists of a space segment, control segment, and a terminal segment (air, ship, ground, etc.). An implementation of a typical satellite link will require the use of satellite terminals, user communications extension, and the use of military or commercial satellite resources.

E.3.2.2.3.1.1 Ultra High Frequency (UHF) Satellite Terminal Standards

E.3.2.2.3.1.1.1 5- and 25-kilo-Hertz (kHz) Service

For 5-kHz or 25-kHz single channel access service supporting the transmission of either voice or data, the following standard is mandated:

- MIL-STD-188-181, Interoperability Standard for Dedicated 5-kHz and 25-kHz UHF Satellite Communications, 18 September 1992.

E.3.2.2.3.1.1.2 5-kHz Demand Assigned Multiple Access (DAMA) Service

For 5-kHz DAMA service, supporting the transmission of data at 75 - 2400 bits per second (bps) and digitized voice at 2400 bps, the following standard is mandated:

- MIL-STD-188-182, Interoperability Standard for 5 kHz UHF DAMA Terminal Waveform, 18 September 1992.

E.3.2.2.3.1.1.3 25-kHz Time Division Multiple Access (TDMA)/Demand Assigned Multiple Access (DAMA) Service

For 25-kHz TDMA/DAMA service, supporting the transmission of voice 2400, 4800, or 16000 bps and data at rates of 75 - 16000 bps, the following standard is mandated:

- MIL-STD-188-183, Interoperability Standard for 25 kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992.

E.3.2.2.3.1.1.4 Data Control Waveform

For interoperable waveform for data controllers used to operate over single access 5 kHz and 25 kHz UHF SATCOM channels, the following standard (a robust link protocol that can transfer error free data efficiently and effectively over channels that have high error rates) is mandated:

- MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993.

E.3.2.2.3.1.2 Super High Frequency (SHF) Satellite Terminal Standards

E.3.2.2.3.1.2.1 Earth Terminals

For minimum mandatory Radio Frequency (RF) and Intermediate Frequency (IF) requirements to ensure interoperability of SATCOM earth terminals operating over C, X, and Ku- band channels, the following standard is mandated:

- MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995.

E.3.2.2.3.1.2.2 Phase Shift Keying (PSK) Modems

For minimum mandatory requirements to ensure interoperability of PSK modems operating in Frequency Division Multiple Access mode, the following standard is mandated:

- MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995.

E.3.2.2.3.1.3 Extremely High Frequency (EHF) Satellite Payload and Terminal Standards

E.3.2.2.3.1.3.1 Low Data Rate (LDR)

For waveform, signal processing, and protocol requirements for acquisition, access control, and communications for low data rate (75 - 2400 bps) EHF satellite data links, the following standard is mandated:

- MIL-STD-1582, EHF LDR Uplinks and Downlinks, 10 December 1992.

E.3.2.2.3.1.3.2 Medium Data Rate (MDR)

For waveform, signal processing, and protocol requirements for acquisition, access control, and communications for medium data rate (4.8 kbps - 1.544 Mbits/s) EHF satellite data links, the following standard is mandated:

- MIL-STD-188-136, EHF MDR Uplinks and Downlinks, 26 August 1995.

E.3.2.2.3.2 Radio Communications

E.3.2.2.3.2.1 High Frequency (HF)

E.3.2.2.3.2.1.1 HF and Automatic Link Establishment (ALE)

For both ALE and radio subsystem requirements operating in the HF bands, the following standard is mandated:

- MIL-STD-188-141A, Medium and High Frequency Radio Equipment Standard, 10 September 1993.

E.3.2.2.3.2.1.2 Anti-jamming Capability

For anti-jamming capabilities for HF radio equipment, the following standard is mandated:

- MIL-STD-188-148A, Interoperability Standard Anti-Jam (AJ) Communication HF Band (2-30 Mhz), 18 March 1992.

E.3.2.2.3.2.1.3 Data Modems

For HF data modem interfaces, the following standard is mandated:

- MIL-STD-188-110A, Data Modems, Interoperability and Performance Standards, 30 September 1991.

E.3.2.2.3.2.2 Very High Frequency (VHF)

For radio subsystem requirements operating in the VHF frequency bands, the following standard is mandated:

- MIL-STD-188-242, Tactical Single Channel (VHF) Radio Equipment, 20 June 1985.

E.3.2.2.3.2.3 Ultra High Frequency (UHF)

For radio subsystem requirements operating in the UHF frequency bands, the following standard is mandated:

- MIL-STD-188-243, Tactical Single Channel (UHF) Radio Communications, 15 March 1989.

E.3.2.2.3.2.4 Super High Frequency (SHF)

For radio subsystem requirements operating in the SHF frequency bands, the following standard is mandated:

- MIL-STD-188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment, 28 July 1992.

E.3.2.2.3.2.5 Joint Tactical Information Distribution System (JTIDS)/Multifunctional Information Distribution System (MIDS) Transmission Media

When communicating with the JTIDS/MIDS radios, the following standards are mandated:

- SSDCB79S4000 - JTIDS System Segment Specification (Class 2 Terminal) (SECRET).

- Standardization Agreement (STANAG) 4175, Edition 1, 29 August 91 - Technical Characteristics of the Multifunctional Information Distribution System (MIDS).

E.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS

There are no exceptions or extensions to the standards in the main body of the JTA-Army.

E.5 HUMAN-COMPUTER INTERFACES

E.5.1 Scope

E.5.2 Mandates

E.5.2.1 Exceptions

There are no exceptions to the standards in the main body of the JTA-Army.

E.5.2.2 Extensions

E.5.2.2.1 Domain-level Style Guides (Reference Section 5.2.2.3)

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 supplements the basic guidelines set forth in the *DOD HCI Style Guide.* The following standard is mandated:

- User Interface Specifications for the Defense Information Infrastructure.

E.5.3 Emerging Standards

There are no exceptions or extensions to the emerging standards in the main body of the JTA-Army.

E.6 INFORMATION SECURITY

There are no exceptions or extensions to the standards in the main body of the JTA-Army.

This page was intentionally left blank.

APPENDIX F - WEAPON SYSTEMS DOMAIN EXCEPTIONS AND EXTENSIONS

F.1 INTRODUCTION

Weapon Systems have special attributes, i.e., timeliness, embedded nature, space limitation, adverse environmental conditions, and critical requirements such as survivability, low power/weight, and hard real time processing that drive system architectures and make system hardware and software highly interdependent and interrelated. In 1996, the Weapon Systems Technical Architecture Working Group (WSTAWG) was formally chartered by both the Army Acquisition Executive (AAE) and the Army Materiel Command (AMC) Commanding General to support the identification, development, and maintenance of unique information standards and related interface specifications for Weapon Systems and the extension of the Technical Architecture Framework for Information Management (TAFIM) Technical Reference Model (TRM) to accommodate the requirements of the Weapon Systems Domain.

F.1.1 Scope

For the purposes of the JTA-Army, the Weapon Systems Domain is organized into four subdomains to facilitate the identification of areas amenable to standardization. The current subdomains are aviation, ground vehicles, soldier systems, and missiles. Definitions of each subdomain are available in JTA-Army Appendix C, Glossary.

F.1.2 Appendix Structure

This Appendix follows the JTA-Army core document structure to facilitate the identification and traceability of the Weapon Systems Domain exceptions and extensions to the standards mandated in the main body of the JTA-Army. The TAFIM TRM is being modified to include weapon system characteristics, specifically *hardware* and *performance*. Therefore, the Weapon Systems Domain Appendix consists of seven sections: Sections 1-6 are the same as those contained in the main body of the JTA-Army; Section 7, Application Hardware Standards, is a new section in this version. Each section is divided into three subsections as follows:

- *Scope,*
- *Mandates,* and
- *Emerging Standards.*

Weapon Systems "mandates" result from significant consensus, concerning the need for the standards and the maturity of their commercial implementations, within the Weapon Systems Domain or within one or more subdomains. "Emerging standards" are those which are expected to become "mandates" when their commercial implementations have matured and/or one or more of the subdomains have completed their evaluation and

testing and reach agreement on the need for the standards. The "emerging standards" subsection also includes new services and/or interfaces for which standards are not available and/or which would require research and development (R&D) investment to generate the appropriate standards.

Currently there are sections within the JTA-Army for which no exceptions or extensions have been mandated by the Weapon Systems Domain or by one or more Subdomains. However, due to their hard real time and embedded system requirements, the Weapon Systems Subdomains are evaluating the available real time standards for possible mandate as exceptions or extensions to each section of the JTA-Army, where appropriate. **Note: A joint working group chaired by the PEO for Battle Management at Air Force Electronic Systems Command (ESC) is investigating the need to develop Real Time Extensions to the DII COE and other areas of the technical architecture, as appropriate, to support the requirements of real time and embedded systems.**

F.2 INFORMATION PROCESSING STANDARDS

F.2.1 Scope

This section applies to mission area, support application, and application platform service software developed or procured by the Army to process information for weapon systems.

The organizational *framework* for the JTA-Army, the TAFIM TRM, must be extended to meet the requirements of the weapons domain. The extended TRM must accommodate a hierarchy of weapon domain reference models of sufficient fidelity to identify critical functions, interfaces, and technical issues. For Weapon Systems, the TAFIM TRM is extended in two ways: (1) two more external environment classes are added, and (2) a hierarchical reference model is introduced.

F.2.1.1 Top Level Extensions

Version 3.0 of the TAFIM TRM is extended for real time embedded weapon systems architectures as shown in Figure F-1. The fundamental extensions of the framework are the modeling of a weapon system's *Performance Environment* and *Application Hardware Environment.*

F.2.1.1.1 Performance Environment

One of the most distinctive features of a weapon system is the importance of performance characteristics. Weapon systems are developed to meet stringent operational performance criteria in order to be lethal and survive. In order to emphasize this issue, performance is modeled as a separate external environment entity. At the lower level of TRMs, performance will be an integral part of the services.

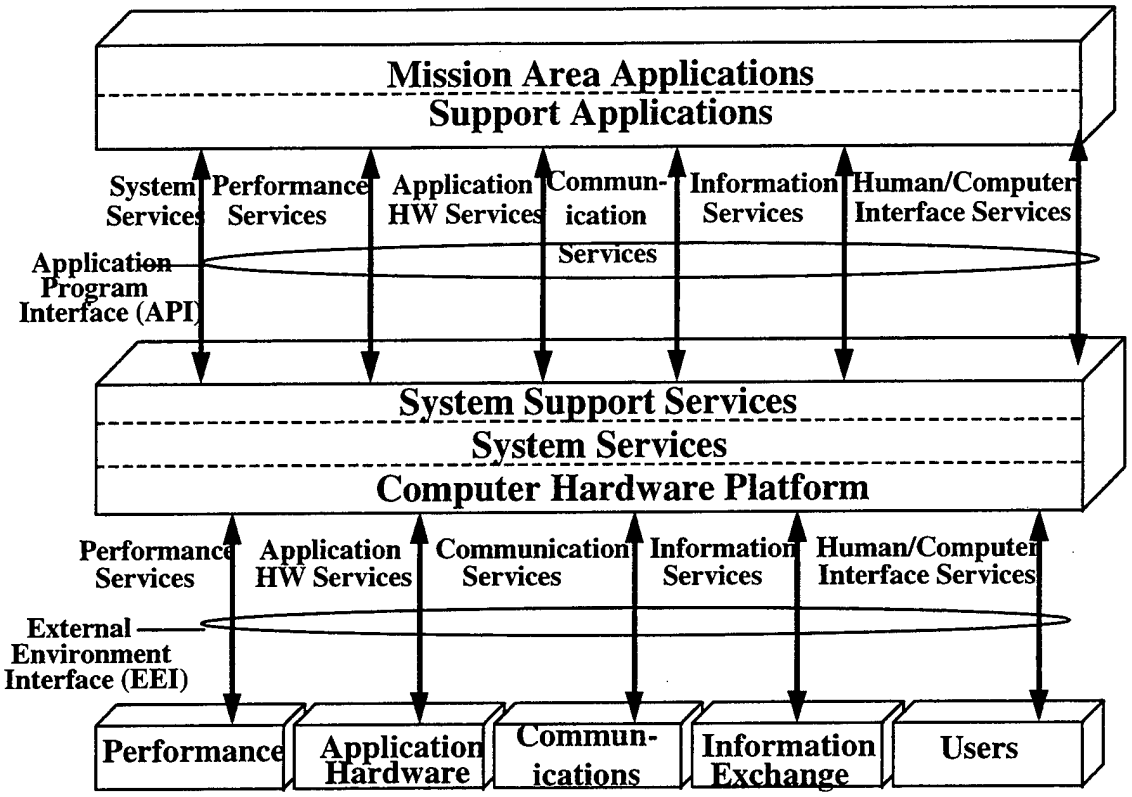


FIGURE F-1 TAFIM TRM, FIRST ORDER EXTENSION FOR WEAPON SYSTEMS

F.2.1.1.2 Application Hardware Environment

Within weapon systems embedded computing hardware and software components are highly interdependent in order to satisfy very demanding requirements. This type of architecture often does not fit a general purpose computing model very well. Therefore the TRM will be extended to capture such features as interconnect and open systems hardware standards.

F.2.1.2 Hierarchy of TRMs

In order to capture the diversity found in weapon subsystem design, a hierarchical approach to TRMs is being established. From the top level of the TAFIM TRM, component TRMs will extend downward into the subdomains to provide the basis for standards identification and traceability. For the near term, the Society of Automotive Engineers (SAE) Generic Open Architecture (GOA), discussed in Section F.2.3.1 Emerging General Standards, is one representative TRM that will be used for the lower level.

F.2.2 MANDATES

F.2.2.1 Exceptions

F.2.2.1.1 Graphic Services (Reference Section 2.2.2.1.5)

ISO/IEC 9636 establishes the conceptual model, functional capability, and minimum conformance requirements of the Computer Graphics Interface (CGI). The Weapon Systems Domain mandates the following standard as the profile to be used with ISO 7942: 1991, Graphics Kernel System (GKS) and ISO 9592: 1989, Programmers Hierarchical Interactive Graphics Systems (PHIGS) for providing graphic services instead of FIPS Pub 120-1 and FIPS Pub 153:

- ISO/IEC 9636, Information Technology-Computer Graphics-Interfacing Techniques for Dialogue with Graphics Devices (CGI), 1991.

F.2.2.1.2 Operating System Services (Reference Section 2.2.2.1.7)

The Weapon Systems Domain is considering several real time extensions (see Section F.2.3) to the POSIX Standards contained in the JTA-Army, and therefore will not use FIPS PUB 151-2: 1994 as the profile for ISO/IEC 9945-1: 1996, Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 1: System Application Program Interface (API).

F.2.2.1.3 User Interface Services (Reference Section 2.2.2.1.2)

The Soldier Systems Subdomain is unable to use X/Open C323, Common Desktop Environment (CDE) Version 1.0, but instead is uniquely structured to support the Weapon Systems Human-Computer Interface (WSHCI) Style Guide and the Soldier Systems Subdomain Style Guide.

F.2.2.2 Extensions

Currently there are no extensions mandated for the Information Processing Standards section.

F.2.3 EMERGING STANDARDS

F.2.3.1 Emerging General Standards

The Weapon Systems Domain is extending the TAFIM TRM to make it more applicable to real time systems. As a result, the following emerging architecture standard is being considered for mandate as a an extension to the TAFIM TRM identified in the JTA-Army:

- *SAE AS 4893. Generic Open Architecture (GOA) Framework, 01 Jan. 96* - The SAE GOA provides a framework to identify interface classes for applying open system interface standards to the design of hardware/software systems. It provides a 2nd order

modeling extension specifically for the application hardware, communication, and information services portion of the Weapon Systems TAFIM TRM extension.

F.2.3.2 Emerging Service Area Standards

F.2.3.2.1 Operating System Services

The Open Systems Joint Task Force (OSJTF) is sponsoring and synchronizing Weapon Systems Domain involvement in the IEEE POSIX working groups. Many POSIX standards are at various stages of standardization and are expected to be revised shortly to accommodate real time systems' requirements and to provide for test methods. Therefore, the following emerging standards are being considered for mandate by the Weapon Systems Domain or by specific Subdomains as exceptions or extensions to the JTA-Army operating system services standards:

- *IEEE P1003.5c/D2 POSIX-Part 1: Binding for API - Amendment 2: Protocol Independent Interfaces, January 1997*
- *IEEE P1003.5f POSIX: Ada binding to 1003.21*
- *IEEE P1003.13/D7 POSIX Realtime Application Environment Support (AEP), August 1995*
- *IEEE P1003.1e/D15 POSIX: Protection Audit And Control Interface (C Language), December 1995*
- *IEEE P1003.22/D6. POSIX-Open System Security Framework, August 95*
- *SAE xxx: Operating System API for ADA Run Time System* (Aviation and Soldier Systems Subdomains only)

F.2.3.2.2 Audio Data Interchange

The Weapon Systems Domain is considering mandating the Audio Data Interchange service area, currently identified only in the Joint Technical Architecture (JTA), as an extension to the JTA-Army Information Processing Standards section. As a result, the following standard is also being considered for mandate by the Weapon Systems Domain as an extension to the standards in this service area:

- *ITU Recommendation G.726 (December 1990): 40, 32, 24, 16 kbps Adaptive Differential Pulse Code Modulation (ADPCM)*

F.2.3.2.3 Real Time Common Object Request Broker Architecture (CORBA)

- *Real Time Common Object Request Broker Architecture (CORBA)* - The OMG Special Interest Group is evaluating the need for real time object oriented standards and products to support real time embedded systems. As more information becomes available from this group the Weapons Domain will consider adopting the standards as emerging exceptions or extensions to the JTA-Army information modeling and data exchange standards.

F.3 INFORMATION TRANSFER STANDARDS

F.3.1 Scope

This section applies to the transfer of information within a Weapon System.

Information processing nodes and groups of processors within a weapon system are connected by a local network. This network, which may be embedded, provides interconnection between the various hardware elements and typically must provide real time communications, i.e., deterministic communications within a system-allocated performance boundary. Weapon system networks consist of both media access control and point-to-point protocols, and typically have differentially based electrical media to provide some inherent electrical noise protection. These data carrying intra-weapon system networks are separated into three classes of data throughput: low, medium, and high.

There are also networks that are embedded as parts of a larger internal interconnect scheme (e.g., busses like VME) which will be covered in Section F.7.

F.3.2 MANDATES

F.3.2.1 Exceptions

Currently there are no exceptions mandated for the Information Transfer Standards section.

F.3.2.2 Extensions

Currently there are no extensions mandated for the Information Transfer Standards section.

F.3.3 EMERGING STANDARDS

Currently there are no emerging standards identified for the Information Transfer Standards section.

F.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS

F.4.1 Scope

This section fosters information exchange among Army Weapon Systems during their development and maintenance phases. During concept exploration and development a large amount of information elements, objects, and artifacts are generated. If these elements, objects, and artifacts are shared across weapon system developments, considerable resources can be saved.

Real time, embedded processing systems must be developed within a development support environment for an entire system. As such, they must integrate into a systems engineering process that culminates in prototype or production weapon systems that meet specific functional and performance requirements. The entire development process relative to the real time, embedded processing system, though not necessarily linear, can be characterized by phases, as depicted in Figure F-2. Information exchange must occur between each of these phases.

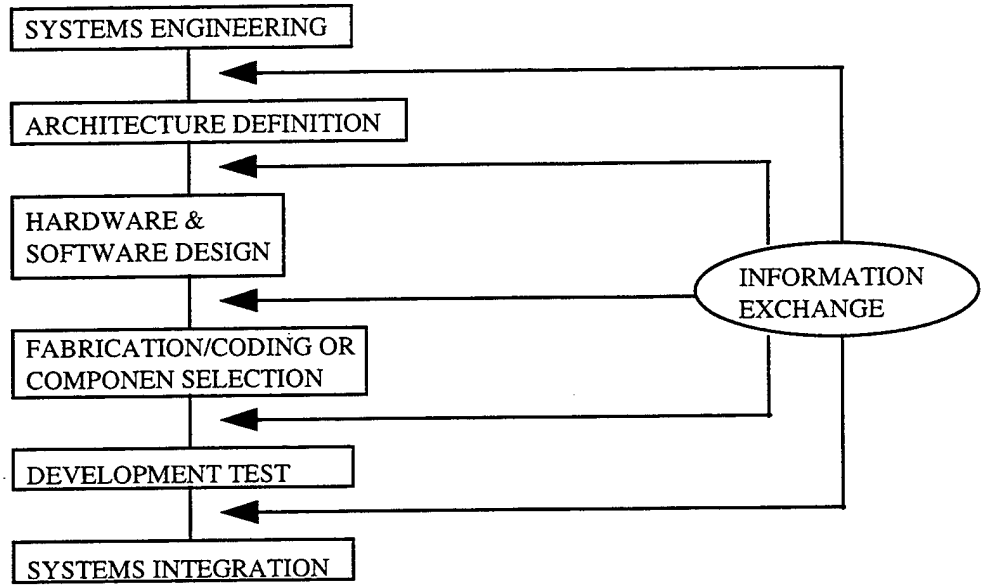


FIGURE F-2 DEVELOPMENT PROCESS RELATIVE TO THE REAL TIME, EMBEDDED PROCESSING SYSTEM

Each phase has its own unique development environment and support tools. The real time, embedded processing system information exchange standards must be compatible with information exchange standards for these various environments.

In addition, the real time embedded processing system must be modeled within a systems electronic/software architecture. Activity and data modeling must be linked to performance modeling.

Finally, there are emerging software reuse processes to meet the Army's software reuse policy. As these software reuse processes are defined, they will and must drive the selection/use of any related information exchange standards.

F.4.2 MANDATES

Currently there are no exceptions or extensions mandated for the JTA-Army information modeling and data exchange standards section.

F.4.3 EMERGING STANDARDS

Statecharts - This is a high order hardware language that can implicitly relate timing constraints to activity modeling. Therefore the following emerging standard is being considered for mandate by the Weapon Systems Domain as an exception or extension to the JTA-Army information modeling standards:

- *IEEE 1076: 1993, Standard VHSIC Hardware Description Language(VHDL)* - VHDL is a high level hardware language.

The Weapon Systems Subdomains are considering the following areas within the realm of information modeling with high activity levels where emerging standards should coalesce:

- *Integrated Software Engineering CASE Tools* - "Open system" interoperability between upper CASE (architecture, modeling, analysis) and lower CASE (design, traceability, test, implementation) tools.

- *Object-Oriented Design Notation and Methods* - (Colbert, Rumbaugh, Booch, etc.).

F.5 HUMAN-COMPUTER INTERFACE STANDARDS

F.5.1 Scope

This section provides a common framework for Human-Computer Interface (HCI) design and implementation in Army weapon systems. It complements and extends the DOD HCI Style Guide. The objective is to standardize user interface design and implementation options across weapon systems, thus enabling Army applications within the Weapon Systems Domain to appear and behave consistently, resulting in higher productivity, shorter training time, and reduced development, operation, and support costs besides influencing commercial HCI development.

This version mandates the design of graphical and character-based displays and controls for Army weapon systems.

F.5.1.1 Definition

In order to identify appropriate Army systems to use for baseline characterization, the following working definition for time criticality is used:

"Systems where little or no delay exists between the time an event occurs and the time it is presented to the user; and where there is an operational requirement for the user to quickly recognize this presentation, comprehend its significance, and determine and execute appropriate action(s)."

F.5.1.2 HCI Hierarchy

There are some aspects of HCI's that can be common across the Weapon Systems Domain, while others are Subdomain specific. Hence, there is an HCI style guide at the

weapon systems level, and one for each of the four subdomains (Ground Vehicle, Aviation, Missile, and Soldier Systems).

F.5.2 MANDATES

F.5.2.1 Exceptions

Currently there are no exceptions mandated for the JTA-Army human-computer interface standards section.

F.5.2.2 Extensions

F.5.2.2.1 Symbology (Reference Section 5.2.1.3)

The primary standard for military symbology for the Weapon Systems Domain is MIL-STD-2525A as mandated in the main body of the JTA-Army. However, other MIL-STD's, such as MIL-STD-1477B, are used as supplements where MIL-STD-2525A symbology does not meet the operational requirements of the Subdomain. For example, the Missile Subdomain (specifically the Air and Missile Defense systems portion of the Subdomain), needs to be able to indicate that an air track is hostile but unengageable. MIL-STD-2525A does not support this capability. Therefore, the following standards are mandated as Subdomain extensions to the JTA-Army symbology standard:

- MIL-STD-1295, Vertical Situation Displays And Electronic Attitude Director Indicators For Rotary-Wing Aircraft (Aviation Subdomain).
- MIL-STD-1477B, Army Air Defense Symbology (Air and Missile Defense portion of Missile Subdomain).
- MIL-STD-1787, Aircraft Display Symbology (Aviation Subdomain).

F.5.2.2.2 Domain-level Style Guide (Reference Section 5.2.2.3)

The Weapon Systems Human-Computer Interface (WSHCI) Style Guide addresses guidelines that are applicable across most or all of the Army Weapon Systems Domain. It provides a starting point for the development of the subdomain specific style guides that will further the goal of standardization. Also, the WSHCI Style Guide provides design guidance based on lessons learned and best practices from past HCI efforts. However, the WSHCI Style Guide does not provide the level of design guidance needed to attain a common behavior and appearance. This is left to the Subdomain-specific style guides. The following standard is mandated:

- U.S. Army Weapon Systems Human-Computer Interface (WSHCI) Style Guide

F.5.3 EMERGING STANDARDS

F.5.3.1 Aviation Subdomain Style Guide

- *Soldier/Aircrew Machine Interface Style Guide* - The WSHCI Style Guide is being tailored and extended for the Army aviation community as the Soldier/Aircrew Machine Interface Style Guide. This document will address the issues that are specific to the Aviation Subdomain. It will provide design guidance which will result in a common HCI behavior and appearance across Army aviation platforms.

F.5.3.2 Ground Vehicle Subdomain Style Guide

The Ground Vehicle Subdomain Style Guide will tailor and extend the WSHCI Style Guide to address the issues that are specific to the Ground Vehicles Subdomain. The Ground Vehicle Subdomain Style Guide will provide design guidance which will result in a common HCI behavior and appearance across Army ground vehicle platforms.

F.5.3.3 Missile Subdomain Style Guide

The Missile Subdomain Style Guide will tailor and extend the WSHCI Style Guide to address the issues that are specific to the Missile Subdomain. The Missile Subdomain Style Guide will provide design guidance which will result in a common HCI behavior and appearance across Army Tactical Missile and Air and Missile Defense platforms.

F.5.3.4 Soldier Systems Subdomain Style Guide

The Soldier Systems Subdomain Style Guide will tailor and extend the WSHCI Style Guide to address the issues that are specific to the Soldier-Systems Subdomain. The Soldier-Systems Subdomain Style Guide will provide design guidance which will result in a common HCI behavior and appearance across Army Soldier-System platforms.

F.6 INFORMATION SECURITY STANDARDS

Currently there are no exceptions or extensions mandated for the Information Security Standards section.

F.7 APPLICATION HARDWARE STANDARDS

F.7.1 Scope

The primary purpose of this section is to minimize the percentage of standalone and closed application modules used in Weapon Systems. The secondary goal is to foster the development of commercial hardware standards that can be used for Weapon Systems development.

Real time embedded processing systems must control, sense, and integrate with an application hardware environment. The application hardware is generally a custom built

electronic or mechanical module. The application hardware along with the processing system and application software must work together to perform unique mission requirements. The level of coupling of the processing system to the application hardware environment determines the possibility of modular partitioning. Considering the level of coupling of embedded processing systems to application hardware as a guide, weapon systems can be divided into the three classes defined below.

Loosely coupled: In this set up the interface between the application hardware environment and the processing system is clearly defined.

Strongly Coupled: In this set up the application hardware environment and the processing system are tightly coupled. Their interface is not clearly defined. The module acts as a standalone unit.

Hybrid: In this set up some standalone units are loosely coupled.

F.7.2 MANDATES

F.7.2.1 Exceptions

Currently there are no exceptions identified for this section as none are contained in the core sections of the JTA-Army.

F.7.2.2 Extensions

F.7.2.2.1 Hardware Interface Standards (annotated with applicable subdomain(s))

F.7.2.2.1.1 Bus Interface Standards

- MIL-STD-1553B, Standard for Medium Speed System Network Bus (Aviation, Ground Vehicles Subdomains).
- ANSI/VITA 1, VME64 Specification, 1994 (Aviation, Ground Vehicles Subdomains).
- PCI Industrial Computer Manufacturer's Group (PICMG): Compact PCI Specification, 1 November 1995 (Ground Vehicle Subdomain).
- MIL-STD-1773, Fiber Optics Mechanization of an Aircraft Internal Time Division Command/Response Multiplex Data Bus (Aviation Subdomain).
- SAE J 1850, Class B Data Communication Network Interface, 1 July 1995 (Ground Vehicles Subdomain).
- ANSI X3.131, Information Systems - Small Computer Systems Interface - 2 (SCSI-2), 1994 (Ground Vehicles Subdomain).

F.7.2.2.1.2 General Hardware Interface Standards

- Personal Computer Memory Card International Association (PCMCIA), PC Card Standard, March 1997 (Ground Vehicles Subdomain).
- IEEE 1101.2, Standard for Mechanical Core Specifications for Conduction-Cooled Eurocards (ANSI), 1992 (Ground Vehicles Subdomain).

- EIA 170, Electrical Performance Standards - Monochrome Television Studio Facilities, November 1957, (Ground Vehicle Subdomain).
- EIA 330, Electrical Performance Standards for Closed Circuit Television Camera 525/60 Interlaced 2:1 (ANSI/EIA 330-68), November 1966, (Ground Vehicle Subdomain).
- EIA 343-A, Electrical Performance Standard for High Resolution Monochrome Closed Circuit Television Camera (November 1966), September 1969, (Ground Vehicle Subdomain).
- SMPTE 170M, Television - Composite Analog Video Signal - NTSC for Studio Applications, 1994, (Ground Vehicle Subdomain).
- MIL-STD-1389D, Standard Electronic Module (SME), (Aviation Subdomain).

F.7.3 EMERGING STANDARDS

F.7.3.1 Emerging General Standards

The following emerging standards are being evaluated for mandate by the Weapon Systems Domain or specific Subdomains:

- *IEEE P996.1/D1, Compact Embedded PC Modules, October 1993*
- *IEEE P1386.1/D2.0 - Physical/Environmental Layers for Peripheral Component Interface (PCI) Mezzanine Cards, PMC, April 1995*
- *ATSC Document A/53, ATSC Digital Television Standard, 16 September 1995*
- *IEEE 1496, S Bus: Backplane (Missile Subdomain)*
- *IEEE 1394: 1994, Standard for a High Performance Serial Bus (Aviation Subdomain)*
- *HSDB: High Speed Data Bus (Aviation Subdomain)*
- *PIB: Parallel Interface Bus (Aviation Subdomain)*
- *TMB: Test and Maintenance Bus (Aviation Subdomain)*
- *IEC 1158/ANSI 850: Fieldbus Standard, 1996*

APPENDIX G - MODELING & SIMULATION DOMAIN EXCEPTIONS AND EXTENSIONS

G.1 INTRODUCTION

The Modeling and Simulation (M&S) Domain consists of live, virtual and constructive models and simulations.

G.1.1 Purpose

This Appendix identifies the minimum information standards applicable to all Army M&S.

G.1.2 Scope

This Appendix provides a set of standards affecting the definition, design, development, and testing of M&S. A model is a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. A simulation is a method for implementing a model(s) over time. Also a simulation is a technique for testing, analysis or training in which real-world systems are used, or where real-world and conceptual systems are reproduced by a model.

Army modeling and simulation ranges from high fidelity engineering simulations to highly aggregated, campaign-level simulations. More specifically it covers the development and use of live, virtual, and constructive M&S including simulators, stimulators, emulators, and prototypes for the purpose of training, analysis, acquisition and development support, or other experimentation. Examples include manned vehicle (virtual) simulators, computer generated forces, integrated simulations, environment simulators, closed form simulations, and interfaces to ranges, C4I systems, and other live players.

M&S developed as an integral part of a weapons system or other Army operational system will be managed IAW the JTA-Army main body, applicable appendices of the JTA-Army and mandates covering the larger system.

G.1.3 Background

The *Department of Defense* (DOD) *Modeling and Simulation Master Plan* (MSMP), authorized by DOD Directive (DODD) 5000.59, *DoD Modeling and Simulation Management*, dated January 4, 1994, provides overall management and technical guidance for all DOD M&S. AR 5-11, *Management of Army Models and Simulations* (draft), dated December 1996, and the *Army Model and Simulation Master Plan* provide additional guidance for Army M&S.

Objective 1 of the DOD and Army MSMPs states ..."Provide a common technical framework for M&S" and includes, under sub-objective 1-1, the establishment of a common high level simulation architecture to facilitate interoperability of all types of simulations among themselves and with C4I systems, as well as facilitate the reuse of M&S components. To meet this objective the Under Secretary of Defense for Acquisition and Technology (USD A&T) designated the High Level Architecture (HLA) as the standard technical architecture for all DOD simulations. The HLA is a technical architecture that applies to all classes of simulations, including live, virtual and constructive simulations. The live simulation class encompasses operational platforms, instrumented ranges and C4I systems. The virtual simulation class comprises human-in-the-loop simulators. The constructive simulation class includes wargames and other automated simulation systems.

As is noted in Sections G.2 through G.4, the efficient and effective use of models and simulations across the Department of Defense requires a common technical framework for M&S to facilitate interoperability and reuse. This technical framework consists of:

(1) a common high-level architecture (HLA) to which all simulations must conform;

(2) conceptual models of the mission space (CMMS) to provide a basis for the development of consistent and authoritative simulation representations; and

(3) data standards to provide common representations of data across models, simulations, and C4I systems.

On September 10, 1996, the Under Secretary of Defense for Acquisition and Technology, Dr. Kaminski, designated the HLA as the standard technical architecture for all DOD simulations. Dr. Kaminski's directive requires that all simulations be HLA compliant by October 1st, 1998. During the transition period from DIS/ALSP to full implementation of HLA, the standards listed in G.2 to G.3 are acceptable. The IEEE Standard 1278 is described in both the Information Transfer and the Information Modeling and Data Exchange sections of this appendix. Based upon its application in these two areas, it defines an interoperable simulation environment, and specifies the requirements that need to be met by simulations participating in a Distributed Interactive Simulation. The standards of the CMMS and common representations of data will be provided in subsequent versions of this document

The DOD High Level Architecture (HLA) for Simulations provides the framework for standards for DOD simulations. The 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 HLA provides a common architecture for all classes of simulation and, consequently, the HLA will support DIS and ALSP distributed simulation architectural requirements.

The DOD Architecture Management Group (HLA Management Plan, Version 1.6, 17 July 1995) is responsible for defining the HLA. An initial HLA definition was established in March 1995, and based on the activities of the Architecture Management Group, a baseline definition was created in August 1996. As established in the DOD MSMP, the HLA under this baseline definition shall be a requirement of all DOD simulations. This appendix describes the critical elements of the HLA, since they are the defining requirements for simulations for the DOD.

The Simulation Interoperability Standards Organization (SISO), which grew out of the DIS Standards organization, has made a commitment to develop standards that apply across multiple classes of simulations by incorporating the HLA and affiliated standards, and hence to support the full range of DOD simulation needs. DIS is a government/industry initiative to define standards for linking various elements of the simulation domain. To date, DIS standards have been applicable to the class of virtual simulation. The current DIS standard (IEEE Standard 1278) is described in the Information Transport Processing and the Information Modeling and Data Exchange Standards sections of this appendix.

G.2 INFORMATION PROCESSING STANDARDS

G.2.1 Scope

G.2.2 Mandates

G.2.2.1 Exceptions

There are no exceptions to the standards in the main body of the JTA-Army.

G.2.2.2 Extensions

G.2.2.2.1 High Level Architecture (HLA) for Simulations (Reference Section 2.2)

The HLA (DOD HLA Mandated Baseline Definition, September 10, 1996) is defined by HLA Rules, the HLA Interface specification and the Object Model Template Specification. In order to promote a clearer understanding of the scope of this mandate, it is necessary to understand the difference between a model and a simulation. A model is "a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process"; whereas, a simulation is "a method for implementing a model over time." The intention is for HLA compliance to be required of simulations, and not models. This would mean that model based analysis tools (e.g. spreadsheets, linear programs) would not be included, although certain users may find HLA to be beneficial for use with this type of tool and therefore desirable.

The following standards are mandated:

- HLA Rules Version 1.0, 15 September 1996: The HLA rules describe the responsibilities of federates (simulations or supporting utilities) and federations (sets of simulations working together to support HLA distributed applications). The rules comprise a set of underlying technical principles for the HLA. For federations, the rules address the requirement for a federation object model, object ownership and representation, and data exchange. For federates, the rules require a simulation object model, time management in accordance with RTI time management services, and certain restrictions on attribute ownership and updates.
- Interface Specification Version 1.0, 15 September 1996: In the 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 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 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 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.2.2.2.2 User Interface Services (Reference Section 2.2.2.1.2)

As an extension to the mandates in Section 2.2.2.1.2, domain applications that require user interaction shall use Motif/X Windows APIs and be capable of executing in the CDE, or the applicable native windowing Win32 APIs. The Motif/X Window APIs should be used for systems requiring high multi-user performance, or when required for reuse of existing POSIX/Unix software. The Win32 APIs are more appropriate for systems requiring substantial use/reuse of COTS/GOTS products on X86 platforms. The following standard is mandated and noted as an extension:

- Microsoft Developer Network Win32 Software Development Kit (SDK), Microsoft.

G.2.2.2.3 Data Management Services (Reference Section 2.2.2.1.3)

This domain may develop or acquire client applications that use Microsoft data management services. In those instances, the following standard may be applied:

- Open Data Base Connectivity (ODBC), ODBC 3.0: Provides standard call level APIs between database application clients and the database server. It is noted that use of this standard is an extension to the standard as defined in the body of the JTA-Army. This ODBC standard is contained in the WIN 32 Software Development Kit referenced in Section G.2.2.2.2.

G.2.2.2.4 Operating System Services (Reference Section 2.2.2.1.7)

As an extension to the mandates in Section 2.2.2.1.7, services shall be accessed by applications through either the applicable standard POSIX APIs or Win32 APIs. The POSIX APIs should be used for systems requiring high multi-user performance, or when required for reuse of existing POSIX/Unix software. The Win32 APIs are more appropriate for systems requiring substantial use/reuse of COTS/GOTS products on X86 platforms. The following standard is mandated and noted as an extension:

- Microsoft Developer Network Win32 Software Development Kit (SDK), Microsoft.

G.2.3 Emerging Standards

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, 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. The Functional Description of the Battlespace (FDB) is the Army's portion of CMMS.

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.

G.3 INFORMATION TRANSPORT STANDARDS

G.3.1 Scope

G.3.2 Mandates

G.3.2.1 Exceptions

There are no exceptions to the standards in the main body of the JTA-Army.

G.3.2.2 Extensions (Reference Section 3.2)

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.

The following standard is in addition to those found in the main body of the JTA-Army. It is approved for use during the transition to the HLA.

- IEEE 1278.2-1995: DIS Communication Services and Profiles.

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. This standard provides service requirements and associated profiles that can be individually selected to meet specific DIS system operational requirements.

G.3.3 Emerging Standard

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). Additionally, 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

G.4.1 Scope

G.4.2 Mandates

G.4.2.1 Exceptions

There are no exceptions to the standards in the main body of the JTA-Army.

G.4.2.2 Extensions

G.4.2.2.1 DIS Application Protocols (Reference Section 4.2)

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.

The following standard is in addition to those found in the main body of the JTA-Army. It is approved for use during the transition to the HLA.

- IEEE 1278.1-1995: DIS Application Protocols.

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. 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.4.2.2.2 Standard Simulator Database Interchange Format (SIF) (Reference Section 4.2)

The following standard is mandated:

- MIL-STD-1821, Standard Simulator Data Base (SSDB) Interchange Format (SIF) Design Standard.

This DOD data exchange standard was adopted as an input/output vehicle for sharing externally created simulator databases among the operational system training and mission rehearsal communities.

G.4.3 Emerging Standards

The next generation of protocol catalogs, the Object Model Library (OML) and the Object Model Content Standards Repository (OMCSR) will include data exchanged in other classes of simulations, and will provide a resource for developing object models for HLA applications.

SIF will be replaced by the Synthetic Environment Data Representation Interchange Specification (SEDRIS). 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, sound, textures, symbols, and special effects.

G.5 HUMAN-COMPUTER INTERFACES

G.5.1 Scope

Same as Section 5 of the main body of the JTA-Army.

G.5.2 Mandates

G.5.2.1 Exceptions

There are no exceptions to the standards in the main body of the JTA-Army.

G.5.2.2 Extensions

G.5.2.2.1 Commercial Style Guides (Reference Section 5.2.2.1)

As an extension to the mandate in Section 5.2.2.1 and for Windows based systems, the following standard is mandated:

- The Windows Interface Guidelines for Software Design, Microsoft, 1995.

G.5.3 Emerging Standards

There are no exceptions or extensions to the emerging standards in the main body of the JTA-Army.

G.6 INFORMATION SECURITY

There are no exceptions or extensions to the standards in the main body of the JTA-Army.

APPENDIX H - JTA-ARMY VERSION CHANGE MATRIX

H.1 ATA 4.0 TO ATA 4.5 CHANGE MATRIX

A summary of the changes between ATA Version 4.0 and ATA Version 4.5 is listed in the tables below.

TABLE H-1 SECTION 1, TECHNICAL ARCHITECTURE OVERVIEW CHANGES

ATA 4.5 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	The same for the Army and the joint community.
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	Army compliance document.
1.1.5	JTA	None	JTA 1.0 is one of 5 primary sources, remove TAFIM discussion	Accuracy
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	Accuracy
1.2.1	DII COE	GCCS	DII	Updated

TABLE H-2 SECTION 2, INFORMATION PROCESSING STANDARDS CHANGES

ATA 4.5 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	Updated
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	Lack of market support
2.2.2.1.4.1	Data Interchg Svs	HTML 3.0	HTML 2.0 mandated HTML 3.2 emerging	HTML 3.0 abandoned
2.2.2.1.4.1	Data Interchg Svs	Table 2-1 Emerging	JTA Table 2-1 - Mandated	Minimal set
2.2.2.1.4.2	Graphics Data Interchg	DMA Geo Data Stds JPEG	New section + WGS 84 JPEG File Interchange Format	Updated
2.2.2.1.4.3	Imagery Data Interchg	NITFS - Except TACO2	NITFS - Broken out w/o TACO2	Updated
2.2.2.1.4.7	Video Data Interchg	MPEG-1 Mandated MPEG-2 Emerging	MPEG-1 & 2 Mandated	Updated
2.2.2.1.4.8	Atmos Data Interchng	None	Mandated	Updated
2.2.2.1.4.9	Ocean Data Interchg	None	Mandated	Updated
2.2.2.1.7	Operating Sys Svs	POSIX suite (-)	POSIX suite + updated 1003.1	* Updated
2.2.2.2.4	Distrib Comp Svs	X/Open XFN CORBA Emerging	XFN Deleted CORBA Emerging	JTA - CORBA Mandated

TABLE H-3 SECTION 3, INFORMATION TRANSFER STANDARDS CHANGES

ATA 4.5 Section	Item	ATA 4.0	ATA 4.5	Remarks
3.2.1.3	BOOTP	Included	Added RFC-1533	Updated
3.2.1.3	Connectionless appl. 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)	Updated
3.2.2	BGP V4	Mandated RFC-1654	Replaced RFC-1654 w/ RFCs 1771 & 1772	Updated
3.2.2	BOOTP	Mandated	Added RFCs mandates	Updated
3.2.2	OSPF	Multicast OSPF (RFC-1584)emerging	Mandated RFC-1584	Updated
3.2.2	Trivial FTP protocol	None	STD-33	Updated
3.2.3.1	Serial Lines	PPP and LAPB	Dropped LAPB for routers	Updated
3.2.3.2	JTF LAN	None	IEEE 802.3, 10Base-T	Updated
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	Updated
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

ATA 4.5 Section	Item	ATA 4.0	ATA 4.5	Remarks
4.2.2	Data Model	Enterp Data Model	Def Data Model	Updated
4.2.2	Data model devel.	DOD 8320.1-M-X	DOD 8320.1-M-1	Updated
4.2.4.6 4.2.5	Data Exch Emerging Stds & Mod & Sim.	Separate paragraphs	4.3 Emerging Std updated Removed Mod & Sim	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	Correctness
4.2.4.4	TADIL Msgs	TADIL J Series...	J-Series of TDLs: Added JTIDS TIDP-TE, and STANAG 5516 - Link 16	Jointness - * (between sys. that use a Joint Tactical Data Link)
4.3.3	MIDS	Emerging	Removed	Updated

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

ATA 4.5 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	Updated
5.3	Emerging Stds	DII UI Spec &	CDENext Style Guide & Wpn Sys Style Guide	Updated

TABLE H-6 SECTION 6, INFORMATION SECURITY CHANGES

ATA 4.5 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	Updated
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	Updated
6.2.1.2	Appl Platform Entity	DCE Security - Emerging	Kerberos - RFC-1510 - for use w/ DCE 1.1	Updated
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	Updated
6.2.2.1	Emerging Stds - App. Sw Entity	ISO/IEC DII 10181 OSI	Deleted	Updated
6.2.2.2	Emerging Stds - App Platform SW	SOCKS	Deleted	Updated
6.2.2.4	Security Extension	FTP Security Extn	Deleted	Updated
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

ATA 4.5 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

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

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

ATA 4.5 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

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

H.2 ATA 4.5 TO JTA-ARMY 5.0 CHANGE MATRIX

A summary of the changes between ATA Version 4.5 and JTA-Army Version 5.0 is listed in the tables below.

TABLE H-11 SECTION 1, TECHNICAL ARCHITECTURE OVERVIEW CHANGES

JTA-Army 5.0 Section	Item	ATA 4.5	JTA-Army 5.0	Remarks
1.2.2	Applicable standards	Included	"If a system relates to a domain, then both the core and domain standards apply to that system."	Clarified
1.2.2	Appendix G lead agency	STRICOM	AMSO	Updated
1.2.2	Emerging Standards	Included	Added areas that are "still evolving or do nor exist"	Added emerging technology for Ap. F in this version

TABLE H-12 SECTION 2, INFORMATION PROCESSING STANDARDS CHANGES

JTA-Army 5.0 Section	Item	ATA 4.5	JTA-Army 5.0	Remarks
2.2 2.2.1	COE	Concept & DII 2.0 APIs	Concept & public DII COE 3.1 APIs for DII systems	Army COE Implementation Guidance Letter In-Process
2.2.2.1.1.1	Programming Languages	Ada 95	3GLs- Ada 95 & C (C++ Emerging)	4GL - None None in JTA 1.0
2.2.2.1.3	Data Management	FIPS 127-2 (ODBC 2.0 - App D)	ISO 9075-1 (FIPS 127-2), ISO 9075-3 (ODBC 3.0 - App D)	Sustainment Domain Leverages of Commercial PC Software Market
2.2.2.1.4.1	Document Interchange	FIPS PUB 152	ISO 8879	Updated
2.2.2.1.4.1 Table 2-1	Document Interchange	Table 2-1 from JTA 1.0	Table 2-1 (No chg from 4.5)	The same for the Army and the joint community.
2.2.2.1.4.2	Graphics Data Interchg	JTA DMA Geo Stds - DTED WGS84 & JPEG	JTA DMA Geo Stds - DTED WGS84 & JPEG - PNG - Emerging	The same for the Army and the joint community.
2.2.2.1.4.4	Imagery Data Interchg	JTA Specific NITFS. Proc. stds (only for secondary imagery dissem.)	JTA Specific NITFS Processing standards (only for secondary imagery dissemination) (No chg from 4.5)	The same for the Army and the joint community.
2.2.2.1.4.6 2.2.2.1.4.7	Video Data & Audio Interchange	MPEG-1 & 2 Mandated (Video only)	Audio - MPEG-1 Layer 3, Video - MPEG-1&2 (JTA)	The same for the Army and the joint community. Added open digital audio file interchange format
2.2.2.1.4.8 2.2.2.1.4.9	Atmos & Ocean Data Interchg	JTA 1.0	JTA 1.0	The same for the Army and the joint community.
2.2.2.1.5	Graphic Services	FIPS PUB 120-1, 153	ISO 7942, 9592	The same for the Army and the joint community.
2.2.2.2.4	Distrib Comp Srvs	Same as 4.0	JTA - OSF-DCE 1.1	CORBA still emerging
2.3.2	Win32 APIs	Sustainment Domain	Win32 APIs are emerging	Emerging for C3I and Weapons Domain. Mandated for the Sustainment and M&S Domains.

TABLE H-13 SECTION 3, INFORMATION TRANSFER STANDARDS CHANGES

JTA-Army 5.0 Section	Item	ATA 4.5	JTA-Army 5.0	Remarks
3	Section format			Modified format
3.2.1.1.1.1	Electronic Mail	DMS	DMS and non-DMS (RFC-821, RFC-822)	Included non-DMS electronic mail
3.2.1.1.1.5	Network and Systems Management	Included	Moved to new 3.2.5	Updated
3.2.1.1.1.6	Network time	None	RFC-1305	The same for the Army and the joint community.
3.2.1.2	VTC, 56-1,920 kbps	H.320	Added H.321 that is an adaptation of H.320	Updated
3.2.1.2	VTC, 56-1,920 kbps	None	H.224, H.281, H.244	Updated
3.2.1.2	VTC applications	T.120 series	Listed T.120, T.122, T.123, T.124, T.125, T.126, T.127	Updated
3.2.1.2	VTC picture format resolution	None	ITU-T H.261, ITU-T G.711, ITU-T G.728	Updated
3.2.1.3	Facsimile	None	TIA/EIA 465-A, TIA/EIA 466, MIL-STD-188-161D	The same for the Army and the joint community.
3.2.2.1	Router, DHCP	None	RFC-1541	Updated
3.2.2.2.1	Ethernet	IEEE 802.3u	Replaced by ISO/IEC 8802-3	ISO/IEC 8802-3 replaces 802.3 and 802.3u as a combined updated international standard.
3.2.2.2.1	Ethernet	None	100Base-T, 100Base-F	Updated
3.2.2.2.1	Ethernet, bridging	None	ISO/IEC 10038	Updated
3.2.2.2.1	Ethernet, management	None	ISO/IEC 15802-2	Updated
3.2.2.2.2	Point to Point	RFC-1333	RFC-1989	Superseded and adopted
3.2.2.2.2	Point to Point	RFC-1334	RFC-1994	Superseded and adopted
3.2.2.2.2	Point to Point	None	RFC-1990	Updated
3.2.2.2.4	ISDN	I.430, I.311, National ISDN 1, National ISDN 2, RFC-1356, Q.921, Q.931	Replaced with: ANSI T1.601, T1.408, T1.602, T1.607, T1.607a, T1.610, T1.619, T1.619a, SR-3875, SR-3888, SR-3887	Updated

TABLE H-13 SECTION 3, INFORMATION TRANSFER STANDARDS CHANGES (CONTINUED)

JTA-Army 5.0 Section	Item	ATA 4.5	JTA-Army 5.0	Remarks
3.2.2.2.5	ATM	None	Physical Interface Spec. UNI V3.1, DS1 Physical Layer Spec., DS3 Physical Layer Interface Spec., UNI Spec V3.1, ILMI, ILMI MIB, UNI Signaling, Traffic Managt Spec., PNNI, LAN Emulation Client Managt, LANE 1.0, LANE Servers Managt	Updated
3.2.2.2.5	ATM	RFC-1577	Replaced by LANE 1.0	Updated
3.2.2.2.6	X.25	None	ANSI X3.100a	Supplement
3.2.3.3	Transmission media, SONET	None	Added: 4 ANSI standards	The same for the Army and the joint community.
3.2.5.1	NSM data communications	None	RFC-1514, STD-50, RFC-1757, RFC-1850	Updated, SNMP for data communications
3.2.5.2	NSM telecommunications	None	ANSI T1.204, T1.208, ITU-T M.3207.1, ITU-T M.3211.1, ITU-T M.3400, ISO/IEC 9595, 9596-1, 9596-2	Updated, added TMN/CMIP standards for telecommunicatio ns

TABLE H-14 SECTION 4, INFORMATION MODELING AND DATA EXCHANGE STANDARDS CHANGES

JTA-Army 5.0 Section	Item	ATA 4.5	JTA-Army 5.0	Remarks
4	Activity Model	Process Model	Activity Model	Consistency
4.2.2	Data model	During PDR and CDR, and prior to Milestone II	Prior to Milestone II	Correctness
4.2.4.4	JTIDS	Test edition	MIL-STD-6016	Updated
4.2.4.4	VMF	None	Added VMF TIDP-TE	Updated
4.2.4.6	Database to Database Exchange	None	Added new paragraph and DDDS mandate	Updated
4.2.6	Calendar Date Data Format	None in ATA 4.5, 12 NOV 1996, but was added by 21 APR 1997 memorandum	DDS and ISO 8601 mandates	Y2K

TABLE H-15 SECTION 5, HUMAN-COMPUTER INTERFACES CHANGES

JTA-Army 5.0 Section	Item	ATA 4.5	JTA-Army 5.0	Remarks
5.2.1	General: Mixing of user interface styles	However, graphical and character-based interface styles shall not be mixed within the same application or family of applications.	In order to present a consistent interface to the user, graphical and character-based application user interface styles should not be mixed.	TAWG, Clarity
5.2.1	Hybrid GUIs	...mix interface styles (e.g., MOTIF and Windows)	A hybrid GUI is one that uses tool kit components from more than one user interface style. An example of a hybrid GUI is one that uses tool kit components from both MOTIF and Windows.	The same for the Army and the joint community.
5.2.2	Style Guides		Added definition of what a style guide is and explanation of what one does.	The same for the Army and the joint community.
5.2.2	Style Guides	Emerging	MIL-STD-1472E	Updated
5.2.2.1	MOTIF Style Guide	Mandated for all GUIs	Mandated for MOTIF based systems	Congruence with Sec 2 mandates
5.2.2.1	CDE	Emerging	'...the user interface "look and feel" shall be based on and consistent with the CDE version of MOTIF.'	Congruence with CDE 1.0 mandate in Sec 2
5.2.2.2	DOD HCI Style Guide	TAFIM Version not specified	TAFIM Version 3.0, Volume 8, 30 April 1996	Updated
5.2.2.3	WSHCI Style Guide		Removed explanatory paragraph.	Readability
5.2.2.3	WSHCI Style Guide	Included	Moved to F.5.2.2.2	For weapons domain only
5.3	MIL-STD-1472	MIL-STD-1472E was emerging	Moved MIL-STD-1472E to mandated; added MIL-STD-1472-F to emerging	Updated
5.3	CDE	CDENext Style Guide	CDENext renamed CDE 2.1, uses MOTIF 2.1 Style Guide.	Updated

TABLE H-16 SECTION 6, INFORMATION SECURITY CHANGES

JTA-Army 5.0 Section	Item	ATA 4.5	JTA-Army 5.0	Remarks
6.2.1.2	Password Usage	None	FIPS PUB 122	Updated
6.3.1.1	Security protocols	None	MIL-STD-2045-18500, SDN.903, SND.301	Updated
6.3.1.2	DMS interface	None	FORTEZZA Application Implementor's Guide, MD4002101-1.52	Updated

TABLE H-17 APPENDIX D, SUSTAINMENT DOMAIN EXCEPTIONS AND EXTENSIONS CHANGES

JTA-Army 5.0 Section	Item	ATA 4.5	JTA-Army 5.0	Remarks
D.2.2.2.1	Win32 APIs User Interface Services	Included	Win32 SDK	Can use Motif/X Window or Win32 depending on requirements.
D.2.2.2.2	ODBC	ODBC 2.0	ODBC 3.0	ODBC 2.0 is no longer available
D.2.2.2.3	USACE direction	None	FIPS 173 Spatial Data Transfer Standard (SDTS)	Presidential Executive Order 12906 mandate
D.2.2.2.4	Win32 APIs OS	Included	Win32 SDK	Can use POSIX or Win32 depending on requirements.
D.3.2.2.1	Medical communications	None	HL7, DICOM V3.0	Updated
D.5.2.2.1	Commercial style guides	Included	Windows Interface Guidelines	Can use Windows style guide depending on requirements.

TABLE H-18 APPENDIX E, C3I DOMAIN EXCEPTIONS AND EXTENSIONS CHANGES

JTA-Army 5.0 Section	Item	ATA 4.5	JTA-Army 5.0	Remarks
E.3.2.2.1.1	Secondary Imagery Dissemination Standards	None	MIL-STD-2045-44500 (TACO2)	The same for the Army and the joint community.
E.3.2.2.3.1	Transmission media, SATCOM	None	Added: 8 military standards	The same for the Army and the joint community.
E.3.2.2.3.2	Transmission media, radio communications	None	Added: 6 military standards, 1 STANAG, 1 specification	The same for the Army and the joint community.

TABLE H-19 APPENDIX F, WEAPONS SYSTEM DOMAIN EXCEPTIONS AND EXTENSIONS CHANGES

JTA-Army 5.0 Section	Item	ATA 4.5	JTA-Army 5.0	Remarks
F.2.1.1 Figure F.2-1	TRM extension for weapons	None	TRM extension	Added GOA model from emerging
F.5.2.2.1	Symbology	MIL-STD-2525A	Moved MIL-STD-2525A to Section 5.2.1.3	In main body
F.5.2.2.1	Symbology	None	MIL-STD-1295 and MIL-STD-1787	Updated
F.5.2.2.2	Style Guide	None	WSHCI Style Guide	Moved from Section 5 to domain
F.7.2.2.1.1	Bus Interface	None	MIL-STD-1553B, ANSI/VITA 1, PICMG Compact PCI Spec., MIL-STD-1773, SAE J 1850, ANSI X3.131	Updated
F.7.2.2.1.2	General hardware interface	None	PCMCIA, IEEE 1101.2, EIA 170, EIA 330, EIA 343-A, SMPTE 170M, MIL-STD-1389D	Updated

TABLE H-20 APPENDIX G, MODELING & SIMULATION DOMAIN EXCEPTIONS AND EXTENSIONS CHANGES

JTA-Army 5.0 Section	Item	ATA 4.5	JTA-Army 5.0	Remarks
G.1.2	Scope	Included	Refined the scope. Addressed the exclusion of embedded M&S (See AR 511)	Clarification
G.2.2.2.2	User Interface Services	None	Win32 SDK	May use Motif/X Windows or Win32 APIs
G.2.2.2.3	Data Management Services	None	ODBC 3.0	Win32 option
G.2.2.2.4	Operating System Sercices	None	Win32 SDK	POSIX or Win32
G.4.2.2.1	DIS Exercise Manag. and Feedback	IEEE 1278.3	None	Deleted to make HLA compliant
G.4.2.2.2	Sim. Database Interch. Format (SIF)	None	MIL-STD-1821	Updated
G.5.2.2.1	Commercial Style Guides	None	Windows Interface Guidelines	Win32 option

This page was intentionally left blank.

APPENDIX I - JTA-ARMY VERSION 5.0 COMPARISON TO JTA 1.0 MATRIX

A summary of the differences between JTA Version 1.0 and JTA-Army Version 5.0 is listed in the tables below.

TABLE I-1 SECTION 1, TECHNICAL ARCHITECTURE OVERVIEW COMPARISON

JTA-Army 5.0 Section	Item	JTA 1.0	JTA-Army 5.0	Remarks
1	Overview			No mandates

TABLE I-2 SECTION 2, INFORMATION PROCESSING STANDARDS COMPARISON

JTA-Army 5.0 Section	Item	JTA 1.0	JTA-Army 5.0	Remarks
2.2	DII COE	DII COE I&RTS level 5 compliant (software is segmented, uses DII COE Kernel, and is installed via COE tools)	COE concept, segment their applications in accordance with the DII COE I&RTS Version 2.0, and use the DII COE 3.1 public APIs	Mandate the public APIs
2.2.2.1.1.1	Programming languages	DODD 3405.1	Refer to DODD 3405.1. ISO/IEC 8652 (Ada 95), ISO/IEC 9899 - C ISO/IEC 9899/Cor. 1 - C ISO/IEC 9899/Cor. 2 - C ISO/IEC 9899/Amd. 1 - C	Added C.
2.2.2.1.1.2	Language Bindings	None	IEEE 1003.5	Updated
2.2.2.1.2, D.2.2.2.1, G.2.2.2.2	User Interface Services	For C3I sys.: Win32 APIs, Window Manag. and Graphics Device Interface, Vol. 1 Microsoft Win32 Prog. Refer. Manual	None in 2.2.2.1.2. In D.2.2.2.1, G.2.2.2.2, Microsoft Developer Network Win32 Software Development Kit (SDK), Microsoft. None in Ap. E for C3I.	Win32 can be used in Sustainment and M&S Domains.
2.2.2.1.3	Data management services	FIPS Pub 127-2: 1993, Open Data Base Conn., ODBC 2.0	ISO/IEC 9075 as modified by FIPS Pub 127-2, ISO/IEC 9075-3	Updated

TABLE I-2 SECTION 2, INFORMATION PROCESSING STANDARDS COMPARISON (CONTINUED)

JTA-Army 5.0 Section	Item	JTA 1.0	JTA-Army 5.0	Remarks
2.2.2.1.4.3	Geospatial Data Interchange (DTED)	DMAL 805-1A, DMA List of Prod. and Services	MIL-D-89020, Digital Terrain Elevation Data (DTED)	Updated
2.2.2.1.4.5	Product Data Interchange	None	MIL-PRF-28000A	Updated
2.2.2.1.4.6	Audio Data Interchange	ISO/IEC 11172-1 ISO 13818-1 ISO 13818-3		No MPEG-2 audio
2.2.2.1.4.7	Video Data interchge (MPEG-1)	Not included	ISO/IEC 11172-3, ISO/IEC 11172-3/Cor. 1	Updated
2.2.2.1.4.7	Video Data interchge (MPEG-2)	Not included	ISO 13818-3	Updated
2.2.2.1.4.10	File compression	None	RFC-1952, GZIP File Format Specification	Updated
2.2.2.1.4.11	Electronic commerce data interchange	None	FIPS Pub 161-1, Elect. Data Interchge (EDI)	Updated
2.2.2.1.5	Graphic Services	ISO/IEC 9636: 1994	Not included	Updated
2.2.2.1.7, D.2.2.2.4, G.2.2.2.4	Operating System Services	For C3I systems: IEEE 1003.1b IEEE 1003.1I IEEE 1003.1c Win32 APIs	None in 2.2.2.1.7. In D.2.2.2.4, G.2.2.2.4, Microsoft Devel. Network Win32 Software Develop. Kit (SDK), Microsoft. None in Ap. E for C3I.	Win32 can be used in Sustainment and M&S Domains.
2.2.2.2.4.1	Remote Procedure Computing	- OSF - DCE Remote Procedure Call (RPC) - OSF - DCE Time Services - OSF - DCE Directory Services	Open Group CAE Spec. C309 8/94 - DCE: Remote Proc. Call which includes DCE IDL, Open Group CAE Spec. C310 11/94, DCE 1.1: Time Serv. Spec., Open Group CAE Spec. C312 12/94, DCE: Dir. Serv.	Updated
2.3.2	Distributed Object Computing	In 2.2.2.2.4.2: OMG - CORBA: Arch. and Spec., OMG - CORBA serv.: Com. Obj. Serv. Spec., OMG - CORBA facil.: Com. Obj. Facil. Arch.	In 2.3.2: CORBA 2.0 is emerging.	Updated

TABLE I-3 SECTION 3, INFORMATION TRANSFER STANDARDS COMPARISON

JTA-Army 5.0 Section	Item	JTA 1.0	JTA-Army 5.0	Remarks
3.2.1.1.1.1	Electronic Mail	DMS	DMS and non-DMS (RFC-821, RFC-822)	Included non-DMS electronic mail
3.2.1.1.1.5, 3.2.5	Network and systems management	In JTA: IAB Standard 15, 16, 17	3.2.5.1 Data Communications - use IAB Standard 15, 16, 17, and added RFC-1514, STD-50, RFC-1757, RFC-1850, 3.2.5.2 Telecommunications - ANSI T1.204, T1.208, ITU-T M.3207.1, M.3211.1, M.3400, ISO/IEC 9595, 9596-1, 9596-2	Updated
JTA 3.2.1.1.1.10	Connectionless Data Transfer	MIL-STD-2045-47001	MIL-STD-2045-47001 in 4.2.4.2	Data format in Section 4
3.2.1.2	VTC, 56-1,920 kbps	None	Added H.321 that is an adaptation of H.320	Updated
3.2.1.2	VTC, 56-1,920 kbps	None	H.224, H.281, H.244	Updated
3.2.1.2	VTC applications	T.120 series	Listed T.120, T.122, T.123, T.124, T.125, T.126, T.127	Updated
3.2.1.2	VTC picture format resolution	None	ITU-T H.261, ITU-T G.711, ITU-T G.728	Updated
3.2.1.5	GPS	Emerging	ASD Memorandum	Updated
3.2.2.1	Ethernet	Not included	Ethernet V2 framing, ISO/IEC 10038 for bridging, ISO/IEC 15802-2 for management	Updated
3.2.2.2.2	Point to Point	RFC-1333	RFC-1989	Updated
3.2.2.2.2	Point to Point	RFC-1334	RFC-1994	Updated
3.2.2.2.2	Point to Point	Not included	RFC-1990	Updated
3.2.2.2.4	ISDN	In JTA and not in JTA-Army: ITU-T Q.921, Q.931, E.164, DCAC 370-175-13, RFC-1356	Additions in JTA-Army: ANSI T1.602, T1.607, T1.607a, T1.610, T1.619, T1.619a, SR-3875, SR-3888, SR-3887	Updated

TABLE I-3 SECTION 3, INFORMATION TRANSFER STANDARDS COMPARISON (CONTINUED)

JTA-Army 5.0 Section	Item	JTA 1.0	JTA-Army 5.0	Remarks
3.2.2.2.5	ATM	In JTA and replaced in JTA-Army: RFC-1577	Additions in JTA-Army: 25.6 Mb/s Over Twisted Pair, DS1 Physical Layer Spec., DS3 Physical Layer Interface Spec., User-Network UNI Spec V3.1, ILMI, ILMI MIB, UNI Signaling, Traffic Management Spec., PNNI, PNNI V1.0 Addendum, LAN Emulation Client Management, LANE 1.0, LANE Servers Management	Updated
3.2.2.2.6	X.25	Not included	ITU-T X.25, ISO 7776, ISO 8208, ACCS-A3-407-008D, ANSI X3.100, ANSI X3.100a	Updated
3.2.2.2.7	FDDI	None	ISO 9314-1, 9314-2, 9314-3, ANSI X3.229, IEEE 802.2, STD-36	Updated
3.2.3.2.1.2	HF Anti-jamming	MIL-STD-188-148	MIL-STD-188-148A	Updated
3.2.3.3	SONET	Not included	ANSI T1.101	Updated
3.3.2	Emerging Network Standards	None	11 standards for NSM for data communications	Updated
3.3.2	Emerging Secondary Imagery Dissemination	None	TACO3	Updated

TABLE I-4 SECTION 4, INFORMATION MODELING AND DATA EXCHANGE STANDARDS COMPARISON

JTA-Army 5.0 Section	Item	JTA 1.0	JTA-Army 5.0	Remarks
4.2.2	Data model	None	Prepared prior to Milestone II or equivalent	Policy
4.2.3	Data definitions	None	DOD Directive 8320.1	Updated
4.2.4.2	Connectionless Data Transfer	In JTA 3.2.1.1.1.10	MIL-STD-2045-47001	Data formats in Section 4
4.2.6	Calendar date data format	None	DDDS and ISO 8601	Y2K

TABLE I-5 SECTION 5, HUMAN-COMPUTER INTERFACES COMPARISON

JTA-Army 5.0 Section	Item	JTA 1.0	JTA-Army 5.0	Remarks
5.2.1.3	Symbology	None	MIL-STD-2525A	Updated
5.2.2	Style guides	None	MIL-STD-1472E	Updated
5.2.2.1, G.5.2.2.1, D.5.2.2.1	Commercial Style Guides	Motif and Win32	None in 5.2.2.1. In G.5.2.2.1, D.5.2.2.1, Motif and Win32	Motif and Win32 for Sustainment and M&S Domains, not C3I Domain
5.2.2.2	DOD HCI Style Guide	Version 2.0	Version 3.0	Updated
5.2.2.3	Domain-level Style Guide	None	DOD HCI Style Guide	Updated
5.3	Emerging	CDE 1.0	Motif 2.1 style guide when CDE 2.1 is mandated	Updated

TABLE I-6 SECTION 6, INFORMATION SECURITY COMPARISON

JTA-Army 5.0 Section	Item	JTA 1.0	JTA-Army 5.0	Remarks
6.2.1.2	Application platform entity	Not included	FIPS PUB 112, RFC-1510	Updated
6.3.1	Evaluation criteria security standards	DOD 5200.28-STD	Not included	Updated
6.3.1.1	Security protocols	Not included	FIPS PUB 196	Updated
6.3.1.2	DMS interface	Not included	FORTEZZA Implementor's Guide, FORTEZZA Cryptologic Interface Programmer's Guide	Updated
6.3.1.3	MISSI Cryptographic algorithms	Not included	NSA SKIPJACK	Updated
6.3.1.4	MISSI digital signature infrastructure	Not included	ITU-T Rec. X.500	Updated
6.4.1	HCI	DOD HCI Style Guide Version 2.0	DOD HCI Style Guide Version 3.0	Updated
6.6	Security related documents	Not included	FIPS PUB 46-2	Updated

TABLE I-7 APPENDIX D, SUSTAINMENT DOMAIN EXCEPTIONS AND EXTENSIONS COMPARISON

JTA-Army 5.0 Section	Item	JTA 1.0	JTA-Army 5.0	Remarks
D.2.2.2	Data management services	None	ODBC 3.0	Updated
D.2.2.2	Geospatial data interchange	None	FIPS PUB 173	Updated
D.3.2.2	Medical information	None	HL7, DICOM V3.0	Updated

TABLE I-8 APPENDIX E, C3I DOMAIN EXCEPTIONS AND EXTENSIONS COMPARISON

JTA-Army 5.0 Section	Item	JTA 1.0	JTA-Army 5.0	Remarks
E.2.2	INFORMATION TRANSFER STANDARDS	Win32 and POSIX APIs are mandated for C3I Domainn	POSIX only.	Win32 APIs are emerging
E.5.2.2	HCI	None	User Interface for the DII	Updated

TABLE I-9 APPENDIX F, WEAPONS SYSTEM DOMAIN EXCEPTIONS AND EXTENSIONS COMPARISON

JTA-Army 5.0 Section	Item	JTA 1.0	JTA-Army 5.0	Remarks
F.2.1.1 Fig. F.2-1	TRM	None	First order extension for weapons systems	Updated
F.2.2.1.1	Graphic services	None	ISO-IEC 9636	Updated
F.5.2.2.1	Symbology	None	MIL-STD-1295, MIL-STD-1477B, MIL-STD-1787	Updated
F.5.2.2.2	Domain-level style guide	None	Army WSHCI	Updated
F.7.2.2.1.1	Bus interface standards	None	MIL-STD-1553B, ANSI/VITA 1, PICMG Compact PCI Spec., MIL-STD-1773, SAE J 1850, ANSI X3.131	Updated
F.7.2.2.1.2	General hardware interface standards	None	PCMCIA, IEEE 1101.2, EIA 170, EIA 330, EIA 343-A, SMPTE 170M, MIL-STD-1389D	Updated

TABLE I-10 APPENDIX G, MODELING & SIMULATION DOMAIN EXCEPTIONS AND EXTENSIONS COMPARISON

JTA-Army 5.0 Section	Item	JTA 1.0	JTA-Army 5.0	Remarks
G.2.2.2.1	HLA for simulations	None	HLA Rules V1.0, Interface Spec. V1.0, Object Model Template V1.0	Updated
G.3.2.2	Distributed Interactive Simulation (DIS)	None	IEEE 1278.2	Updated
G.4.2.2.1	DIS application protocols	None	IEEE 1278.1	Updated
G.4.2.2.2	SIF	None	MIL-STD-1821	Updated