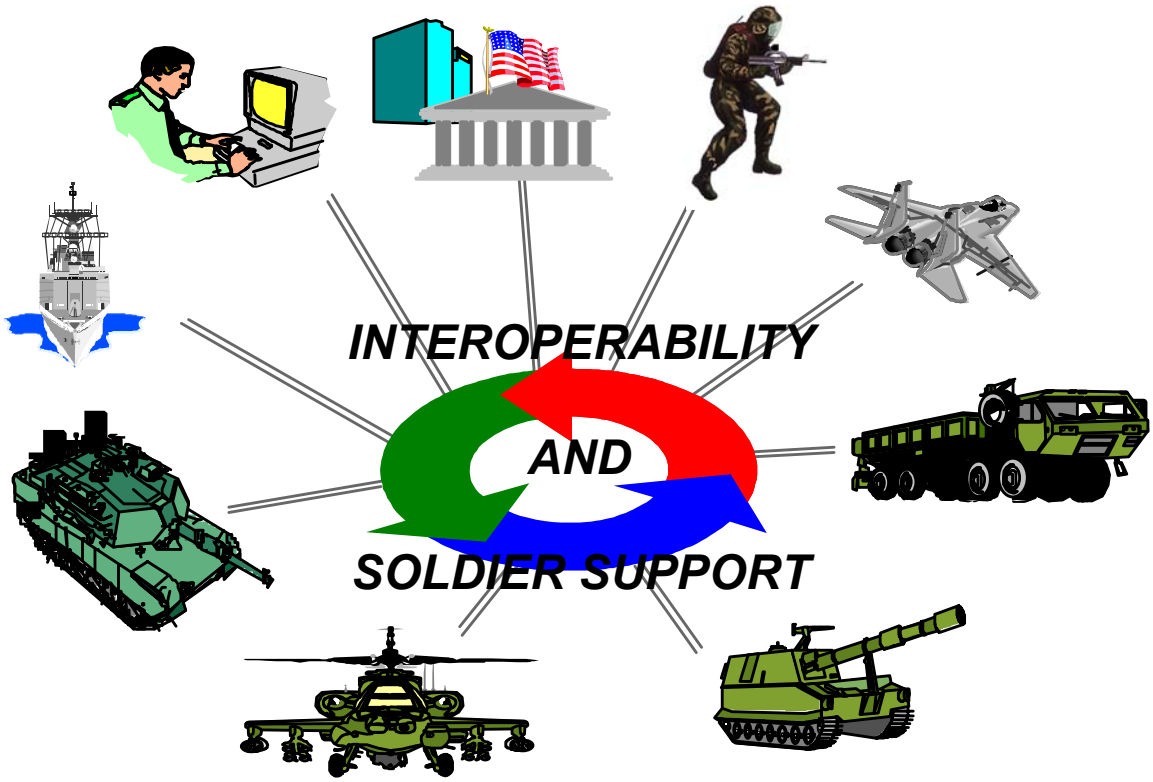
Joint Technical Architecture - Army



Department of the Army

Version 6.5

10 May 2002

Available at http://arch-odisc4.army.mil/aes/aea/jta-a/jtaa65/html/jtaa65.htm

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

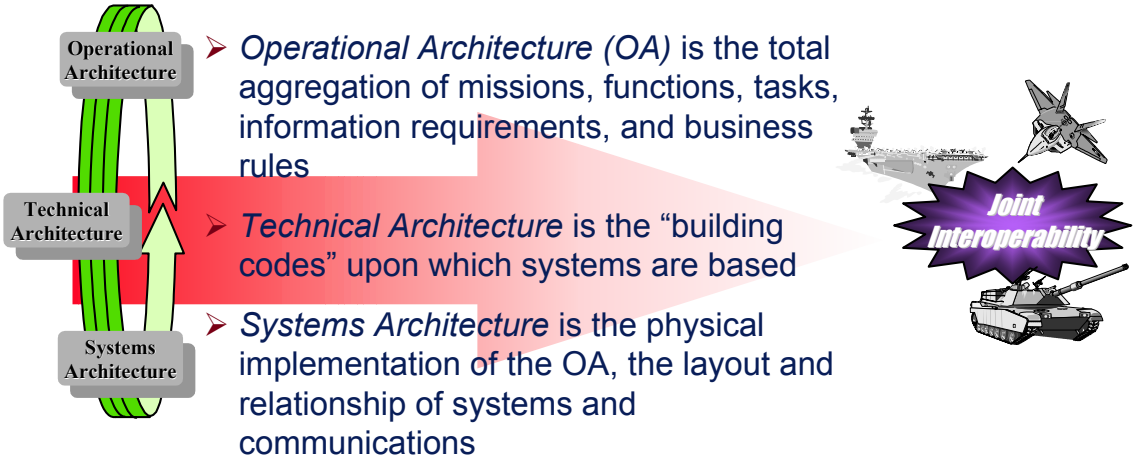
This page was intentionally left blank.

Joint Technical Architecture - Army, Version 6.5
Executive Summary

INTRODUCTION

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

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.



The Joint Technical Architecture - Army (JTA-Army) 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 Joint Technical Architecture (JTA) through the implementation of the JTA-Army. The 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

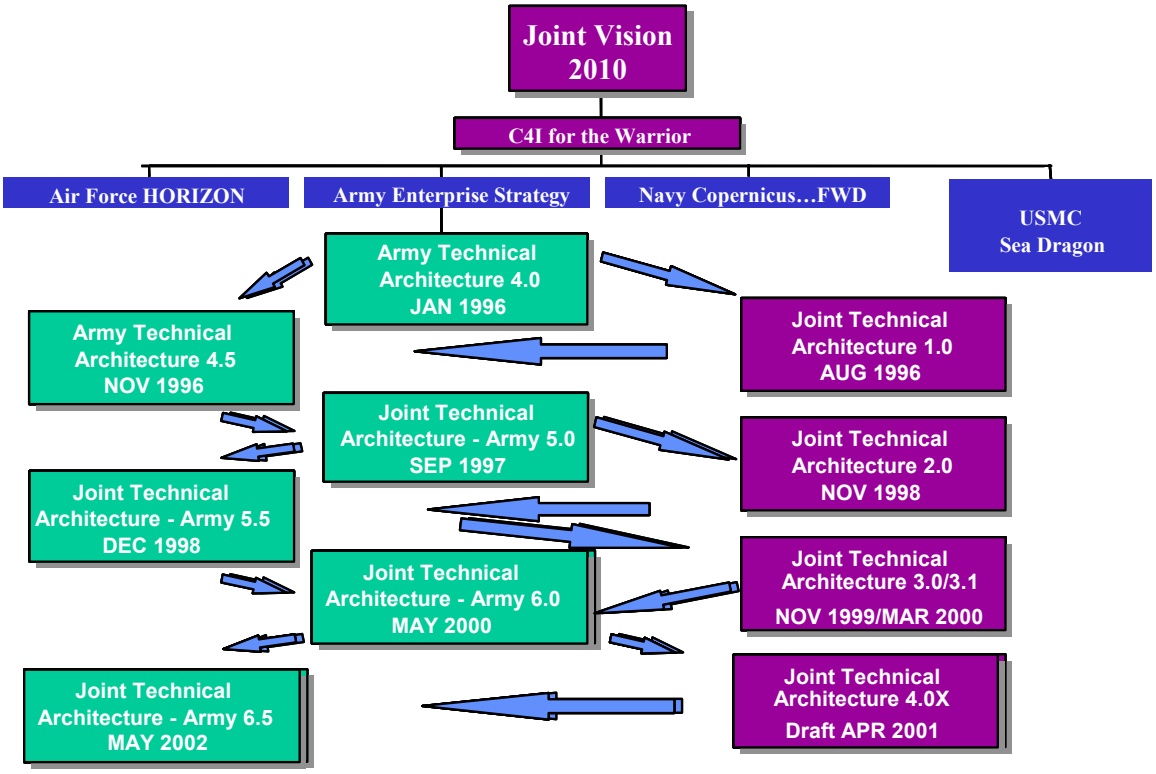
The Joint Technical Architecture - Army (JTA-Army) applies to all systems that produce, use, or exchange information electronically. The JTA-Army will be used by anyone involved in the management, development or acquisition of new or improved systems. Within the Army, the Vice Chief of Staff, Army and 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 Weapon 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 included C and Ada 95 as acceptable programming languages, added SMTP for non-DMS electronic mail, and added network system management standards. Version 5.5 included additional Asynchronous Transfer Mode (ATM) standards, and Date Data Format standards for Year 2000 (Y2K) compliance. Another major change was the use of either the standard Portable Operating System Interface (POSIX®) or the Microsoft ® Win32 Application Program Interfaces (APIs), as applicable, for operating systems (OS) and corresponding Human Computer Interfaces (HCI).

Version 6.0 updates mandated and evolving emerging standards, and includes Gigabit Ethernet standards, the CORBA ORB, Automatic Test System standards and Identification of Friends and Foes (IFF) standards. JTA-Army Version 6.0 aligns with JTA Version 3.1, and also adopts the enhanced DoD Technical Reference Model (TRM) that replaces the Technical Architecture Framework for Information Management (TAFIM) TRM.



WHAT'S NEW IN VERSION 6.5

Version 6.5 will continue to be the central source of Technical Architecture guidance for Army systems. 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. This version is based on the standards in DoD JTA Version 3.1 and draft Version 4.0. Changes include:

- Web enabling standards which support Army Knowledge Management (AKM):

  - Updated HTML 4.01 Specification: Hypertext Markup Language (HTML) is used for hypertext formatted and navigational linked documents.

  - Updated eXtensible Markup Language (XML)-based Information Exchange related standards: XML based information is the widely accepted choice of industry for data/metadata interchange and is vital to the DOD's interoperability strategy.

  - Added Uniform Resource Identifier (URI): A URI is a string identifying an abstract or physical resource on a network. Uniform Resource Locators (URLs) are the subset of URIs that identify resources via their network 'location.

  - Guidance for Personal Digital Assistants (PDAs) and Palmtops: choosing operating systems for hand-held devices.

- Biometric technology:

- Added mandated standard for Biometric Technology Services: Biometric technologies are intended to overlay or replace password systems so that positive access control can be achieved.

- Added mandated Electronic Data Interchange (EDI) standard for Healthcare Environments: ANSI HL7 Health Level Seven Standard.

- Identification:

- Update Bar code standards identify products being shipped and stocked, certain logistics applications, and used on ID cards

- Added emerging standard for Radio Frequency Identification (RFID) to track logistics shipments and other business processes.

- Security:

- Updating the security standards, the Orange Book and its corresponding interpretations known as the Rainbow series are replaced by the Common Criteria: The Common Criteria is a meta-standard (a standard of standards) as it is essentially a list of selectable security requirements (functional and assurance), plus definitions and requirements for how to document security capabilities and needs (as Security Targets and Protection Profiles respectively).

- Smart card standards are mandated, therefore the competing FORTEZZA Cryptographic Card standards are removed.

- Updated the public-key infrastructure (PKI) standards: A PKI supports the following security services: authentication, data integrity, non-repudiation, confidentiality, and (optionally) authorization.

- Wireless:

- Mandate Wireless Local Area Network (LANs) standards: For platforms connected via wireless LAN.

- Added emerging standards for 3rd Generation PCS/Cellular systems: 3G systems need to meet the requirements of supporting data transmission for the vehicular user, the dismounted user and the stationary user.

- Weapons Systems:

- Mandate Weapon System Mapping Services (WSMS) Application Programmer's Interface (API): The WSMS API provides a standardized interface to a set of mapping and mapping related services to be utilized by weapon systems applications in the presentation, interaction, and maintenance of Command, Control, Communications, and Intelligence (C3I) data.

- Mandated Fibre Channel (FC) transport layer technologies standards: FC technology is a popular industry standard in high bandwidth networks such as storage area networks.

- Mandate avionics interconnect bus standards: The standards are widely used in commercial aviation products such as GPS LORAN, ADF, automatic flight controls, moving maps and inertial reference systems.

- Add as emerging in aviation community MIL-STD-1760C: The goal of the standard is to significantly reduce and stabilize the number and variety of signals required at aircraft/store interfaces, minimize the impact of new stores on future stores management systems, and increase store interoperability among the services, within NATO, and with other allies.

- Add as emerging for soldier, ground and munitions weapon systems the Sensor Link Protocol (SLP) Message Set: SLP Message Set was developed for use as a common interface between electro-optical sensor systems and a diverse set of host computer systems.

- Messaging:

- Updated Variable Message Format (VMF) Technical Interface Design Plan (Test Edition), to Reissue 5.

- Updated MIL-STD-6040, United States Message Text Format (USMTF) 31 March 2000.

A more comprehensive catalogue of changes made to JTA-Army, Version 6.5 is contained in Appendix H of the JTA-Army, with respect to Version 6.0 to 6.5. Appendix I is a similar comparison of JTA Version 3.1 to JTA-Army Version 6.5. JTA-Army is available on-line at a World Wide Web (WWW) address, Uniform Resource Locator (URL), of <http://arch-odisc4.army.mil/aes/aea/jta-a/html/homepage.htm>.

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

---

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

This page was intentionally left blank.

INTERNET AVAILABILITY

This document is available electronically on the World Wide Web (WWW) at Uniform Resource Locator (URL) of <http://arch-odisc4.army.mil/aes/aea/jta-a/jtaa65/html/jtaa65.htm>. This 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 E-mail. Submit your comment on the Joint Technical Architecture - Army (JTA-Army) Comment Form. The Comment Form is available on the WWW at URL: <http://arch-odisc4.army.mil/aes/aea/jta-a/html/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.

JTA-Army Standards Evaluation Criteria

The following is a list of specific questions that will be utilized in evaluating the introduction of new JTA-Army standards:

1. Does the introduction of this standard support the JTA-Army objectives of improved system interoperability and/or affordability?

2. What is the nature of the standard (proprietary/open)?

3. What forum is it from (IEEE, SAE, ISO, etc.) and what is its current status (draft, final, approved)?

4. What, if any, existing commercial products have implemented the standard?

5. Where does the standard belong (core mandate, emerging standard, domain specific addition; give section number)?

6. Does the proposed standard create any conflicts with the existing JTA-Army mandates?

In addition, all proposed mandates/emerging standards require the following:

7. A reference that provides a specific name and date for the proposed standard.

More information can be found on the WWW at URL <http://arch-odisc4.army.mil/aes/aea/jta-a/html/homepage.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

SECTION 1 1

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 4
1.1.5 Basis for the JTA-Army Version 6.5 5
1.2 TECHNICAL ARCHITECTURE 6
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, Metadata, and Information-Exchange Standards 8
1.2.2.4 Human-Computer Interfaces 9
1.2.2.5 Information Security 9

SECTION 2 11

INFORMATION PROCESSING STANDARDS 11

2.1 INTRODUCTION 11
2.1.1 Purpose 11
2.1.2 Scope 11
2.1.3 Background 11
2.1.3.1 DoD Technical Reference Model 12
2.2 MANDATES 13
2.2.1 Application Software Entity 13
2.2.1.1 Biometric Technology Services 14
2.2.2 Application Platform Entity 14
2.2.2.1 Service Areas 14
2.2.2.1.1 Software Engineering Services 14
2.2.2.1.1.1 Programming Languages 14
2.2.2.1.1.2 CASE Environments and Tools 15
2.2.2.1.2 User Interface Services 15
2.2.2.1.3 Data Management Services 15
2.2.2.1.4 Data Interchange Services 16
2.2.2.1.4.1 Document Interchange 16
2.2.2.1.4.2 Graphics Data Interchange 17
2.2.2.1.4.3 Geospatial Data Interchange 18
2.2.2.1.4.4 Still Imagery Data Interchange 18
2.2.2.1.4.5 Product Data Interchange 19

2.2.2.1.4.6 Audio Data Interchange 19
2.2.2.1.4.7 Motion Imagery Data Interchange 19
2.2.2.1.4.8 Data Interchange Storage Media 22
2.2.2.1.4.9 Atmospheric and Oceanographic Data Interchange 22
2.2.2.1.4.10 File Compression 22
2.2.2.1.4.11 Electronic Commerce Data Interchange 23
2.2.2.1.5 Graphic Services 23
2.2.2.1.6 Communications Services 23
2.2.2.1.7 Operating System Services 23
2.2.2.1.8 Internationalization Services 24
2.2.2.1.9 Security Services 24
2.2.2.1.10 System Management Services 24
2.2.2.1.11 Distributed Computing Services 25
2.3 EMERGING STANDARDS 25
2.3.1 Application Software Entity 25
2.3.1.1 Environment Management 25
2.3.1.1.1 Learning Technology 25
2.3.1.1.2 Electronic Records Management 26
2.3.1.2 Business Processing 26
2.3.2 Application Platform Entity 26
2.3.2.1 Application Programming Interface for XML-Based Information 26
2.3.2.1.1 Operating System Services 27
2.3.2.1.1.1 Distributed-Object Computing 27
2.3.2.1.1.2 Graphic Data Interchange 27
2.3.2.1.1.3 Multiple-Image Network Graphics 27
2.3.2.1.1.4 Virtual Reality Modeling Language 27
2.3.2.1.1.5 Still-Imagery Data Interchange 27
2.3.2.1.1.6 Motion-Imagery Data Interchange 27
2.3.2.1.1.7 Document Interchange 28
2.3.2.2 Data Management Services 28

SECTION 3 31

INFORMATION TRANSFER STANDARDS 31

3.1 INTRODUCTION 31
3.1.1 Purpose 31
3.1.2 Scope 31
3.1.3 Background 31
3.1.3.1 Communications Framework 31
3.1.3.2 Protocol Standards 32
3.1.3.3 Protocol Profiles 32
3.2 MANDATES 32
3.2.1 End System Standards 32
3.2.1.1 Host Standards 32
3.2.1.1.1 Application Support Services 33
3.2.1.1.1.1 Electronic Mail 33
3.2.1.1.1.2 Directory Services 33
3.2.1.1.1.3 File Transfer 34
3.2.1.1.1.4 Remote Terminal 34
3.2.1.1.1.5 Network and Systems Management 34
3.2.1.1.1.6 Network Time 34

3.2.1.1.1.7 Bootstrap Protocol (BOOTP) 34
3.2.1.1.1.8 Dynamic Host Configuration Protocol (DHCP) 35
3.2.1.1.1.9 World Wide Web (WWW) Services 35
3.2.1.1.2 Transport Services 35
3.2.1.1.2.1 Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) over Internet Protocol (IP) 35
3.2.1.1.2.2 Transmission Control Protocol (TCP) 35
3.2.1.1.2.3 User Datagram Protocol (UDP) 36
3.2.1.1.2.4 Internet Protocol (IP) 36
3.2.1.1.2.5 Open Systems Interconnection (OSI)/Internet Interworking Protocol 36
3.2.1.2 Video Teleconferencing (VTC) Standards 36
3.2.1.3 Facsimile Standards 38
3.2.1.3.1 Analog Facsimile Standard 38
3.2.1.3.2 Digital Facsimile Standard 38
3.2.1.4 Imagery Dissemination Communications Standards 38
3.2.2 Network Standards 38
3.2.2.1 Router Standards 38
3.2.2.1.1 Internet Protocol (IP) 39
3.2.2.1.2 IP Routing 39
3.2.2.1.2.1 Interior Routers 39
3.2.2.1.2.2 Exterior Routers 40
3.2.2.2 Subnetworks 40
3.2.2.2.1 Ethernet 40
3.2.2.2.2 Point to Point Standards 41
3.2.2.2.3 Combat Net Radio (CNR) Networking 41
3.2.2.2.4 Integrated Services Digital Network (ISDN) 42
3.2.2.2.5 Asynchronous Transfer Mode (ATM) 42
3.2.2.2.6 Wireless LAN 44
3.2.3 Transmission Media 44
3.2.3.1 Military Satellite Communications (MILSATCOM) 44
3.2.3.2 Radio Communications 44
3.2.3.3 Synchronous Optical Network (SONET) Transmission Facilities 45
3.2.4 Summary of Packet Standards 45
3.2.5 Network and Systems Management 45
3.2.5.1 Data Communications 47
3.2.5.2 Telecommunications 47
3.3 EMERGING STANDARDS 48
3.3.1 Emerging Host Standards 48
3.3.2 Emerging Network Standards 49

SECTION 4 52

INFORMATION-MODELING, METADATA, AND INFORMATION-EXCHANGE STANDARDS 53

4.1 INTRODUCTION 53
4.1.1 Purpose 53
4.1.2 Scope 53
4.1.3 Background 53
4.2 MANDATES 54
4.2.1 Activity Modeling 54
4.2.2 Data Modeling 55

4.2.3 Object Modeling 56
4.2.4 DoD Data Model Implementation 56
4.2.5 DoD Data Definitions 57
4.2.6 Information Exchange Standards 57
4.2.6.1 Information Exchange Standards Applicability 57
4.2.6.2 Tactical Information-Exchange Standards 58
4.2.6.2.1 Bit-Oriented Formatted Messages 58
4.2.6.2.2 Character-based Formatted Messages 58
4.2.6.2.3 Database to Database Exchange 59
4.2.7 Modeling and Simulation Information and Data Exchange Standards 59
4.2.8 XML-Based Information Exchange 59
4.2.8.1 XML Schema 59
4.3 EMERGING STANDARDS 60
4.3.1 Activity Modeling 60
4.3.2 Data Modeling 60
4.3.3 Object Modeling 60
4.3.3.1 Object Metadata Exchange 60
4.3.4 DoD Data Model Implementation 60
4.3.5 DoD Data Definitions 60
4.3.6 Information Exchange Standards 61
4.3.7 Modeling and Simulation Information and Data Exchange Standards 61
4.3.8 XML-based Information Exchange 61
4.3.8.1 XML Transformation 61
4.3.8.2 XML Parsing and Manipulating 61

SECTION 5 63

HUMAN-COMPUTER INTERFACES 63

5.1 INTRODUCTION 63
5.1.1 Purpose 63
5.1.2 Scope 63
5.1.3 Background 63
5.2 MANDATES 63
5.2.1 General 63
5.2.1.1 Character-based Interfaces 64
5.2.1.2 Graphical User Interfaces 64
5.2.1.3 Security 64
5.2.2 Style Guides 64
5.2.2.1 Commercial Style Guides 65
5.2.2.1.1 X Window Style Guides 65
5.2.2.1.2 Windows Style Guide 66
5.2.2.2 DoD HCI Style Guide 66
5.2.2.3 Domain-level Style Guides 66
5.2.2.4 System-level Style Guides 66
5.2.3 Symbology 67
5.3 EMERGING STANDARDS 67

SECTION 6 69

INFORMATION SECURITY 69

6.1 INTRODUCTION 69

6.1.1 Purpose 69
6.1.2 Scope 69
6.1.3 Background 69
6.2 INFORMATION PROCESSING SECURITY STANDARDS 70
6.2.1 Mandated Standards 70
6.2.1.1 Application Software Entity 71
6.2.1.2 Application Platform Entity 71
6.2.2 Emerging Standards 71
6.2.2.1 Application Platform Entity 71
6.2.2.1.1 Security Alarm Reporting 71
6.2.2.2 Authentication Security Standards 71
6.2.2.3 Generic Security Service Application Program Interface (GSS API) 72
6.2.2.4 Security Management Protocols 72
6.3 INFORMATION TRANSFER SECURITY STANDARDS 72
6.3.1 MANDATES 72
6.3.1.1 Security Protocols 73
6.3.1.2 DMS Interface 73
6.3.1.3 Cryptographic Algorithms 74
6.3.1.4 Secure World Wide Web (WWW) Transactions 74
6.3.2 Emerging Standards 74
6.3.2.1 Security Association Management 74
6.3.2.2 Secure World Wide Web (WWW) Transactions 75
6.3.2.3 Networking Security Standards 75
6.3.2.4 Security Protocols 78
6.3.2.5 Other 78
6.3.2.6 Medium-Assurance Public-Key Infrastructure Security Standards 78
6.3.2.6.1 Background 78
6.3.2.6.2 Directory and Certificate Profile Standards 79
6.3.2.6.3 Operational Protocols and Exchange Formats 79
6.3.2.6.4 Management Protocols 80
6.3.2.6.5 Application Program Interfaces (APIs) 80
6.3.2.6.6 Cryptography 80
6.3.3 Summary of Standards 80
6.4 Information-Modeling, Metadata, and Information-Exchange SECURITY STANDARDS 81
6.4.1 Mandated Standards 81
6.4.2 Emerging Standards 81
6.5 HUMAN-COMPUTER INTERFACE SECURITY STANDARDS 81
6.5.1 Mandated Standards 81
6.5.1.1 Security Banners and Screen Labels 81
6.5.2 Emerging Standards 83
6.5.2.1 Entity Authentication 83
6.5.2.2 Personal Authentication 83

APPENDIX A - ACRONYMS 85

APPENDIX B - LIST OF REFERENCES 95

B.1 MILITARY 95
B.1.1 DoD References 95
B.1.2 Army References 101
B.1.3 Other Government Agency References 102
B.2 COMMERCIAL REFERENCES 104

B.3 Candidates For Removal From The JTA-Army 129

APPENDIX C - GLOSSARY 131

APPENDIX D – COMBAT SUPPORT AND SUSTAINMENT DOMAIN 139

D.1 DOMAIN OVERVIEW 139
D.1.1 Purpose 139
D.1.2 Background 139
D.1.3 Domain Description 139
D.1.4 Scope and Applicability 139
D.1.5 Technical Reference Model 139
D.1.6 Appendix Organization 139
D.2 DOMAIN SPECIFIC STANDARDS 140
D.2.1 Introduction 140
D.2.2 Information Processing Standards 140
D.2.2.1 Mandates 140
D.2.2.1.1 Document Interchange 140
D.2.2.1.2 Graphics Data Interchange 140
D.2.2.1.3 Product Data Interchange 141
D.2.2.1.4 Electronic Data Interchange 141
D.2.2.1.5 Geospatial Data Interchange 142
D.2.2.1.6 Configuration Management Data Interchange 142
D.2.2.1.7 Data Interchange Services for Automatic Test Systems (ATS) 143
D.2.2.1.7.1 Instrument Driver API Standards 143
D.2.2.1.7.2 Digital Test Data Formats 143
D.2.2.2 Emerging Standards 143
D.2.2.2.1 Product Data Interchange 143
D.2.3 Information Transfer Standards 144
D.2.3.1 Mandates 144
D.2.3.1.1 Instrument Communication Manager Standards for ATS 144
D.2.3.2 Emerging Standards 145
D.2.4 Information-Modeling, Metadata, and Information-Exchange Standards. 145
D.2.5 Human-Computer Interface Standards 145
D.2.6 Information Systems Security Standards 145
D.3 DOMAIN SPECIFIC SERVICE AREAS 146
D.3.1 Introduction 146
D.3.1.1 Mandated Standards 146
D.3.1.1.1 Smart Card Technology Standards for Electronic Business/Electronic Commerce146
D.3.1.1.2 System Framework Standards for ATS 146
D.3.1.2 Emerging Standards 147

APPENDIX E - COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C3I) DOMAIN 149

E.1 DOMAIN OVERVIEW 149
E.1.1 Purpose 149
E.1.2 Background 149
E.1.3 Domain Description 149
E.1.4 Scope and Applicability 149
E.1.5 Technical Reference Model 149
E.1.6 Appendix Structure 149
E.2 DOMAIN SPECIFIC STANDARDS 149

E.2.1 Introduction 149
E.2.2 Information Processing Standards 149
E.2.2.1 Mandates 150
E.2.2.1.1 Still-Imagery Data Interchange 150
E.2.2.2 Emerging Standards 150
E.2.3 Information Transfer Standards 150
E.2.3.1 Mandates 150
E.2.3.1.1 End System Standards 150
E.2.3.1.1.1 Secondary Imagery Dissemination Standards 150
E.2.3.1.2 Network Standards 150
E.2.3.1.3 Transmission Media 150
E.2.3.1.3.1 Military Satellite Communications (MILSATCOM) 150
E.2.3.1.3.1.1 Ultra High Frequency (UHF) Satellite Terminal Standards 151
E.2.3.1.3.1.1.1 5-kilo-Hertz (kHz) and 25-kHz Service 151
E.2.3.1.3.1.1.2 5-kHz Demand Assigned Multiple Access (DAMA) Service 151
E.2.3.1.3.1.1.3 25-kHz Time Division Multiple Access (TDMA)/Demand Assigned Multiple Access (DAMA) Service 151
E.2.3.1.3.1.1.4 Data Control Waveform 151
E.2.3.1.3.1.1.5 Demand Assigned Multiple Access (DAMA) Control System 151
E.2.3.1.3.1.2 Super High Frequency (SHF) Satellite Terminal Standards 151
E.2.3.1.3.1.2.1 Earth Terminals 151
E.2.3.1.3.1.2.2 Phase Shift Keying (PSK) Modems 152
E.2.3.1.3.1.3 Extremely High Frequency (EHF) Satellite Payload and Terminal Standards 152
E.2.3.1.3.1.3.1 Low Data Rate (LDR) 152
E.2.3.1.3.1.3.2 Medium Data Rate (MDR) 152
E.2.3.1.3.2 Radio Communications 152
E.2.3.1.3.2.1 High Frequency (HF) 152
E.2.3.1.3.2.1.1 HF and Automatic Link Establishment (ALE) 152
E.2.3.1.3.2.1.2 Anti-Jamming Capability 152
E.2.3.1.3.2.1.3 Data Modems 152
E.2.3.1.3.2.2 Ultra High Frequency (UHF) 153
E.2.3.1.3.2.3 Anti-Jamming Capability 153
E.2.3.1.3.2.4 Link 16 Transmission Standards 153
E.2.3.2 Emerging Standards 153
E.2.4 Information-Modeling, Metadata, and Information-Exchange Standards 153
E.2.4.1 Tactical Information Exchange Standards (Bit Oriented Formatted Messages) 153
E.2.4.1.1 Sensor Link Protocol (SLP) Message Set 153
E.2.5 Human-Computer Interfaces 153
E.2.5.1 Mandates 153
E.2.5.2 Emerging Standards 154
E.2.6 Information Security 154
E.3 DOMAIN SPECIFIC SERVICE AREAS 154
E.3.1 Introduction 154
E.3.1.1 Mandated Standards 154
E.3.1.2 Emerging Standards 154
E.3.1.2.1 Internal Communications 154
E.3.1.2.1.1 Fibre Channel 154
E.3.1.2.1.2 FireWire 155

APPENDIX F - WEAPON SYSTEMS DOMAIN (WSD) 155

F.1 INTRODUCTION 157
F.1.1 Purpose 158
F.1.2 Scope 158
F.1.3 Background 159
F.1.4 Technical Reference Model (TRM) 159
F.1.5 Appendix Structure 160
F.2 DOMAIN SPECIFIC STANDARDS 160
F.2.1 Introduction 160
F.2.2 Information Processing Standards 161
F.2.2.1 Mandates 161
F.2.2.1.1 Operating System Services 161
F.2.2.1.2 Mapping Services 161
F.2.2.2 Emerging Standards 161
F.2.2.2.1 Operating System Services 161
F.2.2.2.2 Mapping Services 161
F.2.3 Information Transfer Standards 162
F.2.3.1 Mandates 162
F.2.3.1.1 Map Data Loading 162
F.2.3.2 Emerging Standards 162
F.2.4 Information-Modeling, Metadata, and Information-Exchange Standards 162
F.2.4.1 Mandates 163
F.2.4.2 Emerging Standards 163
F.2.5 Human-Computer Interface Standards 164
F.2.5.1 Mandates 164
F.2.5.1.1 Domain-level Style Guide 164
F.2.5.1.2 Emerging Standards 164
F.2.5.2 Symbology 164
F.2.6 Information Systems Security Standards 165
F.3 DOMAIN SPECIFIC SERVICES AND INTERFACES 165
F.3.1 Introduction 165
F.3.2 Application Software Layer Interfaces 165
F.3.3 System Services Layer Interfaces 165
F.3.3.1 Mandates 165
F.3.3.1.1 Operating Environment Services 165
F.3.3.2 Emerging 166
F.3.3.2.1 Operating Environment Services 166
F.3.4 Resource Access Services Layer Interfaces 166
F.3.5 Physical Resources Layer Interfaces 166
F.3.5.1 Mandates 166
F. 3.5.1.1 Parallel Buses 166
F.3.5.1.1.1 Single Board Computers (SBCs) and Expansion Cards 166
F.3.5.2 Emerging Standards 167
F.3.5.2.1 Parallel Buses 167
F.3.5.2.1.1 Single Board Computers (SBCs) and Expansion Cards 167
F.3.6 Combat Identification (CI) Services 167
F.3.6.1 Mandates 167
F.3.6.2 Emerging Standards 167

APPENDIX F.AVS - AVIATION SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN 169

F.AVS.1 INTRODUCTION 169
F.AVS.1.1 Purpose 170
F.AVS.1.2 Scope 170
F.AVS.1.3 Background 170
F.AVS.1.4 Technical Reference Model (TRM) 170
F.AVS.1.5 Appendix Structure 170
F.AVS.2 SUBDOMAIN SPECIFIC STANDARDS 170
F.AVS.2.1 Introduction 170
F.AVS.2.2 Information Processing Standards 170
F.AVS.2.2.1 Mandates 171
F.AVS.2.2.1.1 Still Imagery Data Interchange 171
F.AVS.2.3 Information Transfer Standards 171
F.AVS.2.4 Information-Modeling, Metadata, and Information-Exchange Standards 171
F.AVS.2.5 Human-Computer Interface Standards 171
F.AVS.2.5.1 Mandates 171
F.AVS.2.5.1.1 Symbology 171
F.AVS.2.5.1.2 Aviation Systems Subdomain Style Guide 171
F.AVS.2.5.2 Emerging Standards 172
F.AVS.2.5.2.1 Aviation Systems Subdomain Style Guide 172
F.AVS.2.6 Information Systems Security Standards 172
F.AVS.3 SUBDOMAIN SPECIFIC SERVICES AND INTERFACES 172
F.AVS.3.1 Introduction 172
F.AVS.3.2 Applications Layer Interfaces 172
F.AVS.3.3 System Services Layer Interfaces 172
F.AVS.3.4 Resource Access Services Layer Interfaces 172
F.AVS.3.5 Physical Resources Layer Interfaces 173
F.AVS.3.5.1 Mandates 173
F.AVS.3.5.1.1 Serial Buses 173
F.AVS.3.5.1.2 Parallel Buses 174
F.AVS.3.5.1.2.1 Backplane Buses 174
F.AVS.3.5.2 Emerging Standards 174
F.AVS.3.6 Global Air Traffic Management Standards 175
F.AVS.3.6.1 Mandated Standards 175
F.AVS.3.6.2 Emerging Standards 175

APPENDIX F.GVS - GROUND VEHICLE SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN 177

F.GVS.1 INTRODUCTION 177
F.GVS.1.1 Purpose 177
F.GVS.1.2 Scope 178
F.GVS.1.3 Background 178
F.GVS.1.4 Technical Reference Model (TRM) 178
F.GVS.1.5 Appendix Structure 178
F.GVS.2 SUBDOMAIN SPECIFIC STANDARDS 178
F.GVS.2.1 Introduction 178
F.GVS.2.2 Information Processing Standards 178
F.GVS.2.3 Information Transfer Standards 178
F.GVS.2.4 Information-Modeling, Metadata, and Information-Exchange Standards 178
F.GVS.2.4.1 Mandates 178
F.GVS.2.4.2 Emerging Standards 179

F.GVS.2.4.2.1 Tactical Information Exchange Standards (Bit Oriented Formatted Messages) 179
F.GVS.2.5 Human-Computer Interface Standards 179
F.GVS.2.5.1 Mandates 179
F.GVS.2.5.2 Emerging Standards 179
F.GVS.2.6 Information Systems Security Standards 179
F.GVS.3 SUBDOMAIN SPECIFIC SERVICES AND INTERFACES 179
F.GVS.3.1 Introduction 179
F.GVS.3.2 Applications Layer Interfaces 180
F.GVS.3.3 System Services Layer Interfaces 180
F.GVS.3.4 Resource Access Services Layer Interfaces 180
F.GVS.3.5 Physical Resources Layer Interfaces 180
F.GVS.3.5.1 Mandates 180
F.GVS.3.5.1.1 Serial Buses 180
F.GVS.3.5.1.2 Parallel Buses 181
F.GVS.3.5.1.2.1 Backplane Buses 181
F.GVS.3.5.1.2.2 Single Board Computer (SBC) Expansion Buses 181
F.GVS.3.5.1.2.3 Peripheral Bus 181
F.GVS.3.5.2 Emerging Standards 181
F.GVS.3.5.2.1 Serial Buses 181

APPENDIX F.MS - MISSILE SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN 183

F.MS.1 INTRODUCTION 183
F.MS.1.1 Purpose 184
F.MS.1.2 Scope 184
F.MS.1.3 Background 184
F.MS.1.4 Technical Reference Model (TRM) 184
F.MS.1.5 Appendix Structure 184
F.MS.2 SUBDOMAIN SPECIFIC STANDARDS 184
F.MS.2.1 Introduction 184
F.MS.2.2 Information Processing Standards 184
F.MS.2.2.1 Mandates 184
F.MS.2.2.2 Emerging Standards 184
F.MS.2.2.2.1 Geospatial Data Interchange 184
F.MS.2.3 Information Transfer Standards 185
F.MS.2.3.1 Mandates 185
F.MS.2.3.2 Emerging Standards 185
F.MS.2.3.2.1 Joint Range Extension (JRE) Application Protocol (JREAP) 185
F.MS.2.4 Information-Modeling, Metadata, and Information-Exchange Standards 185
F.MS.2.5 Human-Computer Interface Standards 185
F.MS.2.5.1 Mandates 185
F.MS.2.5.1.1 Symbology 185
F.MS.2.5.2 Emerging Standards 185
F.MS.2.6 Information Systems Security Standards 185
F.MS.3 SUBDOMAIN SPECIFIC SERVICES AND INTERFACES 186
F.MS.3.1 Introduction 186
F.MS.3.2 Application Layer Interfaces 186
F.MS.3.3 System Services Layer Interfaces 186
F.MS.3.4 Resource Access Services Layer Interfaces 186

F.MS.3.5 Physical Resources Layer Interfaces 186
F.MS.3.5.1 Mandates 187
F.MS.3.5.1.1 Parallel Buses 187
F.MS.3.5.1.1.1 Single Board Computer (SBC) Expansion Buses 187
F.MS.3.5.2 Emerging Standards 187

APPENDIX F.MUS - MUNITION SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN 189

F.MUS.1 INTRODUCTION 189
F.MUS.1.1 Purpose 190
F.MUS.1.2 Scope 190
F.MUS.1.3 Background 190
F.MUS.1.4 Technical Reference Model (TRM) 190
F.MUS.1.5 Appendix Structure 190
F.MUS.2 SUBDOMAIN SPECIFIC STANDARDS 190
F.MUS.2.1 Introduction 190
F.MUS.2.2 Information Processing Standards 190
F.MUS.2.2.1 Emerging Standards 191
F.MUS.2.3 Information Transfer Standards 191
F.MUS.2.4 Information-Modeling, Metadata, and Information-Exchange Standards 191
F.MUS.2.4.1 Mandates 191
F.MUS.2.4.2 Emerging Standards 191
F.MUS.2.4.2.1 Tactical Information Exchange Standards (Bit Oriented Formatted Messages) 191
F.MUS.2.5 Human-Computer Interface Standards 191
F.MUS.2.6 Information Systems Security Standards 191
F.MUS.3 SUBDOMAIN SPECIFIC SERVICES AND INTERFACES 192
F.MUS.3.1 Introduction 192
F.MUS.3.2 Application Software Layer Interfaces 192
F.MUS.3.3 System Services Layer Interfaces 192
F.MUS.3.4 Resource Access Services Layer Interfaces 192
F.MUS.3.5 Physical Resources Layer Interfaces 192
F.MUS.3.5.1 Mandates 193
F.MUS.3.5.1.1 Parallel Buses 193
F.MUS.3.5.1.1.1 Backplane Buses 193
F.MUS.3.5.1.1.2 Peripheral Buses 193
F.MUS.3.5.2 Emerging Standards 193
F.MUS.3.6 Safety-Critical Software Services 193
F.MUS. 3.6.1 Mandates 194
F.MUS. 3.6.2 Emerging Standards 194

APPENDIX F.SS - SOLDIER SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN 195

F.SS.1 INTRODUCTION 195
F.SS.1.1 Purpose 196
F.SS.1.2 Scope 196
F.SS.1.3 Background 196
F.SS.1.4 Technical Reference Model (TRM) 196
F.SS.1.5 Appendix Structure 196
F.SS.2 SUBDOMAIN SPECIFIC STANDARDS 196
F.SS.2.1 Introduction 196

F.SS.2.2 Information Processing Standards 196
F.SS.2.3 Information Transfer Standards 197
F.SS.2.4 Information-Modeling, Metadata, and Information-Exchange Standards 197
F.SS.2.4.1 Mandates 197
F.SS.2.4.2 Emerging Standards 197
F.SS.2.4.2.1 Tactical Information Exchange Standards (Bit Oriented Formatted Messages) 197
F.SS.2.4.2.1.1 Sensor Link Protocol (SLP) Message Set 197
F.SS.2.5 Human-Computer Interface Standards 197
F.SS.2.6 Information Systems Security Standards 197
F.SS.3 SUBDOMAIN SPECIFIC SERVICES AND INTERFACES 197
F.SS.3.1 Introduction 197
F.SS.3.2 Application Layer Interfaces 198
F.SS.3.3 System Services Layer Interfaces 198
F.SS.3.4 Resource Access Services Layer Interfaces 198
F.SS.3.5 Physical Resources Layer Interfaces 198
F.SS.3.5.1 Mandates 198
F.SS.3.5.1.1 Serial Buses 198
F.SS.3.5.2 Emerging Standards 199
F.SS.3.5.2.1 Serial Buses 199

APPENDIX G - MODELING & SIMULATION DOMAIN 201

G.1 DOMAIN OVERVIEW 201
G.1.1 Purpose 201
G.1.2 Background 201
G.1.3 Domain Description 202
G.1.4 Scope and Applicability 202
G.1.5 Technical Reference Model 203
G.1.6 Appendix Structure 203
G.2 DOMAIN SPECIFIC STANDARDS 203
G.2.1 Introduction 203
G.2.2 Information Processing Standards 203
G.2.2.1 Mandates 203
G.2.2.1.1 HLA Framework and Rules 203
G.2.2.1.2 HLA Interface Specification 203
G.2.2.1.3 HLA Object Model Template (OMT) 203
G.2.2.1.4 High Level Architecture (HLA) for Simulations 204
G.2.2.2 Emerging Standards 204
G.2.3 Information Transport Standards 204
G.2.4 Information-Modeling, Metadata, and Information-Exchange Standards 205
G.2.4.1 Mandates 205
G.2.4.1.1 Federation Execution Details Data Interchange Format (FED DIF) 205
G.2.4.1.2 Object Model Template Data Interchange Format 205
G.2.4.1.3 Standard Simulator Database Interchange format (SIF) 205
G.2.4.2 Emerging Standards 205
G.2.4.2.1 SEDRIS 205
G.2.4.2.2 Object Model Data Dictionary 205
G.2.5 Human-Computer Interfaces 206
G.2.6 Information Security 206
G.3 DOMAIN SPECIFIC SERVICE AREAS 206

APPENDIX H - JTA-ARMY VERSION CHANGE MATRIX 207

APPENDIX I - JTA-ARMY COMPARISON TO JTA MATRIX.....219

LIST OF FIGURES

Figure 1-1. The Different Architectures 2
Figure 1-2. JTA-Army Lineage 4
Figure 1-3. Army System Domains 7
Figure 2-1. DoD Technical Reference Model 12
Figure 3-1. Summary Of The Packet-Switched Transfer Standards 46
Figure 5-1. Hierarchy Of Style Guides 65
Figure F-1. Realm Of Weapon System Functional Time Regimes 157
Figure F-2. Notional JTA-Army Hierarchy 158
Figure F-3. DoD Technical Reference Model Services View And Interfaces View 160
Figure F-4. Development Process Relative To The Real-Time, Embedded Processing System 163
Figure F.AVS-1. Aviation Systems Functional Time Regimes 169
Figure F.GVS-1. Ground Vehicle Systems Functional Time Regimes 177
Figure F.MS-1. Missile Systems Functional Time Regimes 183
Figure F.MUS-1. Muntion Systems Functional Time Regimes 189
Figure F.SS-1. Soldier Systems Functional Time Regimes 195

LIST OF TABLES

Table 2-1 - Document Interchange Formats 17
Table 2-2 - Motion Imagery Standards Profile 20
Table 2-3 - Emerging Standards For Motion Imagery Standards Profile 28
Table 3-1 - VTC Standards For Data Rate 56-1920 Kbps 37
Table 6-1 - Notional Mapping Of Protocols And Security Standards 82

SECTION 1

TECHNICAL ARCHITECTURE OVERVIEW

1.1 INTRODUCTION

The Joint Technical Architecture - Army (JTA-Army) is the Army's implementation of the DoD JTA. As such, it 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 sustainment/combat support systems that produce, use, or exchange information electronically. The second objective is to mandate standards and guidelines for system development and acquisition that will dramatically reduce cost, development time, and fielding time for improved systems. The third objective is to communicate to industry the Army's intent to consider open system products and implementations.

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 each section covers.

1.1.2 Architectures Defined

"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. Figure 1-1 below, 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. The Department of the Army, Army Enterprise Architecture Guidance Document (AEAGD), published in 23 December 1998, identifies the architectural products for each of the three architectures: Operational, System and Technical.

1.1.2.1 Technical Architecture

The Technical Architecture (TA) view 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 view provides the technical systems-implementation guidelines upon which engineering specifications are based, common building blocks are built, and product lines are developed.

This view includes a collection of the technical standards, conventions, rules and criteria organized into profile(s) that govern system services, interfaces, and relationships for particular systems architecture views and that relate to particular operational views.

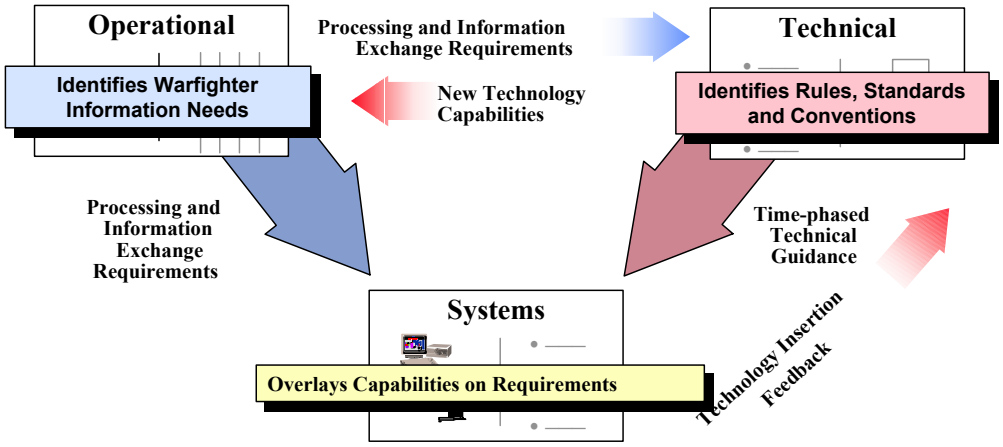


FIGURE 1-1. THE DIFFERENT ARCHITECTURES

1.1.2.2 Operational Architecture

The Operational Architecture (OA) view is a description of the tasks and activities, operational elements, and information flows required to accomplish or support a military operation.

The operational architecture view contains descriptions (often graphical) of the operational elements, assigned tasks and activities, and information flows required to support the warfighter. It defines the types of information exchanged, the frequency of the exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges in detail sufficient to ascertain specific interoperability requirements.

1.1.2.3 Systems Architecture

The Systems Architecture (SA) view is a description, including graphics, of the systems and interconnections providing for, or supporting, warfighting functions.

For a domain, the systems architecture view shows how multiple systems link and interoperate, and may describe the internal construction and operations of particular systems within the architecture. For the individual system, the systems architecture view includes the physical connection, location, and identification of key nodes (including materiel item nodes), circuits, networks, warfighting platforms, etc., and specifies system and component performance parameters (e.g., mean time between failure, maintainability, availability). The systems architecture view associates physical resources and their performance attributes to the operational view and its requirements following standards defined in the technical architecture.

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.

The mandated standards in the JTA-Army represents the minimum set of standards and guidelines for the acquisition of all systems that produce, use, or exchange information electronically. The applicable mandated standards in the JTA-Army are the starting set of standards for a system, and additional standards may be used to meet requirements if they are not in conflict with standards mandated in 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 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 Acquisition Executive (AAE) and the Vice Chief of Staff of the Army (VCSA) reaffirmed the Chief's “Mark on the Wall” in the 4 October 2001 memorandum, “Achieving Interoperability Among Army Systems.” All Army systems must comply with the JTA-Army by 30 September 2006.

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 Chief Information Officer/G-6 (CIO/G-6) 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 in Version 5.0.

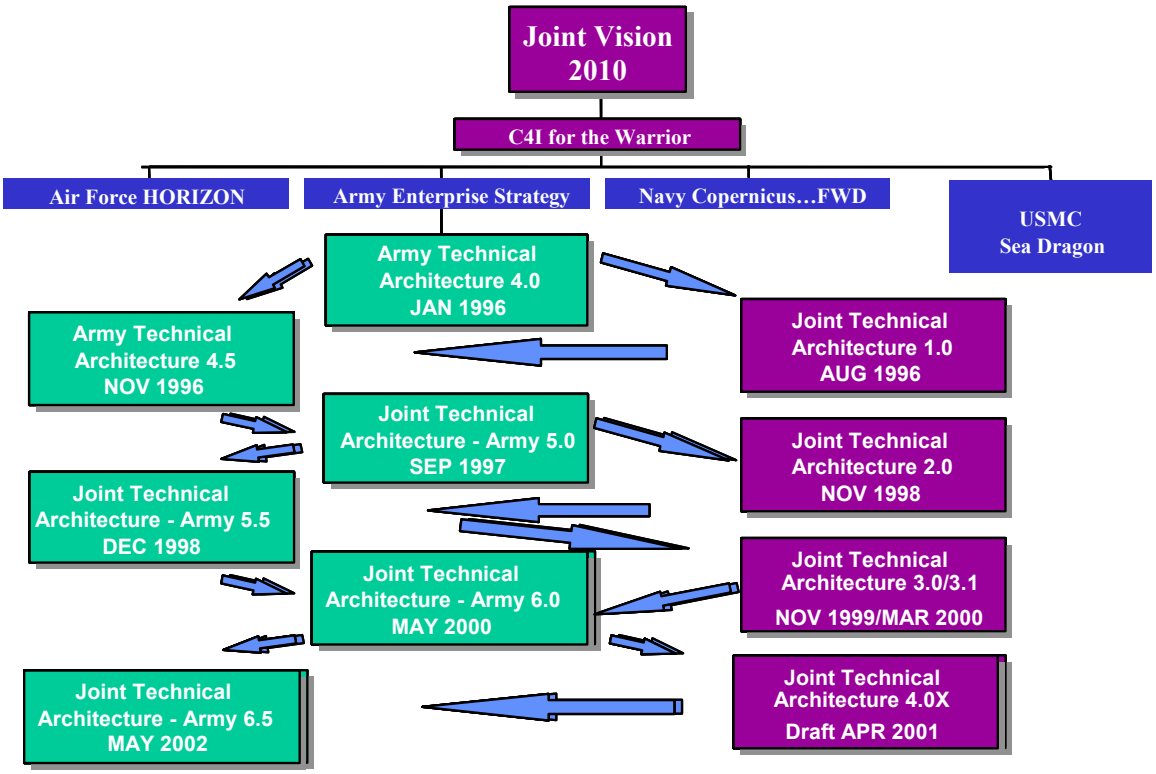


FIGURE 1-2. JTA-ARMY LINEAGE

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, "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 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 Army system "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 updated mandated and emerging standards, completed the alignment of Army Technical Architecture mandates with JTA Version 1.0, completed the minimal interoperability standards for all domains, and started to expand the scope to include open information electronic hardware standards. JTA-Army Version 5.5 updated the mandated and emerging standards, and included standards from JTA Version 2.0. JTA-Army Version 6.0 updated the mandated and emerging standards, and included standards from JTA Version 3.1. JTA-Army Version 6.5 updated the mandated and emerging standards, and included standards from Draft JTA Version 4.0. JTA-Army Version 6.5 remains the central source of Technical Architecture guidance for Army systems. Appendix H contains the list of changes in JTA-Army Version 6.5 with respect to Version 6.0. Appendix I contains the list of differences between JTA Version 3.1 and JTA-Army 6.5.

1.1.5 Basis for the JTA-Army Version 6.5

The JTA-Army Version 6.5 extends, updates and supercedes JTA-Army Version 6.0. The JTA Version 3.1 and Draft JTA Version 4.0 are the primary basis for the changes contained in this JTA-Army release. The JTA and JTA-Army are “forward-looking” documents. Their purpose is to guide the acquisition and development of new and emerging functionality and provide a baseline towards which existing systems will move. The JTA-Army is a compendium of interface and service standards that can be used now and in the future.

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 followed by allied standards such as NATO Standardization Agreements (STANAG), and finally government standards such as Federal Information Processing Standards 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 on developing and testing computer software. Even when software development is completed on schedule, few systems operate in isolation, so additional resources are spent 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 whose goal is to standardize the external environment interfaces and the Application Program Interface (API) for mission application system developers. The COE concept assists in maintaining interoperability over time because the common software infrastructure is upgraded as a whole. It also frees the mission application developer to concentrate efforts on enhancing operational functionality rather than building common infrastructure services.

DoD has adopted the Defense Information Infrastructure (DII) COE, which was based on the Global Command and Control System (GCCS) COE. The DII COE provides the Army's foundation for standardized common services. It is an approach for building interoperable systems, based on a collection of reusable software components that defines a reusable, common software infrastructure. The JTA-Army emphasizes the adoption of the COE concept, the COE software architecture, the reuse of COE components, and designing Army system application software to the COE set of APIs.

Software reuse in Army and DoD systems has 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 the major Army system domains are shown in Figure 1-3.

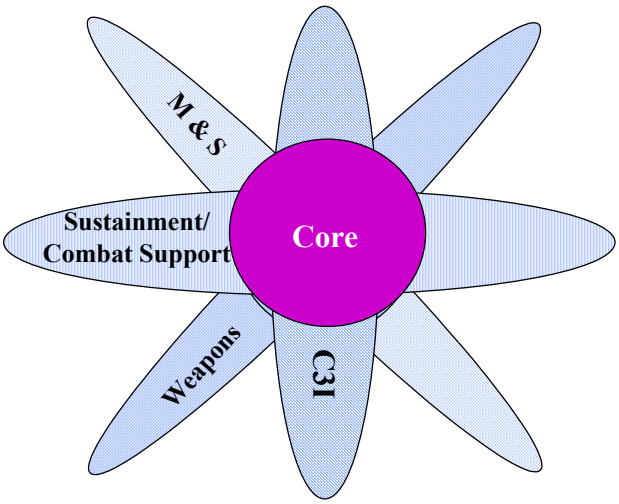


FIGURE 1- 3. ARMY SYSTEM DOMAINS

1.2.2 Document Organization

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

Appendix A contains acronyms used in the document. Appendix B is the list of references. Standards that are candidates for being removed from the JTA-Army in the next version are listed in Appendix B, Table B-5. Appendix C is a glossary of terms with definitions.

In addition, there is an appendix for each domain containing domain specific mandatory and emerging standards. For a given interface or service, the core standards are preferred for inter-domain interoperability, however, the choice to use the core, the domain, or both standards should be the result of analyzing the system requirements (operational architecture) and applying the best solutions (systems architecture). A lead agency for each domain, shown in parentheses below, has been designated to further develop each domain appendix.

1. Appendix D – Combat Support and Sustainment Domain. (PEO-Standard Army Management Information System (STAMIS)).

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

3. Appendix F – Weapon Systems Domain. (Weapon Systems Technical Architecture Working Group (WSTAWG)). The Weapons Systems Domain has several subdomains, which are as follows:

Appendix F.AVS - Aviation Systems Subdomain for the Weapon Systems Domain,

Appendix F.GVS - Ground Vehicle Systems Subdomain for the Weapon Systems Domain,

Appendix F.MS – Missile Systems Subdomain for the Weapon Systems Domain,

Appendix F.MUS - Munition Systems Subdomain for the Weapon Systems Domain, and

Appendix F.SS – Soldier Systems Subdomain for the Weapon Systems Domain.

4. Appendix G - Modeling & Simulation Domain. (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 purposes only. It defines the purpose and scope of the section and provides background descriptions and definitions that are unique to the section.
2. *Mandates* - This subsection identifies mandatory standards or practices. Each mandated standard or practice is clearly identified on a separate bulletized line and includes a formal reference citation.

   A standard is mandatory in the sense that if a service is going to be implemented, it will 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 or program 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. All mandatory standards in the JTA-Army are of the types that have been identified by the DoD Standards Reform as waiver-free or for which an exemption has already been obtained.
3. *Emerging Standards* - This subsection provides an information-only description of standards that are candidates for possible addition to the JTA-Army mandates. The purpose of listing these candidates is to help the program manager determine those areas that are likely to change in the near term (within three years) and suggest those areas in which "upgradability" should be a concern.

   The expectation is that emerging standards will be elevated to mandatory status when 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.

Appendix H is a list of changes for this version of the JTA-Army referenced to the earlier version of the JTA-Army. Appendix I is a comparison of the JTA-Army with the previous version of the JTA.

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.

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).

1.2.2.3 Information-Modeling, Metadata, and Information-Exchange Standards

Section 4 describes the use of integrated information modeling and mandates applicable standards. Information modeling consists of activity, data, and dynamic modeling. Section 4 of the JTA-Army currently addresses only activity and data modeling. This section explains the

use of the DoD Command and Control (C2) Core Data Model (C2CDM) and the Defense Data Dictionary System (DDDS), formerly the Defense Data Repository System (DDRS). Section 4 also mandates information standards including message formats.

1.2.2.4 Human-Computer Interfaces

Section 5 provides a common framework for Human-Computer Interface (HCI) design and implementation in Army 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.

1.2.2.5 Information Security

Section 6 prescribes the standards and protocols to be used to satisfy security requirements. This section provides the mandated and emerging security standards that apply to JTA-Army Sections 2 through 5. Section 6 is structured to mirror the overall organization of the JTA-Army so that readers can easily link security topics with the related JTA-Army subject areas.

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 standards in this section are drawn from widely accepted commercial standards that meet DoD requirements. Where necessary for interoperability, profiles of commercial standards are used. Military standards are mandated only when suitable commercial standards are not available.

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 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 DoD Technical Reference Model (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 DoD TRM organizes software into two entities, an Application Software Entity and an Application Platform Entity. The Application Software Entity communicates with the Application Platform Entity through an API. The Application Platform Entity communicates with the external environment through the External Environment Interface (EEI). The DoD 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 major service areas and associated mandates are detailed in Section 2.2.2.1 .

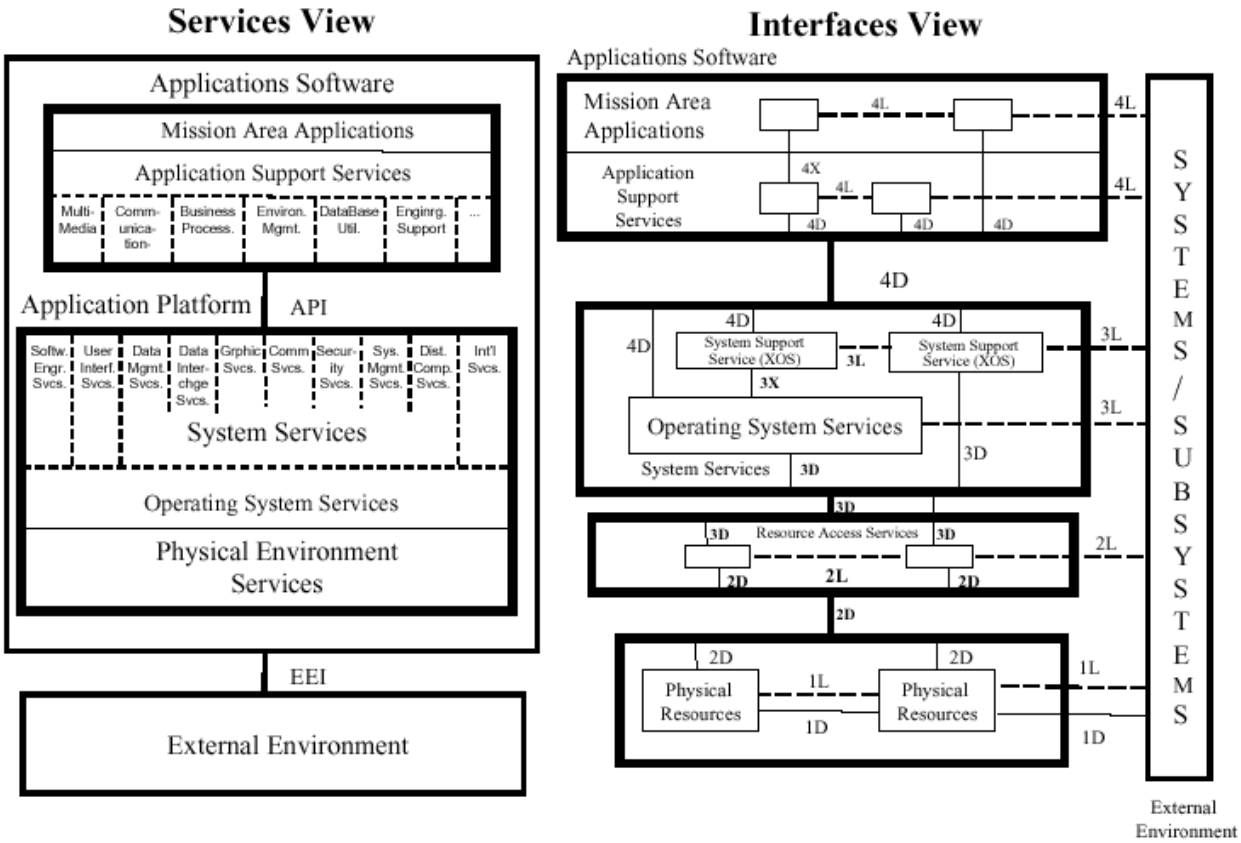


FIGURE 2-1. DOD TRM

2.1.3.1 DoD Technical Reference Model

The DoD TRM and the core set of standards mandated in the JTA define the target technical environment for the acquisition, development, and support of DoD information technology. The purpose of the DoD TRM is to provide a common conceptual framework, and define a common vocabulary so that the diverse components within the DoD can better coordinate acquisition, development, and support of DoD information technology. Interoperability is dependent on the establishment of a common set of services and interfaces that system developers can use to resolve technical architectures and related issues. The DoD TRM structure is intended to reflect the separation of data from applications, and applications from the computing platform – a key principle in achieving open systems. The model is to be used as a guideline for system planning, interoperability, and selecting appropriate standards. The DoD TRM is intended to ensure the use of consistent definitions between the services, domains, interfaces and other elements needed to define architectural and design components. The model identifies service areas (i.e., sets of capabilities grouped by functions) and their interfaces. The model's separation of the application platform from the application and external environment supports the development of open systems. Portability (i.e., open systems) enables utilization of open standards whereby a conforming application can be used on different and independent platforms.

The model is partitioned into the following: Application Software Entity that includes both mission area and support applications; Application Platform Entity that contains the system support services and operating system services; External Environment; and a number of

interfaces. The interfaces provide support for a wide range of applications and configurations, and consist of the following: Application Program Interfaces (APIs), and External Environment Interfaces (EEIs).

2.2 MANDATES

The Common Operating Environment (COE) concept is described in the Integration and Runtime Specification (I&RTS). The Defense Information Infrastructure COE (DII COE) is implemented with a set of modular software that provides 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 be adapted and tailored to meet the specific requirements of a domain. COE Implementations provide standard, modular software services that are consistent with the service areas identified in the DoD Technical Reference Model. Application programmers then have access to these software services through standardized APIs.

The DII COE, as defined in the DII COE I&RTS, is fundamental to a Joint System Architecture (JSA). In the absence of a JSA, the JTA mandates that at a minimum, all Command and Control (C2), Combat Support, and Intelligence Systems supporting the Joint Task Forces (JTFs) and Combatant Commands will use the DII COE where applicable. All applications of a system, which must be integrated into the DII COE, will be at least DII COE I&RTS level 5 compliant (software is segmented, uses DII COE Kernel, and is installed via COE tools) with a goal of achieving level 8. The following standard is mandated:

- Defense Information Infrastructure Common Operating Environment, Integration and Runtime Specification (I&RTS), Version 4.1, 3 October 2000.

If a required service is not available in the DII COE, software developed will adhere to the individual processing standards in this section and the applicable domain appendix.

2.2.1 Application Software Entity

The Application Software Entity is one part of the DoD Technical Reference Model (TRM) and includes both mission-area applications and support applications. Mission-area applications implement specific users' requirements and needs (e.g., personnel, material and management), and may include COTS, GOTS, custom-developed software, or a combination of these. Support applications are those that can be standardized across individual or multiple mission areas (e.g., e-mail and word processing). The services they provide can be used to develop mission-area-specific applications or made available to the user. The DoD TRM defines six support application categories: Multimedia, Communications, Business Processing, Environment Management, Database Utilities, and Engineering Support. The Application Software Entity includes all Army application software.

All system developers will identify their mission applications and their associated common support functional requirements. Mission area applications will make use of the DII COE Infrastructure Services and DII COE Common Support Applications, in accordance with the DII COE I&RTS, to the maximum extent practical based on system requirements. DII COE API documentation is included with the release of each of the DII COE Components, and can be obtained from the Army DII COE Software Repository, <http://acmb-arch-odisc4.army.mil/>.

2.2.1.1 Biometric Technology Services

The BioAPI Specification defines an open system standard application program interface (API) that allows software applications to communicate with a broad range of biometric technologies. The BioAPI is intended to provide a high-level generic biometric authentication model; one suited for any form of biometric technology. It covers the basic functions of Enrollment, Verification, and Identification, and includes a database interface to allow a biometric service provider (BSP) to manage the Identification population. A reference implementation (framework software) of the BioAPI Specification is also available as open source software. Biometric technologies are intended to overlay or replace password systems so that positive access control can be achieved. Additional information about the BioAPI Consortium, the BioAPI Specification, and the BioAPI Reference Implementation can be found at http://www.bioapi.org. The following standard is mandated:

- BioAPI Specification, Version 1.1, March 16, 2001.

2.2.2 Application Platform Entity

The Application Platform Entity is the second layer of the DoD TRM and it includes the common system services upon which required information-processing functionality is built. The Application Platform Entity is composed of 11 service areas. The corresponding mandates are provided in the following subsections.

2.2.2.1 Service Areas

Eleven primary system services and operating systems services are defined within the Application Platform Entity: Software Engineering, User Interfaces, Data Management, Data Interchange, Graphics, Communications, Operating System, Internationalization, Security, System Management, and Distributed Computing 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 will 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. Programming language selections should be made in the context of the system and software engineering factors that influence overall life-cycle costs, risks, and potential for interoperability. The following standards are mandated when using Ada, C or C++:

- ISO/International Electrotechnical Commission (IEC) 8652:1995 (Ada 95), Ada Reference Manual, Language and Standard Libraries.
- ISO/IEC 9899:1999, Information Technology -Programming Language C.

- ANSI/ISO/IEC 14882-1998, Information Technology - Programming Languages - C++.

2.2.2.1.1.2 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 CASE tools will follow.

2.2.2.1.2 User Interface Services

User Interface Services implement the Human-Computer Interface (HCI) style and control how users interact with the system by providing consistent access to application programs, operating system functions and system utilities. For UNIX-based systems, the Common Desktop Environment (CDE)/Motif provides a common set of desktop applications and management capabilities. CDE/Motif uses the underlying X-Windows system. The following standards and documentation sets are mandated for UNIX-based systems:

- T251: CDE 2.1 and MOTIF 2.1 Documentation - Full Set, Open Group Publication Set, October 1997.
- C320, Motif Toolkit API, Open Group Technical Standard, ISBN 1-85912-024-5, April 1995.
- C323, XCDE Services and Applications, Open Group Technical Standard, ISBN 1-85912-074-1, April 1995.
- C324, XCDE Definitions and Infrastructure, Open Group Technical Standard, ISBN 1-85912-070-9, April 1995.
- C510, Window Management (X11R5): File Formats and Application Conventions, Open Group Technical Standard, ISBN 1-85912-090-3, May 1995.
- C903, X Window System (X11R6): Protocol, Open Group Technical Standard, July 1999.
- C904, X Window System (X11R6): C-Language Library (Xlib), Open Group Technical Standard, December 1999.
- C905, X Window System (X11R6): Toolkit, Open Group Technical Standard, December 1999.

For Microsoft Windows-based systems, the Win32 API set provides user interface services. Documentation for the Win32 APIs is found within the Microsoft Platform SDK. The following standard is mandated for use with Microsoft Windows-based systems:

- Win32 APIs, as specified in the Microsoft Platform SDK, which can be found on the Microsoft Developer Network.

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 will 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).

The ISO/IEC 9075-3 mandate does not preclude the use of Open Database Connectivity (ODBC) 3.0 or JDBC extensions in situations where the capabilities supported by ISO/IEC 9075-3 cannot satisfy user-functional requirements. Note that ISO/IEC 9075-3 is a subset of ODBC 3.0

2.2.2.1.4 Data Interchange Services

The data interchange services provide specialized support for the exchange of data between applications and to and from the external environment. These services include document, graphics data, geospatial data, still-imagery data, product data, audio data, motion-imagery data, storage media, atmospheric and oceanographic data, file compression and electronic commerce data.

Message interchange standards are covered in Section 4.

2.2.2.1.4.1 Document Interchange

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-independent and application-independent language for managing document structures. SGML is a meta-language, providing the rules for designing and applying a system of markup tags rather than the specific set of tags. The following standard is mandated:

- ISO 8879: 1986, Information processing -- Text and office systems --Standard Generalized Markup Language (SGML).

The Hypertext Markup Language (HTML) is used for hypertext formatted and navigational linked documents. For hypertext documents intended to be interchanged via the World Wide Web (WWW) or made available via organizational intra-nets, the following standard is mandated:

- HTML 4.01 Specification, W3C Recommendation, revised on 24-Dec-1999, REC-html401-19991224 <http://www.w3.org/TR/1999/REC-html401-19991224>.

The eXtensible Markup Language (XML), based on SGML, is used for describing the structure of documents. Refer to section 4.2.8 for further information.

Table 2-1 identifies file formats for the interchange of common document types such as text documents, presentation graphics, spreadsheets, and databases. Individual vendors control some of these formats, but multiple companies' products can translate all of these formats. In support of the standards mandated in this section, Table 2-1 identifies 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 will be capable of generating at least one of the formats listed in Table 2-1 for the appropriate document type.
- All organizations will 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 format	.txt	ISO/IEC 646:1991 International Reference Version (IRV).
Compound Document	Adobe® Acrobat 4.0 format HTML 4.01 format MS® Word 6.0 format MS® Word 7.0 format Rich Text Format WordPerfect® 5.2 format	.pdf .htm .doc .doc .rtf .wp5	Adobe PDF 1.3 W3C Vendor Vendor Vendor Vendor
Briefing - Graphic Presentation	Freelance Graphics 2.1 format MS® Powerpoint® 4.0 format	.pre .ppt	Vendor Vendor
Spreadsheet	Lotus® 1-2-3 Release 3.x format MS® Excel® 5.0 format	.wk3 .xls	Vendor Vendor
Database	Dbase 4.0 format	.dbf	Vendor
Compression	GZIP file format ZIP file format	.gz .zip	IETF RFC-1952 Vendor
Computer Automated Design	AutoCad 14 format	.dxf	Vendor
Phone Listing	vCard	.vcf	IETF RFC-2425, and RFC-2426

2.2.2.1.4.2 Graphics Data Interchange

These services are supported by device-independent descriptions of the picture elements for vector and raster graphics. The International Organization for Standardization (ISO) Joint Photographic Expert Group (JPEG) standard describes several alternative algorithms for the representation and compression of raster images, particularly for imagery; JPEG images may be transferred using the JPEG File Interchange Format (JFIF). Graphics Interchange Format (GIF) and JFIF are de facto standards for exchanging graphics and images over an internet. GIF supports lossless compressed images with up to 256 colors and short animation segments. Note that Unisys owns a related patent, which requires a license for software that reads or writes the GIF format. Portable Network Graphics (PNG) is an extensible file format for the lossless, portable, well-compressed storage of a raster image. Indexed-color, grayscale, and truecolor images are supported, plus an optional alpha channel for transparency.

For the interchange of very large still-raster images that have no geospatial context and where lossy Decompression is acceptable, the mandated standard is:

- JPEG File Interchange Format, Version 1.02, C-Cubed Microsystems, 1 September 1992.

For the interchange of other single raster images that have no geospatial context and where lossy compression is not acceptable, the mandated standard is:

- IETF RFC 2083, Portable Network Graphics (PNG) Specification, Version 1.0, January 1997.

For the lossless interchange of raster images that have no geospatial context and where none of the above cases apply, such as the exchange of still-images that can be viewed in sequence (also referred to as animation), the mandated standard is:

- Graphics Interchange Format (GIF), Version 89a, 31 July 1990, CompuServe Incorporated.

2.2.2.1.4.3 Geospatial Data Interchange

Geospatial services are also referred to as mapping, charting, and geodesy (MC&G) services. Raster Product Format (RPF) defines a common format for the interchange of raster-formatted digital geospatial data among DoD Components. Existing geospatial products, which implement RPF, include Compressed Arc Digitized Raster Graphics (CADRG), Controlled Image Base (CIB), and Digital Point Positioning Data Base (DPPDB). For raster-based products, the following standard is mandated:

- MIL-STD-2411, Raster Product Format, 6 October 1994; with Notice of Change, Notice 1, 17 January 1995.

Vector Product Format (VPF) defines a common format, structure, and organization for data objects in large geographic databases that are based on a georelational data model and intended for direct use. Existing geospatial products which implement VPF include Vector Map (VMap) Levels 0-2, Urban Vector Map (UVMap), Digital Nautical Chart (DNC), Vector Product Interim Terrain Data (VITD), Digital Topographic Data (DTOP), and World Vector Shoreline Plus (WVS+). For vector-based products, the following standard is mandated:

- MIL-STD-2407, Interface Standard for Vector Product Format (VPF), 28 June 1996.

WGS 84, a Conventional Terrestrial Reference System (CTRS), is mandated for representation of a reference frame, reference ellipsoid, fundamental constants, and an Earth Gravitational Model with related geoid. Included in the Reference System are parameters for transferring to/from other geodetic datums. WGS 84 will be used for all joint operations and is recommended for use in multinational and unilateral operations after coordination with allied commands (CJCS). The following standard is mandated:

- MIL-STD-2401, Department of Defense World Geodetic System (WGS 84), 11 January 1994.

FIPS PUB 10-4 provides a list of the basic geopolitical entities in the world, together with the principal administrative divisions that comprise each entity. For applications involving the interchange of geospatial information requiring the use of country codes, the following standard is mandated:

- FIPS PUB 10-4, Countries, Dependencies, Areas of Special Sovereignty, and Their Principal Administrative Divisions, April 1995.

Additional information on other Geospatial services not identified in the mandated standards is available in NIMAL 805-1A, NIMA GGI&S List of Products and Services, January 1997.

2.2.2.1.4.4 Still 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 and image related products. NITFS provides a package containing information about the image, the image itself, and optional overlay graphics. The Standard provides a ”package” containing an image(s), subimages, symbols, labels, and text as well as other information related

to the image(s). NITF supports the dissemination of secondary digital imagery from overhead collection platforms. Guidance on applying the suite of standards composing NITFS can be found in MIL-HDBK-1300A. The following standards are mandated for imagery product dissemination:

- MIL-STD-2500B, National Imagery Transmission Format (Version 2.1) for the National Imagery Transmission Format Standard, 22 August 1997 with Notice 1, 2 October 1998.
- MIL-STD-188-196, Bi-Level Image Compression for the National Imagery Transmission Format Standard, 18 June 1993.
- MIL-STD-188-199, Vector Quantization Decompression for the National Imagery Transmission Format Standard, 27 June 1994.
- ISO/IEC 8632:1992 Computer Graphics Metafile (CGM) for the Storage and Transfer of Picture Description Information, as profiled by MIL-STD-2301A, Computer Graphics Metafile (CGM) Implementation Standard for the National Imagery Transmission Format Standard, 5 June 1998.
- ISO/IEC 10918-1: 1994, Joint Photographic Experts Group (JPEG) as profiled by MIL-STD-188-198A, Joint Photographic Experts Group (JPEG) Image Compression for the National Imagery Transmission Format Standard, 15 December 1993.

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.

Communication protocols for transmission of imagery over point-to-point tactical data links in high Bit Error Rate (BER), disadvantaged communications environments are specified in Appendix E.2.3.1.1.1.

2.2.2.1.4.5 Product Data Interchange

Refer to Appendix D.2.2.1.3 for requirements on product data interchange standards.

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 for decoding in an environment with a target bit rate of about 56 to 64 kilobits per second (kbps) per audio channel, the following standards are mandated:

- ISO/IEC 11172-1: 1993 Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s - Part 1: Systems, 1993; with Technical Corrigendum 1:1995.
- ISO/IEC 11172-3: 1993, Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Megabits per second (Mbit/s) - Part 3 (Audio Layer-3 only); with Technical Corrigendum 1:1996.

2.2.2.1.4.7 Motion Imagery Data Interchange

Motion Imagery is defined as imaging sensors/systems that generate/process sequential or continuous streaming images at specified temporal rates (normally expressed as Frames Per

Second (FPS) or hertz (Hz)). Motion Imagery defines temporal domains of 1 Hz or higher, and still imagery defines temporal domains of less than 1 Hz.

2.2.2.1.4.7.1 Video Imagery

The Motion Imagery Standards Profile (MISP) 1.7 Chapter 2.0, Commercial Standards, Interoperability Profiles, and Recommended Practices profile the following standards in Table 2-2 for DoD/IC/USIGS Implementations, 1 March 2001, are mandated:

TABLE 2-2 - MOTION IMAGERY STANDARDS PROFILE (MISP)

Standard	Title	Usage
ITU-R BT.601-4	Encoding Parameters of Digital Television for Studios, 1994	Digital encoding of standard-definition television for studio distribution
ISO/IEC 13818-1:1996	Information technology - Generic coding of moving pictures and associated audio information - Part 1:Systems (MPEG-2); 1996, with Amendment 1:1997	MPEG-2 Systems for Standard and High-definition Compression
ISO/IEC 13818-2:1996	Information technology - Generic coding of moving pictures and associated audio information - Part 2: Video (MPEG-2); 1996, with Amendment 1:1997.	MPEG-2 Video for Standard and High-definition Compression.
ISO/IEC 13818-4:1996	Information technology - Generic coding of moving pictures and associated audio Information - Part 4: Conformance Testing; 1996	MPEG-2 Conformance for Standard and High-definition Compression
ANSI/SMPTE 12M-1999	Television, Audio, and Film - Time and Control Code	525-line Time Annotation and Embedded Time References
ANSI/SMPTE 309M-1999	Television - Transmission of Date and Time Zone Information in Binary Groups of Time and Control Code.	Transmission of Date and Time Zone Information
ANSI/SMPTE 259M-1997	Television - 10 bit 4:2:2 Component (Serial Digital Interface).	Serial Digital Interface Interconnection and Processing
ANSI/SMPTE 292M-1998	Television - Bit-Serial Digital Interface for High-Definition Television Systems	High-Definition Baseband Signal Transport and Processing
ITU-R BT. 1358	Studio Parameters of 625 and 525 line Progressive Scan Television Systems, February 1998 - Digital Representation.	Progressive Video Sampling Structure - Standard-definition
ANSI/SMPTE 296M-2001	Television - 1280 x 720 Progressive Image Sample Structure - Analog and Digital Representation and Analog Interface	720-line Video Sampling Structure - High-definition
ANSI/SMPTE 274M-1995	Television - 1920 x 1080 Scanning and Interface	1080-line Video Sampling Structure - High-definition
ANSI/SMPTE 297M-1997	Television - Serial Digital Fiber Transmission System for ANSI/SMPTE 259M Signals	Serial Digital Fiber for Uncompressed Baseband Signal Transport and Processing
ANSI/SMPTE 291M-1996	Television - Ancillary Data Packet and Space Formatting	Use of Ancillary Data Space Formatting Structure

The standards for the Video Imagery section do not completely define an architecture for interoperability for low bandwidth (below 1.5 Mbps) real-time streaming applications. Standards

for such low-bandwidth applications are actively under development. Until such standards are available, users may use 'MPEG-1' or 'MPEG-2 4:20 MP@ML Adaptive Field Frame' standards for low bandwidth video applications. DoD users who adopt proprietary video compression systems for very low bandwidth applications are cautioned that such systems are generally not supported within DoD and that the interoperability of such systems is not ensured. It is also anticipated that MPEG-4 may be used for very low data rate video dissemination applications (such as VSM 1 and VSM 2).

2.2.2.1.4.7.2 Audio for Video Imagery

For audio systems associated with Video Imagery applications, the audio sub-sections of the " DoD/IC/USIGS Motion Imagery Standards Profile (MISP), Version 1.7, 1 March 2001, apply. The following standards are mandated:

- ANSI S4.40-1992/AES3-1992, AES (Audio Engineering Society) Recommended Practice for Digital Audio Engineering - Serial transmission format for two-channel linearly represented digital audio data, 1992 (reaffirmed and amended 1997).
- ISO/IEC 13818-3:1995, Information technology - Generic coding of moving pictures and associated audio information, with Amendment 1:1996. Used for compressed digital audio systems, MPEG-2 Part 3: Audio.

2.2.2.1.4.7.3 Video Support

MPEG-1 is an open international standard for video compression that has been optimized for single- and double-speed CD-ROM data transfer rates. The standard defines a bit-stream representation for synchronized digital video and audio, compressed to fit into a bandwidth of 1.5 Mbps. This corresponds to the data retrieval speed from CD-ROM and Digital Audio Tape (DAT). With 30 FPS 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 that of a VHS recording. A major application of MPEG is the storage of audiovisual information on CD-ROM and DAT. MPEG is also gaining ground on the Internet as an interchange standard for video clips because the shell format is interoperable across platforms and considered to be platform-independent. The following standards are mandated:

- ISO/IEC 11172-1: 1993, Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s - Part 1: Systems, 1993; with Technical Corrigendum 1:1995.
- ISO/IEC 11172-2: 1993 Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s - Part 2 Video; 1993.

MPEG-2 Main Profile @ Main Level (MP@ML) 4:2:0 systems are fully backward compatible with the MPEG-1 standard. MPEG-2 MP@ML can be used with all video support systems (storage, broadcast, network) at bit rates from 3 to 10 Mbps, where limited additional processing is anticipated, operating in either progressive or interlaced scan mode, optimally handling the resolution of the ITU-R 601 recommendation (i.e., 720 x 480 pixels for the luminance signal and 360 x 480 pixels for the color space). The following video support standards for compressed video are mandated:

- ISO/IEC 13818-1: 1996, Information Technology - Generic Coding of Moving Pictures and Associated Audio Information - Part 1: Systems (MPEG-2); 1996, with Amendment 1:1997).
- ISO/IEC 13818-2: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 2: Video (MPEG-2); 1996, with Amendment 1:1997 and Amendment 2:1997. (The identical text is also published as ITU-T Rec. H.262).

2.2.2.1.4.7.4 Audio for Video Support

For audio files intended for decoding in an environment with a target bit rate of about 56 to 64 Kbps per audio channel, the following standard is mandated:

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

2.2.2.1.4.8 Data Interchange Storage Media

MIL-HDBK-9660B, 1 September 1997, provides additional guidance in the use of Compact Disc-Read Only Memory (CD-ROM) technology. In cases where CD-ROM/CD-RW media is used, the following file system format (at a minimum) is mandated:

- ISO 9660:1988, Information processing - Volume and file structure of CD-ROM for information interchange.

Additional standards used for the exchange of multimedia data can be found in Section 3.2.1.2.

2.2.2.1.4.9 Atmospheric and Oceanographic Data Interchange

The World Meteorological Organization (WMO) Commission established the following formats for Basic Systems (CBS) for atmospheric and oceanographic data. The WMO Format for the Storage of Weather Product Information and the Exchange of Weather Product Messages in Gridded Binary (GRIB) Form 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 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. The following standard is mandated:

- FM 92-X Ext. GRIB WMO No. 306, Manual on Codes, International Codes, Volume I.2 (Annex II to WMO Technical Regulations) Parts B and C.

The WMO Binary Universal Format for Representation (BUFR) is used for interchange of atmospheric and oceanographic data. Besides being used for the transfer of data, BUFR is used as an on-line storage format and as a data archiving format. A BUFR record (message) containing observational data of any sort also contains a complete description of what those data are: the description includes identifying the parameter in question, (height, temperature, pressure, latitude, date, and time), the units, any decimal scaling that may have been employed to change the precision from that of the original units, data compression that may have been applied for efficiency, and the number of binary bits used to contain the numeric value of the observation. BUFR is a purely binary or bit oriented form. The following standard is mandated:

- FM 94-X Ext. BUFR WMO No. 306, Manual on Codes, International Codes, Volume I.2 (Annex II to WMO Technical Regulations) Parts B and C.

2.2.2.1.4.10 File Compression

File Compression techniques can reduce the number of bits required to represent information in a file thereby reducing storage requirements and bandwidth resource consumption during file transfer. For the interchange of files among different platforms and organizations, a common,

general purpose and platform-independent file compression format is useful. Unless another more specific mandated compression format is defined within a Service area (e.g. NITF JPEG) the following compressed file format is mandated:

- IETF Request For Comment (RFC)-1952, GZIP File Format Specification, Version 4.3, 23 May 1996.

2.2.2.1.4.11 Electronic Commerce Data Interchange

Refer to Appendix D.2.2.1.4 for requirements on message standards.

2.2.2.1.5 Graphic Services

These services support the creation and manipulation of graphics. The following standards are mandated for non-COTS graphics development:

- ANSI/ISO/IEC 9636-1,2,3,4,5,6:1991 (R1997), Information Technology Computer Graphics Interfacing (CGI) Techniques for Dialogue with Graphics Devices.
- The OpenGL Graphics System: A Specification (Version 1.2.1), 1 April 1999.

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. They include kernel operations, shell, and utilities. The operating system controls access to information and the underlying hardware. These services will be accessed by applications through either the standard Portable Operating System Interface (POSIX®) or Win32 APIs. The operating system services mandates in this section currently do not apply to limited-use handheld devices like Personal Digital Assistants (PDAs) and Palmtops. When choosing an OS for hand-held devices, developers should consider the need to integrate these devices with existing desktop and server-based systems, and whether application code from these systems can be reused on the hand-held devices.

When requiring real-time operating systems, the IEEE 1003.13:1998 Standardized Application Environment Profile - POSIX® Realtime Application Support standard should be considered for use. It has been designed to satisfy a wide range of real-time system requirements based upon the Application Platform's size and function. It identifies four real-time application environment profiles based on the ISO/IEC 9945-1 series of standards including: Minimal Realtime System Profile (PSE51), Realtime Controller System Profile (PSE52), Dedicated Realtime System Profile (PSE53), and Multi-Purpose Realtime System Profile (PSE54).

Not all operating-system services are required to be implemented, but those that are used will comply with the standards listed below.

Note: References to 'C language' and 'Ada language' are part of the formal titles of some standards in this section, denoting the language used to define the standard.

The following standards are mandated for use with POSIX®-compliant operating systems running (or intended to run) POSIX®-compliant applications:

- ISO/IEC 9945-1:1996, Information Technology - Portable Operating System Interface (POSIX®) Part 1: System Application Program Interface (API) [C language] (Mandated Services).
- ISO/IEC 9945-1:1996, (Real-time Extensions) to ISO/IEC 9945-1:1996, Information Technology - Portable Operating System Interface (POSIX®) - Part 1: System Application Program Interface (API) [C language] (Real-time Optional Services).
- ISO/IEC 9945-1:1996:(Thread Extensions) to ISO/IEC 9945-1:1996, Information Technology - Portable Operating System Interface (POSIX®) - Part 1: System Application Program Interface (API) [C language] (Thread Optional Services).
- ISO/IEC 9945-2:1993, Information Technology Portable Operating System Interface (POSIX®) - Part 2: Shell and Utilities, Information Technology - Portable Operating System Interface (POSIX®) - Recommendations (Section 12) and Implementation Guidance (Section 13).
- IEEE 1003.2d:1994, POSIX® - Part 2: Shell and Utilities – Amendment 1: Batch Environment.
- ISO/IEC 14519:1999, Information Technology - POSIX® Ada Language Interfaces -Binding for System Application Program Interface (API) - Realtime Extensions.

Documentation for the Win32 APIs is found within the Microsoft Platform SDK. This documentation is mandated for use with any operating system running (or intended to run) Win32 applications:

- Win32 APIs, as specified in the Microsoft Platform SDK.

2.2.2.1.8 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 8859-1:1998, Information technology -- 8-bit single-byte coded graphic character sets -- Part 1: Latin alphabet No. 1.
- ISO/IEC 10646-1:2000, Information Technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane.

2.2.2.1.9 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.

2.2.2.1.10 System Management Services

These services provide capabilities to manage an operating platform and its resources and users. System management services include configuration management, network management, fault management, and performance management. The standards that apply are provided in Section 3.

2.2.2.1.11 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. Because of the declining use of the Distributed Computing Environment (DCE), the JTA-Army no longer mandates any specifications for Remote Procedure Computing.

Currently, there are a number of competing middleware technologies, which enable distributed objects to interoperate. In recognizing that each of these distributed-object computing technology has strengths that differentiate it from the others, the JTA-Army does not mandate the use of any single one. However, in order to ensure interoperability between application objects in heterogeneous distributed environments or different object models, the JTA-Army mandates a requirement for interworking with the Object Management Group (OMG) Object Management Architecture (OMA). The OMA is composed of the Common Object Request Broker Architecture (CORBA), CORBA services, and CORBA facilities. Interworking with the following specification is mandated:

- OMG document formal/99-10-07, Common Object Request Broker: Architecture and Specification, Version 2.3.1, October 1999.

2.3 EMERGING STANDARDS

2.3.1 Application Software Entity

2.3.1.1 Environment Management

2.3.1.1.1 Learning Technology

Learning Technology standards provide for an integrated environment for education, training, and decision support and are considered a subset of the Environment Management services within the DOD TRM. A growing number of technical standards for this field are in varying stages of development by standards bodies including the following, each of which can be accessed on the Web at the following URLs: Educom Instructional Management System, <http://www.imsproject.org>, Aviation Industry Computer-Based Training (CBT) Committee <http://www.aicc.org>, Alliance of Remote Instructional Authoring and Distribution Networks for Europe (ARIADNE) <http://ariadne.unil.ch/main.htm>, and IEEE Learning Technology Standards Committee <http://www.manta.ieee.org/P1484>.

The following standards are being tracked as Learning Technology emerging standards:

- IEEE 1484.1, Architecture and Reference Model Working Group Document: Learning Technology Systems Architecture (LTSA), Draft 5, 1999-12-08.
- IEEE P1484.2, Learner Model Working Group Document: Public and Private Information (PAPI) for Learners, Draft Version 6, 2000-06-23.
- IEEE 1484.11, Computer Managed Instruction (CMI) Working Group Document: Computer-Managed Instruction (CMI), Draft 3.3, 1999-02.

- IEEE P1484.12, Learning Object Metadata (LOM), Working Group Document: Learning Object Metadata, Draft 4, 2000-02-05.

2.3.1.1.2 Electronic Records Management

DoD 5015.2-STD, Design Criteria Standard for Electronic Records Management Software Applications, Sections 2.2.1 through 2.2.11, provides a mandatory baseline set of requirements for Records Management Application (RMA) software. RMA software may be used by DoD Components in the implementation of records management programs. Each official Component record is defined by an approved Records Control Schedule (RCS). If a Component chooses to maintain official records in an electronic form, those records must be managed by application(s) consistent with this standard. Future versions of this standard will address interoperability requirements. The following standard is emerging:

- DoD-5015.2-STD, Design Criteria Standard for Electronic Records Management Software Applications, November 1997 (Sections 2.2.1-2.2.1.1 only).

2.3.1.2 Business Processing

Current workflow applications available from different vendors are for the most part stove-piped systems having little or no cross-vendor interoperability. The Workflow Management Coalition (WFMC) accessible at <http://www.aiim.org/wfmc/mainframe.htm> has promulgated a terminology and glossary as well as a Workflow Reference Model (WRM) that identifies five interfaces from a central Workflow Enactment Service. In addition, the WFMC has published at least one specification for each of the five interfaces. These WFMC specifications provide the basic framework for achievement of interoperability between disparate workflow applications and for the integration of existing services in support of workflow applications. The following specifications are emerging:

- OMG document formal/2000-05-02, Workflow Management Facility Specification, V1.2 April 2000
- WFMC-TC-1016-P, Workflow Management Coalition, Interface 1: Process Definition Interchange, Process Model, 12 November 1998
- WFMC-TC-1013, Workflow Management Coalition, Workflow Client Application (Interface 2) Application Programming Interface (WAPI), Naming Conventions, 1 November 1997
- WFMC-TC-1009, Workflow Management Application Programming Interface (Interface 2&3) Specification, July 1998
- WFMC-TC-1018, Workflow Management Coalition, Workflow Standard - Interoperability, Internet e-mail MIME Binding, 25 September 1998
- WFMC-TC-1023, Workflow Management Coalition, Workflow Standard - Interoperability WF-XML Binding, 20 April 1999.

2.3.2 Application Platform Entity

2.3.2.1 Application Programming Interface for XML-Based Information

Document Object Model (DOM) and Simple API for XML (SAX) APIs are used for this purpose. These are described under Section 4.3.8.2 *XML Parsing and Manipulating*.

2.3.2.1.1 Operating System Services

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.

2.3.2.1.1.1 Distributed-Object Computing

The emerging standards for distributed object computing are the specifications, which are included in the OMG's CORBA 3. These include specifications for three major categories: Internet Integration, Quality of Service Control, and the CORBA component architecture. Additional details can be found on the OMG's website <http://www.omg.org/>.

2.3.2.1.1.2 Graphic Data Interchange

The PNG 1.2 specification is currently in the Final Committee draft (FCD) stage with the ISO/IEC. The following is an emerging standard:

- ISO/IEC 15948:2000, Portable Network Graphics (PNG): Functional Specification Final Committee Draft (FCD).

2.3.2.1.1.3 Multiple-Image Network Graphics

The Multiple-Image Network Graphics (MNG) format is an extension to the PNG format, developed by the PNG Development Group, for the storage and transmission of animated graphics and complex still images. It was designed to replace GIF animation with a true animation format. The following standard is emerging:

- MNG (Multiple-Image Network Graphics) Format Version 1.0, January 2001.

2.3.2.1.1.4 Virtual Reality Modeling Language

The Virtual Reality Modeling Language (VRML) is a commercial standard with capabilities for 3-D representation of data. The following standard is emerging:

- ISO/IEC 14772-1:1998, Information Technology - Computer graphics and Image Processing -The Virtual Reality Modeling Language - Part 1: Functional specification and UTF-8 encoding.

2.3.2.1.1.5 Still-Imagery Data Interchange

JPEG 2000 Image Coding System provides a new means of image representation containing a rich set of features, all supported within the same compressed bit stream. The following standard is emerging:

- ISO/IEC 15444-1, Information Technology - JPEG 2000 Image Coding System - Part 1: Core Coding System.

2.3.2.1.1.6 Motion-Imagery Data Interchange

The following emerging standards shown in Table 2-3, are profiled by the Motion Imagery Standards Profile (MISP) 1.7, Chapter 2.0, Commercial Standards, Interoperability Profiles, and

Recommended Practices for Army systems using DoD/IC/USIGS Implementations, 27 July 2000 are as follows:

TABLE 2-3 - EMERGING STANDARDS FOR MOTION IMAGERY STANDARDS PROFILE (MISP)

Standard	Title	Usage
SMPTE RP210.2-2000	SMPTE Metadata Dictionary Contents, 2000	Dictionary Contents
SMPTE EG37-2000	Node Structure for the SMPTE Metadata Dictionary, 2000	Dictionary Node Structure
SMPTE 335M-2000	Dynamic Metadata Dictionary Structure, 2000	Dictionary Structure
SMPTE 336M-2000	Data Encoding Using Key-Length Value (KLV), 2000	Standard Protocol for Encoding Metadata into Video Datastreams
MISP 9716	Packing KLV Packets into SMPTE 291M Ancillary Data Packets, 20 October 1999	Standard Method for Packing Metadata into 291M
MISP 9717	Packing KLV Packets into MPEG-2 Systems Streams, 20 October 1999	Standard Method for Packing Metadata into MPEG-2
SMPTE 355M-2000	Format for Non-PCM Audio and Data in AES3 - KLV Data Type, 2000	Standard Method for Packing Video Metadata into AES

The following standard is emerging for advance television applications:

- ATSC Doc. A/52, Digital Audio Compression Standard (AC-3), 20 December 1995.

2.3.2.1.1.7 Document Interchange

XHTML (eXtensible Hypertext Markup Language) is the next-generation follow-on to HTML. XHTML reformulates HTML as an XML (eXtensible Markup Language) application, bringing the modular capabilities of XML to web development. A single XML data stream can be used by a variety of applications to support multiple devices, such as cellular telephones, computers, Web television, and embedded applications simply by processing the needed XHTML tags within the XML data stream. The following standard is emerging:

- XHTML(tm) 1.0: The Extensible Hypertext Markup Language: A Reformulation of HTML 4 in XML 1.0, W3C Recommendation 26, January 2000. <http://www.w3.org/TR/2000/REC-xhtml1-20000126>.

XForms architecture separates purpose (semantics) from presentation (syntax), and associates the capabilities of XML and the ease of HTML for a wide range of devices. The following standards are emerging:

- XForms 1.0: Data Model W3C Working Draft, 06 April 2000.
- XForms Requirements, W3C Working Draft, 29 March 2000.

2.3.2.2 Data Management Services

Parts one through five of the emerging SQL3 specification were completed in December 1999 and contain a number of data abstraction facilities, including user-defined data types and methods. The emerging SQL specification also contains facilities for defining and referencing object identifiers. Additionally, the emerging SQL3 specification supports knowledge-based data management and remote data access capabilities. The following SQL3 standards are emerging:

- ANSI/ISO/IEC 9075-1:1999, Information technology - Database languages - SQL - Part 1: Framework (SQL/Framework).
- ANSI/ISO/IEC 9075-2:1999, Information technology - Database languages - SQL - Part 2: Foundation (SQL/Foundation).
- ANSI/ISO/IEC 9075-3:1999, Information technology - Database languages - SQL - Part 3: Call-Level Interface (for SQL3).
- ANSI/ISO/IEC 9075-4:1999, Information technology - Database languages - SQL - Part 4: Persistent Stored Modules (SQL/PSM).
- ANSI/ISO/IEC 9075-5, Information technology - Database languages - SQL - Part 5: Host Language Bindings (SQL/Bindings).

SQL Multimedia (SQL/MM) is a set of extensions to the SQL3 specification and will specify packages of SQL abstract data type (ADT) definitions using the facilities for ADT specification and invocation provided in the SQL3 specification. SQL/MM intends to standardize class libraries for science and engineering; full-text and document processing; and methods for the management of multimedia objects such as image, sound, animation, music, and video. The emerging standard for SQL/MM is:

- ISO/IEC 13249-3:1999, Information technology - Database languages - SQL Multimedia and Application Packages - Part 3: Spatial.

The SQL - RDA standard specifies a message format for remote communication of SQL database language statements (query and update) to a remote database. The specification defines uses of the message fields and other implementation information including sequencing and how SQL statements map to the Remote Database Access (RDA) protocol, a TCP/IP-compatible communications protocol that enables a database client to gain access to database servers. The emerging standard for SQL - RDA is:

- ISO/IEC 9579:2000, Information technology - Remote Database Access for SQL with security enhancement.

The Object Database Management Group (ODMG) has published a third version of their standard for an Object Storage API that can work with any DBMS or tool. The ODMG has defined a comprehensive object model, described an object specification language, defined an object interchange format, defined an object query language (based on the relational query language, SQL) and worked to make the programming language bindings consistent with the ODMG model. Version 3.0 improves the ODMG model, enhances the Java bindings, and broadens the standard for use by object-relational mapping systems as well as for object DBMSs. The ODMG specification is published as a hardcover book. The following standard is emerging:

- The Object Database Standard: ODMG 3.0, Edited by R.G.G. Cattell et al. The Morgan Kaufmann Series in Data Management, 2000, ISBN 1-55860-647-4.

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 4.2.6.2 will 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 end-systems, networks, and transmission media. End-systems (e.g., host computers, terminals) generally execute applications on behalf of users and share information with other end-systems via networks. Networks may be relatively simple (e.g., point-to-point links or sub-networks that are homogenous in protocol stacks) or have complex internal structures of diverse sub-networks. The term networks also include routers, which interconnect two or more sub-networks and forward packets across sub-network boundaries. Routers are distinct from hosts in that they are normally not the destination of data traffic. End-systems and networks are connected by transmission media.

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

The Internet Engineering Task Force (IETF) publishes a number of the standards mandated in this section. The IETF 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

IETF Standard 3 consists of RFC-1122 and RFC-1123. These pair of documents defines and discusses the requirements for host system implementations of the Internet Protocol suite. RFC-1122 covers the communications protocol layers (link layer, IP layer, and transport layer). RFC-1123 covers the application layer protocols. Both RFCs amend, correct, and supplement the primary protocols standards documents relating to the hosts. The following standard is mandated:

- IETF Standard 3 (IETF RFC-1122 and IETF RFC-1123), Requirements for Internet Hosts, October 1989.

3.2.1.1.1 Application Support Services

3.2.1.1.1.1 Electronic Mail

The standard for official organizational messaging traffic between DoD organizations is the Defense Message System's (DMS) X.400-based suite of military messaging standards defined in Allied Communication Publication (ACP) 123. The ACP 123 annexes contain standards profiles for the definition of the DMS "Business Class Messaging" (P772) capability and the Message Security Protocol (MSP). Organizational messaging is considered a high assurance messaging service that requires authentication, delivery confirmation, and encryption. See Section 6 for security standards. Since X.400 is not an internet standard, see Section 3.2.1.1.2.2 for operation over Internet Protocol (IP) based networks. The following standards are mandated:

- ACP 123 Edition A, Common Messaging Strategy and Procedures, 15 August 1997.
- ACP 123 - Common Messaging Strategy and Procedures (US Supplement No. 1) US SUPP-1 dated 28 March 1997.

DMS has expanded its baseline to include a medium assurance messaging service. The requirements for medium assurance messaging are less stringent than organizational messaging and can be met by existing IP-based mail standards. This allows the augmentation of DMS to include the use of the Simple Mail Transfer Protocol (SMTP) for medium assurance messaging. For SMTP, the following standards are mandated:

- IETF Standard 10/IETF RFC-821/IETF RFC-1869/IETF RFC-1870, Simple Mail Transfer Protocol (SMTP) Service Extensions, November 1995.
- IETF Standard 11/IETF RFC-822/IETF RFC-1049, Standard for the Format of ARPA Internet Text Messages, August 1982.
- IETF RFCs 2045-2049, Multipurpose Internet Mail Extensions (MIME) Parts 1-5, November 1996.

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 Lightweight Directory Access Protocol (LDAP)

LDAP (Version 2) is an internet protocol for accessing online directory services. It runs directly over TCP. LDAP derives from the X.500 Directory Access Protocol (DAP). It is appropriate for

systems, which need to support a medium grade of service where security is not an issue and access is only needed to a centralized server. The following standard is mandated:

- IETF RFC-1777, LDAP, March 1995.

3.2.1.1.1.2.3 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:

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

Dynamic DNS enables the automation of DNS updating by introducing a new messaging mechanism to selectively insert or delete new entries into or from the DNS database. The following standard is mandated:

- IETF RFC-2136, Dynamic Updates in the Domain Name System, April 1997.

3.2.1.1.1.3 File Transfer

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

- IETF Standard 9/IETF 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

For ASCII text oriented remote terminal services, Telecommunications Network (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:

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

Remote terminal services supporting graphics oriented environments on UNIX® platforms is accomplished using the windows based 'XTERM' functionality. Refer to section 2.2.2.1.2 of this document wherein Common Desktop Environment (CDE) is mandated.

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:

- IETF RFC-1305, Network Time Protocol (V3), March 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:

- IETF RFC-951, Bootstrap Protocol, September 1, 1985.
- IETF RFC-2132, DHCP Options and BOOTP Vendor Extensions, March 1997.
- IETF 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. The following standard is mandated:

- IETF RFC-2131, Dynamic Host Configuration Protocol, March 1997.

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:

- IETF RFC-2616, Hypertext Transfer Protocol - HTTP /1.1, June 1999.

3.2.1.1.1.9.2 Uniform Resource Identifier (URI)

A Uniform Resource Identifier (URI) is a string identifying an abstract or physical resource on a network. Uniform Resource Locators (URLs) are the subset of URIs that identify resources via a network 'location.' URIs (particularly URLs) are used extensively on the Internet. RFC 2396 defines the generic syntax of URIs, while RFC 1738 defines the syntax for specific URL schemes (such as http: and ftp:). For the syntax of URIs and URLs, the following standards are mandated:

- IETF RFC-1738, Uniform Resource Locators, 20 December 1994.
- IETF RFC 2396, Uniform Resource Identifiers (URI), Generic Syntax, August 1998.

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)

There are no mandated standards.

3.2.1.1.2.2 Transmission Control Protocol (TCP)

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

- IETF Standard 7/IETF RFC-793, Transmission Control Protocol, September 1981. PUSH flag and NAGLE algorithm, as defined in IETF Standards 3, Host Requirements are mandated.
- IETF RFC 2581, TCP Congestion Control, April 1999.

3.2.1.1.2.3 User Datagram Protocol (UDP)

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

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

3.2.1.1.2.4 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:

- IETF Standard 5/IETF RFC-791/IETF RFC-950/IETF RFC-919/IETF RFC-922/IETF RFC-792/IETF 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.

Internet Group Management Protocol (IGMP) as defined by RFC-1112 is an integral part of Standard 5. IGMP v2 updates RFC-1112 by defining minor changes to the message codes and version/type fields of the datagram structure. For routers using IGMPv2, the following additional standard is mandated:

- IETF RFC-2236, Internet Group Management Protocol, Version 2, November 1997.

For hosts that transmit or receive multi-addressed datagrams over Combat Net Radio (CNR), the multi-addressed IP option field must be used. The following is mandated:

- IETF Informational RFC-1770, IPv4 Option for Sender Directed Multi-Destination Delivery, 28 March 1995.

3.2.1.1.2.5 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:

- IETF Standard 35/IETF RFC-1006, ISO Transport Service on top of the TCP, May 1987.

3.2.1.2 Video Teleconferencing (VTC) Standards

The ASD (C3I) mandated Federal Telecommunications Recommendation (FTR) 1080A-1998Video Teleconferencing Profile identifies ITU-T H.320 as the key standard to provide interoperability between VTC terminal equipment, both point-to-point and multipoint configurations operating at data rates of 56-1,920 Kilobits per second (Kbps). ITU-T H.320, Narrow Band Visual Telephone Systems and Terminal Equipment, July 1997, is an umbrella standard of recommendations addressing audio, video, signaling, and control. Also in the FTR is ITU-T T.120, Transmission Protocols for Multimedia Data, July 1996, which references a family of standards for applications implementing the features of audio graphic conferencing, facsimile, still-image transfer, annotation, pointing, whiteboard, file transfer, audiovisual control, and application sharing.

For VTC units (VTUs) and Multipoint Control Units (MCUs) operating at data rates of 56-1,920Kbps, except for operation over packet-based TCP/IP networks, the standards contained in FTR1080A-1998, Appendix A (See Table 3-1) are mandated:

- FTR 1080A-1998, Appendix A, Video Teleconferencing Profile, October 1998.

TABLE 3-1 - VTC STANDARDS FOR DATA RATE 56-1920 KBPS

Standard	Description	Usage
H.221	Frame structure for 64 to 1920 Kbit/s channel in audio visual services, May 1999	VTU/MCU General
H.230	Frame-synchronous control and indication signals for audio visual systems, May, 1999	VTU/MCU General
H.242	System for establishing communication between audio visual terminals using digital channels up to 2 Mbits/s, May, 1999	VTU/MCU General
H.261	Video CODEC for audiovisual services at px64 Kbps, March, 1993	VTU/MCU Video
H.320	Narrow-band visual telephone systems and telephone equipment, May, 1999	VTU/MCU General
T.120	Transmission protocols for multimedia data, July 1996	VTU/MCU Multimedia
T.122	Multipoint communications service for audiographic and audio visual conferencing service definition, March 1993	VTU/MCU Multimedia
T.123	Protocol stacks for audiographic and audio visual teleconferencing applications, May, 1999	VTU/MCU Multimedia
T.124	Generic conference control for audiographic and audio visual terminals and multipoint control units, January, 1998	VTU/MCU Multimedia
T.125	Multipoint communications service protocol specification, February, 1998	VTU/MCU Multimedia
T.126	Multipoint still image and annotation conferencing protocol specification, July, 1997	VTU Multimedia
T.127	Multipoint binary file transfer protocol, August, 1995	VTU Multimedia
T.128	Multipoint application sharing, January, 1998	VTU Multimedia
T.4	Group 3 facsimile – hardcopy representation, July, 1996	VTU Multimedia
T.82	Softcopy image compression (Joint Bi-level Image Experts Group [JBIG]), March, 1993	VTU Multimedia
T.81	Softcopy color image compression (Joint Photographic Experts Group [JPEG]), September, 1992	VTU Multimedia
H.224	Real-time control protocol for simplex applications using the H.221 LSD/HSD/MLP channels, November, 1994	VTU Multimedia
H.281	Far-end camera control protocol for video conferences using H.224, November, 1994	VTU Multimedia
G.711	Pulse code modulation 3.1 KHz to 48, 56, and 64 (narrowband speech mode), November, 1988	VTU Audio
G.722	Audio CODEC, 7 KHz at 48, 56, and 64 Kbps (wideband speech), November, 1988	VTU/MCU Audio
G.728	Audio CODEC 3.1 KHz at 16 Kbps (narrowband speech mode), September, 1992	VTU/MCU Audio
H.231	Multipoint control unit functional description, July, 1997	MCU General
H.243	Procedure for establishing communication between three or more audio visual terminals using digital channels up to 2 Mbit/s, July, 1997	MCU General
EIA-422B	Electrical characteristics of balanced voltage digital interface circuits, 1994	VTU/MCU Encryption Interface

For applications implementing the features of audiographic conferencing, facsimile, still-image transfer, annotation, pointing, whiteboard, file transfer, audiovisual control, and application sharing, over LANs and at low bit rates (9.6-28.8 Kbps), the following standard is mandated:

- ITU-T T.120, Transmission Protocols for Multimedia Data, July 1996.
- For VTC terminals operating within IP Packet Networks, the following standard is mandated: ITU-T H.323, Packet-based Multimedia Communications Systems, January 1998.

For all other implementations of H.323, such as used over wide area networks, bandwidth, quality of service, and scalability may not be sufficient for IP-based video conferencing. For VTC terminals operating at low bit rates (9.6 to 28.8 Kbps) the following standard is mandated:

- ITU-T H.324, Terminal for Low Bit Rate Multimedia Communications, January 1998.

For inverse multiplexers connected to VTC terminals, and for VTC terminals with built-in inversemultiplexers, the following standard is mandated:

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

For information on the ASD (C3I) VTC guidance and the Federal Telecommunications Recommendation FTR 1080A-1998 Video Teleconferencing Profile, see URL: <http://www.ncs.gov/n6> and URL: <disavtc.spawars.navy.mil>.

3.2.1.3 Facsimile Standards

3.2.1.3.1 Analog Facsimile Standard

For Facsimile (analog output) standards, which comply with the 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-A, Procedures for Document Facsimile Transmission, 27 September 1996.

3.2.1.3.2 Digital Facsimile Standard

Digital Facsimile equipment standards for Type I and/or Type II modes are used for digital facsimile terminals operating in tactical, high Bit Error Rate (BER) environments, and for facsimile transmissions utilizing encryption or interoperability with NATO countries. The following standard is mandated:

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

3.2.1.4 Imagery Dissemination Communications Standards

Refer to Appendix E.2.3.1.1.1.

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. IETF 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:

- IETF RFC-1812, Requirements for IP Version 4 Routers, June 22, 1995.
- IETF Standard 6/IETF RFC-768, User Datagram Protocol, August 1980.
- IETF Standard 7/IETF RFC-793, Transmission Control Protocol, September 1981.
- IETF Standard 8/IETF RFC-854/IETF RFC-855, TELNET Protocol, May 1983.
- IETF Standard 13/IETF RFC-1034/IETF RFC-1035, Domain Name System, November 1987.
- IETF RFC-951, Bootstrap Protocol, September 1, 1985.
- IETF RFC-2132, DHCP Options and BOOTP Vendor Extensions, March 1997.
- IETF RFC-2131, Dynamic Host Configuration Protocol, March 1997.
- IETF RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, October 27, 1993.
- IETF Standard 33/IETF 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:

- IETF Standard 5/IETF RFC-791/IETF RFC-950/IETF RFC-919/IETF RFC-922/IETF RFC-792/IETF RFC-1112, Internet Protocol, September 1981.

Internet Group Management Protocol (IGMP) as defined by RFC-1112 is an integral part of Standard 5. IGMPv2 updates RFC-1112 by defining minor changes to the message codes and version/type fields of the datagram structure. For routers using IGMPv2, the following additional standard is mandated:

- IETF RFC-2236, Internet Group Management Protocol, Version 2, November 1997.

For hosts that transmit or receive multi-addressed datagrams over Combat Net Radio (CNR), the multi-addressed IP option field must be used. The following is mandated:

- IETF Informational RFC-1770, IPv4 Option for Sender Directed Multi-Destination Delivery, 28 March 1995.

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. For unicast interior gateway routing the following standard is mandated:

- IETF Standard 54/ RFC-2328, Open Short Path First Routing Version 2, April 1998.

3.2.2.1.2.2 Exterior Routers

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

- IETF RFC-1771, Border Gateway Protocol 4, March 21, 1995.
- IETF 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, 100 Mbps, or 1,000 Mbps. Hosts use a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) scheme to control access to the cable.

At the physical layer, 10 Mbps Ethernet is implemented with any of six different types of cable. 10 Mbps Ethernet's physical layer and CSMA/CD access scheme are specified in the following mandated standards:

- 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.

For framing, Ethernet V2 framing is mandated in lieu of 802.2 framing on Ethernet LANs.

For Bridging (or switching) among Ethernet LAN segments, the following standards are mandated:

- 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.

For the interface between Ethernet and IP, the following standards are mandated:

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

An extension to Ethernet, Fast Ethernet provides interoperable service at both 10 Mbits/s and 100 Mbits/s. Higher speed interconnections are provided by 100BASE-TX (two pairs of Category 5 unshielded twisted pair, with 100BASE-TX Auto-Negotiation features employed to permit interoperation with 10BASE-T). For platforms physically connected to a Joint Task Force LAN, the following standards are mandated as the minimum set for operation in a Joint Task Force:

- ISO/IEC 8802-3:1996, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 10BASE-T Medium-Access Unit (MAU).
- IEEE 802.3u-1995, Supplement to ISO/IEC 8802-3:1993, Local and Metropolitan Area Networks: Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100 Mbps Operation, Type 100BASE-T (Clauses 21-30).
- IETF Standard 41/IETF RFC-894, Standard for the Transmission of IP Datagrams Over Ethernet Networks, April 1984.
- IETF Standard 37/IETF RFC-826, An Ethernet Address Resolution Protocol, November 1982.

When using Gigabit Ethernet, which provides service at 1,000 Mbps, the following physical layer and framing standards are mandated:

- IEEE 802.3-1998 Edition Information Technology (Clauses 34-42)-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, (which includes IEEE 802.3z-1998).
- IEEE 802.3ab-1999 Supplement to IEEE 802.3-1998: Physical Layer Parameters and Specifications for 1000 Mb/s Operation over 4-Pair of Category 5 Balanced Copper Cabling, Type 1000BASE-T.

For Ethernet management, the following is mandated:

- 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:

- IETF Standard 51/IETF RFC-1661/IETF RFC-1662, Point-to-Point Protocol (PPP), July 1994.
- IETF RFC-1332, PPP Internet Protocol Control Protocol (IPCP), May 26, 1992.
- IETF RFC-1989, PPP Link Quality Monitoring, August 1996.
- IETF RFC-1994, PPP Challenge Handshake Authentication Protocol (CHAP), August 1996.
- IETF RFC-1570, PPP Link Control Protocol (LCP) Extensions, January 11, 1994.
- IETF RFC-1990, The PPP Multilink Protocol, August 1996.

For the serial line interface, one of the following is mandated:

- Electronics Industries Association's (EIA)/TIA-232-F, Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, October 1997.
- 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/TIA-530-A, High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment, December 1998, 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-188-220B. With the exception of High Frequency (HF) networks, MIL-STD-188-220B will be used as the standard communications net access protocol for CNR networks. The following standard is mandated:

- MIL-STD-188-220B, Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, January 20, 1998.

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 –1999 ISDN Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT (Layer 1 Specification), 1999.
- ANSI T1.605-1991 (R1999), ISDN Basic Access Interface for S and T Reference Points - Layer 1 Specification, 1991.

For the PRI Physical Layer:

- ANSI T1.403.01-1999, ISDN Primary Rate - Customer Installation Metallic Interfaces (Layer 1 Specification), 1999.

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 (DSS1) - Layer 3 Signaling Specification for Circuit Switched Bearer Service, 1998.
- ANSI T1.610-1998, DSS1 - Generic Procedures for the Control of ISDN Supplementary Services, 1998.
- 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 will be as profiled by the following National ISDN documents as adopted by the North American ISDN Users' Forum (NIUF).

For addressing:

- ITU-T E.164, Numbering Plan for the ISDN Era, May 1997.
- DISA Circular (DISAC) 310-225-1, Defense Switched Network (DSN) User Services Guide, 2 April 1998.

For transmitting IP packets when using ISDN packet-switched services:

- IETF RFC-1356, Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode, 6 August 1992.

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

- IETF RFC-1618, PPP over ISDN, May 1994.

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 adapt any traffic (video streams, data packets from upper layer protocols) into the ATM format of 48 octet payload. It also receives the cells from the ATM layer and reassembles the protocol data units. The ATM Layer adds the necessary header information that is used by switches and end systems alike to transfer cells across the ATM network. The Physical Layer converts the cell information to the appropriate electrical/optical signals for the given transmission medium. The ATM Forum's User-Network Interface (UNI) Specification defines the primary specification for end-system connection to ATM networks. The Private Network-Network Interface (PNNI) Specification defines the PNNI protocol for use between private ATM switches, and between groups of private ATM switches. The PNNI supports the distribution of topology information between switches and clusters of switches to allow paths to be computed through the network. The PNNI also defines the signaling to establish point-to-point and point-to-multipoint connections across the ATM network. ATM Forum's Local Area Network Emulation supports the emulation of Ethernet allowing ATM Networks to be deployed without disruption of host network protocols and applications. For information on the ASD C3I ATM guidance, see URL: <http://www.disa.mil>. The following standards are mandated:

For Physical Layer:

- ATM Forum, af-phy-0040.000, Physical Interface Specification for 25.6 Mb/s over Twisted Pair Cable, November 1995.
- ATM Forum, af-uni-0010.002, ATM UNI Specification V 3.1, Section 2.1and 2.4, September 1994.
- ATM Forum, af-phy-0015.000, ATM Physical Medium Dependent Interface Specification for 155 Mb/s over Twisted Pair Cable, September 1994.
- ATM Forum, af-phy-0016.000, DS1 Physical Layer Interface Specification, September 1994.
- ATM Forum, af-phy-0054.000, DS3 Physical Layer Interface Specification, January 1996.
- ATM Forum, af-phy-0046.000, 622.08 Mb/s Physical Layer Specification, January 1996.
- ATM Forum, af-phy-0064.000, E-1 Physical Layer Interface Specification, September 1996.
- ATM Forum, af-phy-0043.000, A Cell-based Transmission Convergence Sublayer for Clear Channel Interfaces, November 1995.
- ATM Forum, af-phy-0086.000, Inverse Multiplexing for ATM (IMA) Specification Version 1.0, July 1997.

For User to Network Interface:

- ATM Forum, af-uni-0010.002, ATM User-Network Interface Specification (UNI) Specification, Version 3.1, September 1994.
- ATM Forum, af-sig-0061.000, ATM User-Network Interface Signaling Specification Version 4.0, July 1996.

For Layer Management Capabilities:

- ATM Forum, af-ilmi-0065.000, Integrated Local Management Interface (ILMI) Specification, Version 4.0, September 1996.
- ATM Forum, af-uni-0010.002, ATM UNI Specification V 3.1, (Section 4: ILMI for UNI 3.1), September 1994.

For Traffic Management Functions:

- ATM Forum, af-tm-0056.000, Traffic Management Specification, Version 4.0, April 1996.

For Circuit Emulation Functions:

- ATM Forum, af-vtoa-0078.000, Circuit Emulation Service Interoperability Specification Version 2.0, January 1997.

For AAL1 and AAL5 Functions:

- ITU-T I.363.1, B-ISDN ATM Adaptation Layer Specification: Type 1 ATM Adaptation Layer (AAL1), August 1996.
- ITU-T I.363.5, B-ISDN ATM Adaptation Layer Specification: Type 5 ATM Adaptation Layer (AAL5), August 1996.

For Private Network-Network Interfaces:

- ATM Forum, af-pnni-0055.000, Private Network-Network Interface Specification Version 1.0 (PNNI 1.0), March 1996.
- ATM Forum, af-pnni-0066.000, Private Network-Network Interface Specification Version 1.0 Addendum (soft PVC MIB), September 1996.

For Local Area Network Emulation and IP Over ATM:

- ATM Forum, af-lane-0084.000, LANE Emulation Over ATM Version 2 - LUNI Specification, July 1997.
- ATM Forum, af-lane-0093.000, LAN Emulation Client Management Specification Version 2.0, October 1998.
- ATM Forum, af-lane-0050.000, LAN Emulation Over ATM Version 1.0 Addendum, December 1995.
- ATM Forum, af-lane-0057.000, LANE Servers Management Specification Version 1.0, March 1996.
- ATM Forum, af-mpoa-0087.000, Multi-Protocol Over ATM, Version 1.0, July 1997.

For ATM Addressing Format:

- DoD ATM Addressing Plan, 17 April 1998.

3.2.2.2.6 Wireless LAN

For Wireless LAN, the following standards are mandated for non-sensitive operations:

- ISO/IEC 8802-11: 1999 (ISO/IEC) (IEEE standard 802.11-1999) Information Technology-Telecommunications and Information Exchange Between Systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
- IEEE 802.11b -1999 Supplement to Information Technology - Telecommunications and Information Exchange Between Systems - Local and metropolitan area networks - Specifications requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band.

3.2.3 Transmission Media

3.2.3.1 Military Satellite Communications (MILSATCOM)

Refer to Appendix E.2.3.1.3.1.

3.2.3.2 Radio Communications

Refer to Appendix E.2.3.1.3.2 Radio Communications.

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 T1.117-1991 (R1997), Digital Hierarchy - Optical Interface Specifications (SONET) (Single Mode - Short Reach), 1991.
- ANSI T1.101-1999, Telecommunications – Synchronization Interface Standard.

The citation of applicable ANSI standards for SONET does not assure interoperability in regions outside North America where standards for these services differ. The JTA-Army recognizes that this is a critical area affecting interoperability but does not recommend specific solutions in this version.

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.

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.

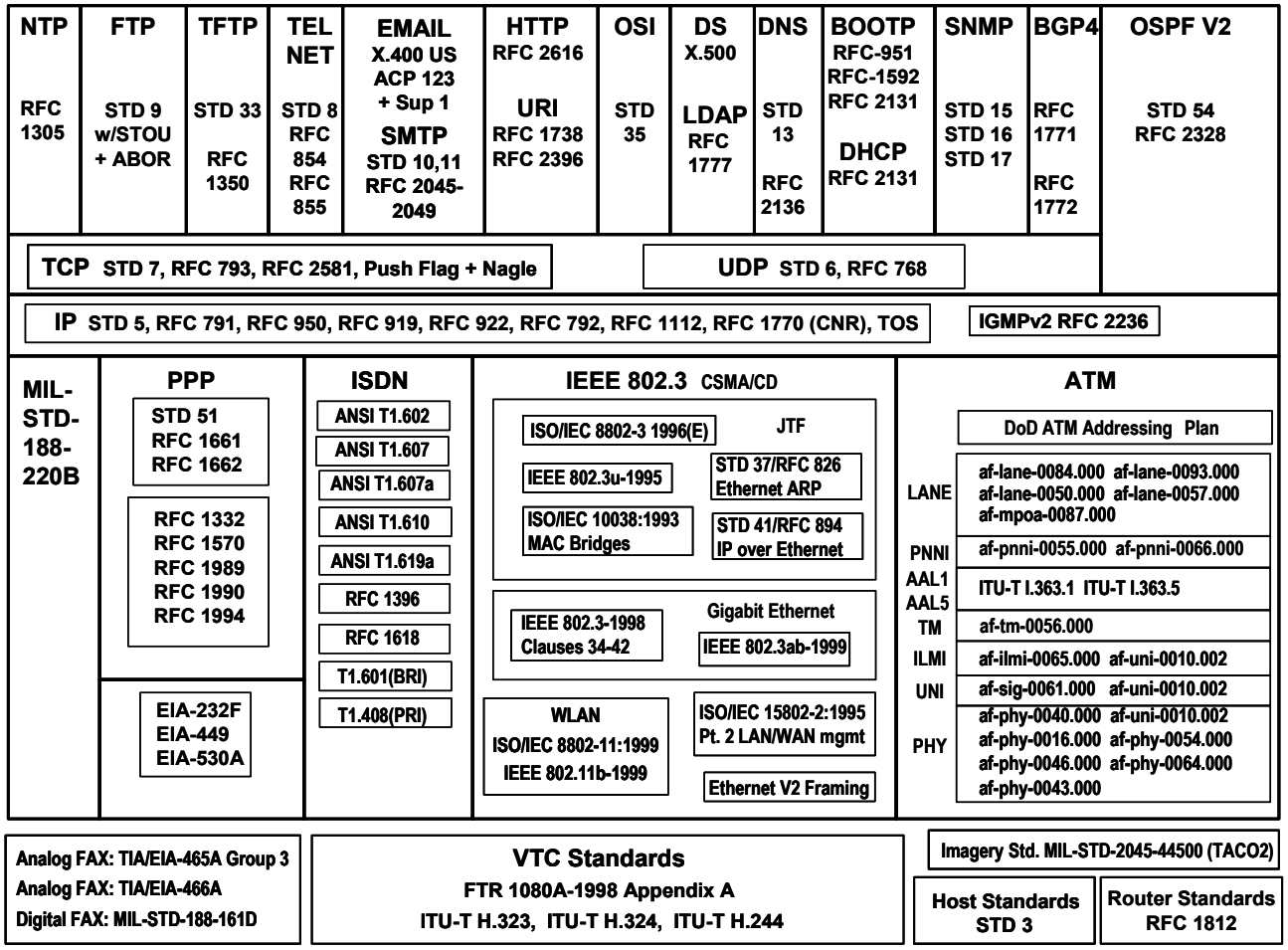


FIGURE 3-1. SUMMARY OF THE PACKET-SWITCHED TRANSFER STANDARDS

3.2.5.1 Data Communications

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

- IETF Standard 15/IETF 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:

- IETF Standard 16/IETF RFC-1155, Structure and Identification of Management Information for TCP/IP-based Internets, May 1990/IETF RFC-1212, Concise MIB Definitions, March 1991.
- IETF Standard 17/IETF RFC-1213, Management Information Base for network management of TCP/IP-based Internets: MIB-II, March 1991.
- IETF RFC-1514, Host Resources MIB, September 1993.
- IETF STD-50/IETF RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994.
- IETF RFC-1757, Remote Network Monitoring Management Information Base, (RMON Version 1), February 1995.
- IETF 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, 1997.
- ANSI T1.208, OAM&P - Upper Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements, 1997.
- 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, 1997.
- ISO/IEC 9595:1998, Information Technology - Open Systems Interconnection Common Management Information Services (CMIS).
- ISO/IEC 9596-1:1998 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 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, auto-configuration, and increased quality of service capabilities. IPv6 is described in the following emerging IETF standards:

- IETF RFC 2374, IPv6 Aggregatable Global Unicast Address Format.
- IETF RFC 2452, IPv6 MIB for the TCP.
- IETF RFC 2454, IPv6 MIB for the UDP.
- IETF RFC 2460, IPv6 Specification.
- IETF RFC 2461, Neighbor Discovery for IPv6.
- IETF RFC 2462, IPv6 Stateless Address Autoconfiguration.
- IETF RFC 2463, ICMPv6 for the IPv6 Specification.
- IETF RFC 2464, Transmission of Ipv6 Packet Over Ethernet Networks.
- IETF RFC 2466, MIB for IPv6:ICMPv6 Group.
- IETF RFC 2472, IPv6 Over PPP.
- IETF RFC 2492, IPv6 Over ATM Networks.

Mobile Host Protocol (MHP) - This protocol allows the transparent routing of IP datagrams to mobile nodes in the Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. A mobile IP protocol is currently available as an IETF proposed standard, IETF RFC-2002, entitled IP Mobility Support.

Video Teleconferencing Standards - There are two emerging standards for VTC over ATM:

- ITU-T H.310 includes underlying standards for video (MPEG2) and audio (MPEG1, MPEG2). H.310 can be used for high-quality VTC requiring > 2 Mbps infrastructure, but does not currently have much industry support.
- ITU-T H.321 specifies the operation of H.320 codecs over ATM using AAL-1 or AAL-5. H.321 uses Quality of Service to manage videoconferencing quality. It lacks industry wide support.

IETF RFC-2581 specifies congestion control algorithms and actions to be completed by TCP connections after relatively long idle periods. It also specifies or clarifies some of the issues pertaining to TCP ACK generation. IETF RFC-2581 may replace IETF RFC-2001 in the next revision. The following standard is emerging:

- IETF RFC-2581, TCP Congestion Control, April 8, 1999.

Lightweight Directory Access Protocol 3 (LDAP v3) - The proposed standard for LDAPv3, IETF RFC-2251, supports standards based authentication, referrals, and all protocol elements of LDAP

(IETF RFC- 1777). Other features still under development include standards based access control, signed operations, replication, knowledge references, and paged results.

Quality of Service - Quality of Service (QoS) is the ability of a network to ensure that the predetermined traffic and service requirements of a network element (e.g., end-system, router, application) can be satisfied. Multiple fora including the IETF and IEEE are engaged in this evolving end-to-end networking effort to enhance the current networking architecture with support for QoS. To provide services over the LAN/WAN beyond the current best-effort IP-based service, the protocols currently under development to enable end-to-end QoS include:

Resource Reservation Protocol (RSVP) - Communicates the QoS requirements for a given application to a device in the path of the transmission. A reservation for the required bandwidth is allowed or denied depending on the current network conditions. RSVP is expected to be utilized predominantly in the campus-level networks. The following standards are emerging:

- IETF RFC 2205 Resource ReSerVation Protocol RSVP-Version 1.
- IETF RFC 2207 RSVP Extensions for IPSEC Data Flows.
- IETF RFC 2380 RSVP over ATM Implementation Requirements.
- IEEE 802.1p and IEEE 802.1q - These IEEE standards specify the traffic classification method used by Ethernet switches, to expedite delivery of time critical traffic. IEEE 802.1p governs the prioritization of packets, offering eight discrete priority levels from the default (best effort) through reserved (highest priority). IEEE 802.1q defines an additional 4-octet field in the LAN header to support Virtual LANs.

3.3.2 Emerging Network Standards

For Wireless LAN, the following standards are mandated for non-sensitive operations:

- Wireless LAN - IEEE 802.11a-1999 Supplement to Information Technology - Telecommunications and Information Exchange Between Systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High Speed Physical Layer (PHY) in the 5 GHz band.
- *ATM-Related Standards* - ATM Forum, af-tm-0121.000, Traffic Management Specification Version 4.1, March 1999 is an ATM Forum standard and replaces Traffic Management Specification Version 4.0 (af-tm-0056.000, April 1996) and Addedum to Traffic Management V4.0 for ABR parameter negotiation (af-tm-0077.000, January 1997). The major advance in this standard include definition of GFR service category and clarifications to UPC, operation of ABR VPCs, and clarifications to VCC to VPC multiplexing effects are provided.
- ATM Forum, af-sig-0076.000, Addendum to UNI Signaling V4.0 for ABR parameter negotiation, January 1997 is an ATM Forum standard addendum to accommodate ABR signaling.
- ATM Forum, af-mpoa-0114.000, Multi-Protocol Over ATM Version 1.1, May 1999 is an ATM Forum standard and incorporates errata document, PICS Proforma, NHRP and MPOA authentication extensions, and new version of MPOA 1.0 MIB.
- ATM Forum, af-vtoa-0113.000, ATM Trunking Using AAL2 for Narrowband Services is an ATM Forum standard and provides efficient transport mechanism to carry voice, voice-band data, circuit mode data, frame mode data, and fax traffic. Voice transport includes support for compressed voice and non-compressed voice together with silence removal.
- ATM Forum, af-phy-0086.001, Inverse Multiplexing for ATM (IMA) Specification Version 1.1, March 1999 is revision of IMA 1.0 and introduces IMA PICS proforma and new version of the IMA MIBs as well as several minor corrections and clarifications to the content of IMA v1.0.

- ATM Forum, af-saa-0124.000, Gateway for H.323 Media Transport Over ATM, July 1999 is an ATM Forum standard and specifies implementation for Real-time Multimedia Over ATM service including telephony, video-conferencing and distance learning based on the exchange of audio, video, data. It describes the access to an ATM network using H.323.
- ATM Forum, af-vtoa-0119.000, Low Speed Circuit Emulation Service (LSCES), May 1999 specifies point-to-point unstructured circuit emulation (CBR traffic) service using AAL1 at user-defined rates over ATM networks. This standard is targeted to support low speed applications (less than 64 kbit/s), but can also support higher rates.
- ATM Forum, af-lane-0112.000, LAN Emulation Over ATM Version 2 - LNNI Specification is an ATM Forum standard and provides some value-added features to LANE, such as multicast support and distributed LANE services.

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.

Third Generation PCS/Cellular - Third generation cellular systems are currently being developed in North America, Europe, and in various Asian countries. 3G systems need to meet the requirement of supporting data transmission at 144 kb/s for the vehicular user, 384 kb/s for the dismounted user and 2Mb/s for the stationary user. The major issues that are being resolved include support for legacy cellular systems and mutually agreed upon cellular standards that permit global roaming. The standards associated with the groups devoted to developing 3G are the following:

- The 3rd Generation Partnership Project (3GPP), which is focused on 3G extensions of the European GSM system and North American TDMA (IS-136). The core of their data architecture is based upon GSM's General Packet Radio System (GPRS) with an interface to the Internet. Also known as the Universal Mobile Telecommunications System (UMTS), the 3GPP standard encompasses GSM and Wideband CDMA (WCDMA), a CDMA standard developed for European applications.
- The 3GPP2, which is focused on the 3G extension of the cdmaOne (North American) CDMA standard. The Third Generation Partnership Project 2 (3GPP2) develops global specifications for network evolution of ANSI/TIA/EIA-41 to 3G and global specifications for the radio transmission technologies (RTTs). 3GPP2 data standards (including cdma2000) are based upon IS-95B. IS-95B is the packet mode version of direct sequence CDMA standard IS-95A. 3GPP2 has taken advantage of existing work in the Internet Engineering Task Force (IETF) on mobile IP to enhance network architecture. 3GPP2 was born out of the International Telecommunication Union's (ITU) International Mobile Telecommunications 'IMT-2000' initiative, covering high speed, broadband, and IP-based mobile systems.

Network Management - Simple Network Management Protocol Version 3 (SNMPv3). The SNMPv3 Management Framework is described in IETF- Draft Standard RFCs 2571-2575. SNMPv3 builds on the mandate SNMPV1 and addresses the deficiencies in SNMPv2 relating to security (e.g. authentication and privacy) and administration (e.g., naming of entities, usernames and key management, and proxy relationships). The following standards are emerging:

- IETF RFC 2575, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).
- IETF RFC 2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).
- IETF RFC 2573, SNMP Applications.
- IETF RFC 2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).
- IETF RFC 2571, An Architecture for Describing SNMP Management Frameworks.

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

- IETF RFC 1657, Border Gateway Protocol version 4 (BGP-4) MIB, defines a set of standard objects for managing this internetwork routing protocol.
- ITEF RFCs 1611, and 1612, Domain Name Service (DNS) MIBs, define a set of standard objects for managing these name server and name resolver services.
- IETF RFCs 1471 through 1474, Point-to-Point Protocol (PPP) MIBs, define a set of standard objects for managing PPP links, security, IP network level, and bridge-level services.
- IETF RFCs 2006 and 2011, Internetwork Protocol (IP) MIBs, define a set of standard objects for managing traditional static IP and emerging mobile IP services.
- IETF RFC 2021, Remote Network Management Monitoring Version 2 (RMON2) MIB, defines a set of standard objects for monitoring protocol communications services across a subnetwork on all seven layers of the OSI model.
- IETF RFC 2012, Transmission Control Protocol (TCP) MIB, defines a set of standard objects for managing a system's TCP services.
- IETF RFC 2013, User Datagram Protocol (UDP) MIB, defines a set of standard objects for managing a system's UDP services.
- IETF RFC 2515, Definitions of Managed Objects for ATM Management, defines a set of standard objects for managing ATM-based interfaces, devices, networks, and services.
- IETF RFC 2605, Directory Server Monitoring MIB, currently defines a set of standard objects for monitoring X.500 directory services and is being updated to add support for LDAP.

ATM Physical Layer - ATM Forum, af-phy-0086.000, Inverse ATM Mux, July 1997, is approved by the ATM Forum and is widely implemented by vendors (Nortel). It is available in products. This standard is desired to send data across non-conventional data rates.

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.

This page was intentionally left blank.

SECTION 4

INFORMATION-MODELING, METADATA, AND INFORMATION-EXCHANGE STANDARDS

4.1 INTRODUCTION

4.1.1 Purpose

This section specifies the minimum information modeling, metadata, and information exchange standards the Army will use to develop or upgrade integrated, interoperable systems that directly or indirectly support the Warfighter.

4.1.2 Scope

This section applies to activity models, data models, object models and data definitions used to define physical databases, and formatted messages used to exchange information among systems.

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. Within the Information System (IS) domain, there are three basic types of models frequently created: activity, data, and object.

Activity Models are representations of mission area processes, composed of one or more related activities. The primary product of each activity model is the definition of a measurable set of products and services required to support the mission area function. An activity model is also referred to as a function or process model.

Data Models, developed from the information requirements documented in the activity model, define entities, their data elements and illustrate the interrelationships among the entities. A data model identifies the logical information requirements and metadata, applicable to persistently stored data, which form a basis for physical database schemata and standard data elements within a relational database.

Object Models define the combined information and process requirements within a domain needed to accomplish a particular capability or set of capabilities; for example, as defined by activity models. Such models form the basis of object-oriented system implementations. They also model system interoperability by combining the metadata for shared data with the allowable interfaces for sharing that data. Such models show associations and dependencies between system interfaces and the essential business rules for exercising those relationships.

In order to provide an authoritative source for DoD data standards, the DoD created the Defense Data Dictionary System (DDDS). The DDDS, managed by the Defense Information Systems Agency (DISA), is a DoD-wide central database that includes standard names and definitions for data entities, and data elements (i.e., attributes). The DDDS server also provides password-

protected access to DoD standard data models. The DDDS is used to collect individual data standards derived from the DoD Data Architecture (DDA) and to document content and format for data elements. A classified version of the DDDS, known as the Secure Intelligence Data Repository (SIDR), has been developed to support standardization of classified data elements and domains. System developers use these repositories as a primary source of data element standards.

Today, battlefield information exchange is accomplished primarily by sending formatted messages. The definition and documentation of these exchange mechanisms are provided by various messaging standards, such as Variable Message Format (VMF), and the U.S. Message Text Format (USMTF). Each message standard provides a means to define message form and functions (i.e., transfer syntax), which includes the definition of the message fields that are contained in each message. The message fields, which are currently defined in the various message standards, are not mutually consistent across message types, nor are they based on any activity or data models, either within a message system or across message systems. Newer techniques provide more direct 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 Section 4.2.1 and 4.2.2. A model-based structure will provide definitions, which will be data element-based and will be compliant with the DoD data element standards established in accordance with the DoD Directive (DoDD) 8320.1, Data Administration, and associated DoD 8320.1 manuals.

Efficient execution of Information Exchange Requirements (IERs) throughout the joint battlespace is key to evolving DoD toward the ultimate goal of seamless information exchange. Dependence on generalized message formats falls short of meeting this goal because the message formats require human intervention to interpret complete meaning from the generalized structure. IERs between systems need to be developed, therefore, which provide clear, functionally relevant information requirements, without regard to any particular physical implementation. IERs could be specified in a standardized interface definition language (IDL) that defines the capabilities of distributed system interfaces along with a common set of data types for interacting with those interfaces. The IDL could be platform and implementation language independent, with a strong separation between the specification of an interface and the implementation of that interface. System developers who use the interface would therefore have no need to know how that interface is implemented. Communication through the IDL would be possible for any system using any programming language that has an IDL mapping defined. This is an objective goal of the Army interoperability program.

4.2 MANDATES

This subsection identifies the mandatory standards, profiles, and practices for information-modeling, metadata, and information-exchange standards.

4.2.1 Activity Modeling

Activity models are used to document/model the activities, processes, and data flows supporting the requirements of process improvement and system development activities. Prior to system development (Milestone B) or major system update, an activity model must be prepared to depict the mission area function to a level of detail sufficient to identify each product or service that

supports the mission. Decomposition will be continued until each of these products and services provides a single measurable final output or result for an identifiable primary system user. The activity model forms the basis for data and/or object model development or refinement. It is validated against the requirements and doctrine, and approved by the operational sponsor. IEEE 1320.1-1998, IEEE Standard for Functional Modeling Language-Syntax and Semantics for IDEF0, is the standard, which describes the IDEF0 modeling language semantics and syntax, and associated rules and techniques, for developing structured graphical representations of a system or enterprise. The doctrinally based activity models will 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 will be used as support criteria for Milestone B and C decisions.

As activity models are developed, security levels will 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 also be possible to classify a previously unclassified model when it is re-used within a different context.

The mandated standard for activity modeling is:

- IEEE 1320.1-1998, IEEE Standard for Functional Modeling Language-Syntax and Semantics for IDEF0.

4.2.2 Data Modeling

Relational data models, and associated activity models which provide context information, are used in software requirements analyses and design activities as a logical basis for physical data exchange and shared data structures that can benefit from a relational schema definition, including message formats and schema for shared databases. Object oriented systems use data models to design relational data structures when there is a requirement to maintain persistent data storage for that system in a relational database. IDEF1X is used to produce a graphical information model, which represents the structure and semantics of information within an environment or system. Developers of new and existing systems maintain traceability between their physical database schema and the DDA and C2CDM (See Section 4.2.4), 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 B or equivalent decision. As data models are developed, security levels and caveats will 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. FIPS Pub 184 is the

standard, which describes the IDEF1X modeling language (semantics and syntax) and associated rules and techniques, for developing a logical model of data. Use of this standard permits the construction of semantic data models, which support the management of data as a resource, the integration of information systems, and the building of relational databases.

System engineering methodology internal to a system is unrestricted. The mandated standards for data modeling are:

- FIPS PUB 184, Integration Definition for Information Modeling (IDEF1X), December 1993, http://www.quam.cl/WEBPAGES/IDEF/IDEF1X/idef1x.html.
- C2 Core Data Model (C2CDM) - C2 Core Data Model (C2CDM) a.k.a C3 Functional View of the DDA Tactical Systems, http://www-datadmn.itsi.disa.mil/ddm.html.
- DoD Defense Data Architecture (DDA), http://www-datadmn.itsi.disa.mil/ddm.html.

4.2.3 Object Modeling

Object-oriented modeling techniques are used in the specification and development of object-oriented systems (as an extension to but not as a replacement for the requirement for activity modeling as defined above) and to model and design the interoperability requirements of distributed components. Object classes encapsulate a data structure (equivalent to one or more related entities) with business rules for employment, information access, and update to that data structure within a particular context. Object modeling techniques employ use case models, sequence diagrams, collaboration diagrams, state transition diagrams, and static object models to define the structure and interaction of object classes within a particular context (i.e., domain). The Unified Modeling Language (UML) is a language for specifying, constructing, visualizing, and documenting such artifacts of a software-intensive system. In an elaborate approach, developers develop models and increasingly add details until the model becomes the actual system being developed. Information may be obtained from the World Wide Web at: http://www.uml.org/. The particular software engineering method used for Object-oriented development is unrestricted. The mandated standard notation for Object model development is:

- The Uniform Modeling Language (UML) version 1.3 of June 1999 as adopted by the Object Management Group (OMG).

4.2.4 DoD Data Model Implementation

The DoD Data Architecture (DDA) is an enterprise view of the data, which provides the standard definition of specific data elements to the developers of all DoD systems. The DDA has replaced the Defense Data Model (DDM) and is now available for use by the DoD Community. The DDA portrays DoD data standards grouped in functional views, which are aligned by Functional Data Administrators rather than subject areas as in the DDM. Tactical systems must incorporate applicable C2 Core Data Model (C2CDM) elements. The C2CDM is a subset of the DDA.

Implementation of the DDA will be interpreted to mean that the DDA will serve as the logical reference model database schema defining the names, representations, and generalized relations of data within DoD systems. System developers comply by using this reference model database schema as a guide to reusable data structures that can form the basis of their own physical database schemas. Developers of new and existing systems will maintain traceability between data structures used in their physical database schemas and the DDA, by registering both the reuse of the data standards in the DDDS and the development/adoption of additional data

structures. Information regarding access to the DDA can be obtained from the DoD Data Administration Web home page at <http://www-datadmn.itsi.disa.mil/>.

Adherence to the DDA for shared or sharable data will aid DoD Agencies in developing interoperability among all information systems. The shared or sharable data of a new or major system upgrade that are to be persistently stored in a relational or object-relational database will be documented within a data model based on the DDA. New information requirements for shared data are submitted by DoD Components and approved by functional data stewards in accordance with DoD Manual 8320.1-M-1, DoD Data Standardization Procedures. This data will be used to extend the DDA, as appropriate. System engineering methodology internal to a system is unrestricted. The following standard for DDA implementation is mandated:

- DoD Manual 8320.1-M-1, DoD Data Standardization Procedures, April 1998.

4.2.5 DoD Data Definitions

The Defense Data Dictionary System (DDDS) is a central database that includes standard data entities, data elements, and provides access to DDA files from the DDDS server. The procedures for preparing and submitting data definitions and data models for standardization are covered in DoD Manual 8320.1-M-1. A classified version of the DDDS, Secure Intelligence Data Repository (SIDR), has been developed to support standardization of classified data elements and domains. System developers will use these repositories as a primary source of data element standards.

The mandated standards for DoD Data Definitions are:

- Defense Data Dictionary (DDDS).
- DoD Manual 8320.1-M-1, DoD Data Standardization Procedures, April 1998.
- Secure Intelligence Data Repository (SIDR).

4.2.6 Information Exchange Standards

4.2.6.1 Information Exchange Standards Applicability

Information Exchange Standards refer to the exchange of information among mission area applications within the same system or among different systems. The scope of information exchange standards is as follows:

1. The exchange of information among applications using shared databases or formatted message structures will 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 will be developed into physical database schemata and standard data elements.
2. The standard data elements will 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.
3. Information exchange between systems using object-oriented interface definitions can be based on object models depicting those interfaces and the functional dependency of those interfaces. With object models, standard data elements are typically associated with the atomic data attributes that represent shared data.
4. XML based information is the widely accepted choice of 21st Century industry data/metadata interchange and is vital to the DOD's interoperability strategy. XML is widely used for metadata definition, management, and exchanges. Integrating XML with middleware technologies, CORBA for example, and

core database technologies will provide the capability to exchange battlefield data among heterogeneous environments. Refer to Section 4.2.8 for XML standard.

Interchange standards help form the DII Common Operating Environment (COE) ensuring the use of system or application formats that can share data. 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.

In distributed databases, other types of data messaging may be used as long as they remain DDDS compliant.

4.2.6.2 Tactical Information-Exchange Standards

The message standards below are joint/combined message standards that provide for the formatted transfer of information between systems. Although it must be recognized that the J-Series Family of TDLs and the USMTF Standards are not model-based and therefore do not meet the goals of standard information exchange, they must be recognized as existing standards. As more systems are developed using logical data models and standard data elements, these message standards must evolve to be data model-based if they are to continue to support joint automated systems.

4.2.6.2.1 Bit-Oriented Formatted Messages

The J-Series Family of TADILs allows information exchange using common data element structures and message formats that support time-critical information. They include Air Operations/Defense Maritime, Fire Support, and Maneuver Operations. These are the primary data links for exchange of bit-oriented information. The family consists of LINK 16, and the Joint Variable Message Format (VMF) and interoperability is achieved through use of J-Series family messages and data elements. The policy and management of this family is described in the Joint Tactical Data Link Management Plan (JTDLMP), dated 6 June 1996. VMF messages use a connectionless application layer as described in MIL-STD-2045-47001B.

New message requirements will use these messages and data elements or use the message construction hierarchy described in the JTDLMP. The mandated standards for information exchange are:

- MIL-STD-6016A, Tactical Digital Information Link (TADIL) J Message Standard, 30 April 1999.
- Variable Message Format (VMF) Technical Interface Design Plan (Test Edition), Reissue 5, 21 January 2002.
- MIL-STD-2045-47001B, Connectionless Data Transfer Application Layer Standard, January 20, 1998.

NOTE: Between publications of the above mandated standards, the TADIL Interface Change Proposals (ICPs) status report lists changes to the standards. Once a TADIL ICP has the status 'approved and awaiting incorporation,' it is approved for implementation. The TADIL ICP Status Report is located at <http://www-tadil.itsi.disa.mil/index.htm>.

STANAG 5516 (Link 16 message) is the NATO equivalent to the corresponding U.S. TADIL J message specification (MIL-STD-6016A). Both message standards are interoperable.

4.2.6.2.2 Character-based Formatted Messages

US Message Text Format (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), 31 March 2000.

4.2.6.2.3 Database to Database Exchange

The following is mandated:

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

4.2.7 Modeling and Simulation Information and Data Exchange Standards

Refer to Appendix G for information standards, both mandated and emerging that is 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).

4.2.8 XML-Based Information Exchange

The eXtensible Markup Language (XML) is a markup language, based on SGML, describing structural information for data (or documents) in tagged format. The tags themselves are not pre-defined, but user-defined that enables flexibility in its usage. In other words, XML models structural information of data independent of tag names. It is independent of any platform and is machine and human readable enabling it to be effectively used for data/metadata interoperability. This section is concerned with exchange involving XML data formats. Examples of such data formats include object meta-data, APIs for database, transaction request-receive, mathematical equations etc. (The XML Documents Interchange is described in section 2.2.2.1.4.1.) The following standard is mandated:

- Extensible Markup Language (XML) 1.0 (Second Edition) W3C Recommendation 6 October 2000'<http://www.w3.org/TR/2000/REC-xml-20001006>.

This second edition is not a new version of XML (first published 10 February 1998); it merely incorporates the changes dictated by the first-edition errata (available at http://www.w3.org/XML/xml-19980210-errata).

NOTE: In order to facilitate interoperability, the DII COE has established an XML Registry for collection, storage and dissemination of XML components (schemas/DTD, XML tags, elements, XSL/XSLT style sheets, etc.)

The DII COE XML Registry is designated to be the single authoritative DOD repository for these XML components. System developers using XML for public interface are required to consult XML Registry before creating new components and reuse exiting XML where practical. The DII COE XML Registry is located at: http://diides.ncr.disa.mil/xmlreg/index.cfm.

4.2.8.1 XML Schema

XML Schemas express shared vocabularies and provide a means for defining the structure, datatype, content and semantics of XML documents. XML Schemas play a major role in extending the capabilities and ease-of-use for XML technology. The following standards are mandated for XML Schema:

- W3C Recommendation, XML Schema Part 1: Structures, 2 May 2001,< http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/>
- W3C Recommendation, XML Schema Part 2: Datatypes, 2 May 2001, <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>

4.3 EMERGING STANDARDS

4.3.1 Activity Modeling

Currently, there are no known emerging Activity Modeling Standards.

4.3.2 Data Modeling

A SHAPE-sponsored initiative, Army Tactical Command and Control Information System (ATCCIS) with current participation by 11 NATO nations, has been evolving a data model to specify core standards for automated battlefield information exchange among national and multinational formations. The model is referred to as the Generic Hub (GH) and it has evolved through four major versions; the last version being labeled GH4. The model focuses on the conduct of both wartime operations and operations other than war at echelons from Brigade to Corps. The generic and modular structure of the model permits ready extension to incorporate additional information exchange requirements that integrate both more detailed data and broader functional areas. GH4 has been submitted to NATO Data Administration Office in October 1999 as a proposed STANAG to serve as the Land C2 Information Exchange Data Model.

4.3.3 Object Modeling

4.3.3.1 Object Metadata Exchange

The XML Metadata Interchange (XMI) standard describes an object related information interchange metamodel. This allows developers using UML object technology tools to exchange UML-based metadata, such as models, in a common format by defining a set of XML DTDs (Document Type Definitions) for the UML constructs. The following standard is emerging:

- XML Metadata Interchange (XMI), Version 1.1, ad/99-10-22, 25 October 1999.
- XML Metadata Interchange (XMI), Version 1.1 - Appendices, ad/99-10-13, 25 October 1999.

4.3.4 DoD Data Model Implementation

Currently, there are no known emerging DoD Data Model Implementation standards.

4.3.5 DoD Data Definitions

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 normalized Data Model 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. e Data Model basis for the data elements will ensure that the information is normalized.

4.3.6 Information Exchange Standards

The emerging standards for information exchange are as follows:

- Distributed Component System Interfaces. Distributed component systems are systems where application functionality and/or data are distributed and interface is accomplished via an RPC API, Common Object Request Broker (CORBA) interface, or similar function call, which matches functionality with the data transfer that applies. For distributed component applications, the evolving standard for interface specification is OMG (ISO/IEC DIS 14750) Information technology -- Open Distributed Processing -- Interface Definition Language.

4.3.7 Modeling and Simulation Information and Data Exchange Standards

Currently, there are no known emerging Modeling and Simulation Information and Data Exchange standards.

4.3.8 XML-based Information Exchange

4.3.8.1 XML Transformation

The Extensible Stylesheet Language (XSL) is being defined in the World Wide Web Consortium. XSL will be used where powerful formatting capabilities are required or for formatting highly structured information such as XML-structured data or XML documents that contain structured data. The new capabilities provided by the XSL proposal include: the formatting of source elements based on ancestry/descendency, position, and uniqueness; the creation of formatting constructs including generated text and graphics; the definition of reusable formatting macros; direction-writing, independent stylesheets; and extensible set of formatting objects. XSL uses XML syntax and combines formatting features from Document Style and Semantics Specification Language (DSSSL). The following standard is emerging:

- Extensible Stylesheet Language (XSL) Version 1.0, W3C Candidate Recommendation, 21 November 2000' <http://www.w3.org/TR/2000/WD-xsl-20000327>.

XML Stylesheet Language Transformations (XSLT) is a language for transforming XML documents into other XML documents and is used as a transformation part of XSL. XSLT has also been designed to be used independently, but is used primarily with XSL. The following standard is emerging:

- XSL Transformations (XSLT) Version 1.0, W3C Recommendations, 16 November 1999 <http://www.w3.org/TR/1999/REC-xslt-19991116>.

4.3.8.2 XML Parsing and Manipulating

The Document Object Model (DOM) is a platform- and language-neutral API that is used to dynamically access and update the content, structure and style of XML-based data (or documents). DOM facilitates a tree-structured representation of XML data enabling the programs to traverse and process it. It also allows for modifications to the documents. The following standard is emerging:

- Document Object Model (DOM) Level 2 Core Specification Version 1.0 W3C Recommendation, 13 November 2000.

The Simple API for XML (SAX) is an event-based interface to XML data (or document) for dynamic access and update. The development of SAX is supported by OASIS, which is a non-profit, international consortium that creates interoperable industry specifications based on public standards. The following standard is emerging:

- SAX, The Simple API for XML, Version 2.0, 28 December 2000.

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 addresses the presentation and dialogue of the Human-Computer Interface. Section 2 addresses the application program interface (API) definitions and protocols. See JTA-Army Section 6.5, and Appendix A of the DoD HCI Style Guide, Security Presentation Guidelines, and other applicable portions of the DoD HCI Style Guide for HCI Security.

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. In keeping with the stated purpose of this section and to provide a standardized HCI within the Army that will result in higher productivity, shorter training time, and reduced

development, operation, and support costs, developers will opt to develop a GUI over a character based interface. 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 (e.g. handheld devices, radios, etc.). These specialized interfaces will be defined by domain-level style guides and further detailed in system-level user interface specifications. The presentation of a consistent interface to the user is paramount to achieving the stated purpose of this section, therefore the mixing of character based and graphical user interface styles is not permitted, except in cases where a specialized interface is a documented requirement.

5.2.1.1 Character-based Interfaces

Systems with an approved requirement for a character-based interface will comply with the character-based interface design criteria contained in the *DoD HCI Style Guide*. The following standard is mandated:

- DoD HCI Style Guide, 30 April 1996.

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).

5.2.1.2 Graphical User Interfaces

Graphical user interfaces for Army automated systems will be based on a commercial user interface style in accordance with Section 5.2.2.1. Hybrid GUIs will 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 ® 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.

Developers will 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 will provide detailed justification and receive approval before proceeding with development.

5.2.1.3 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 will 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.

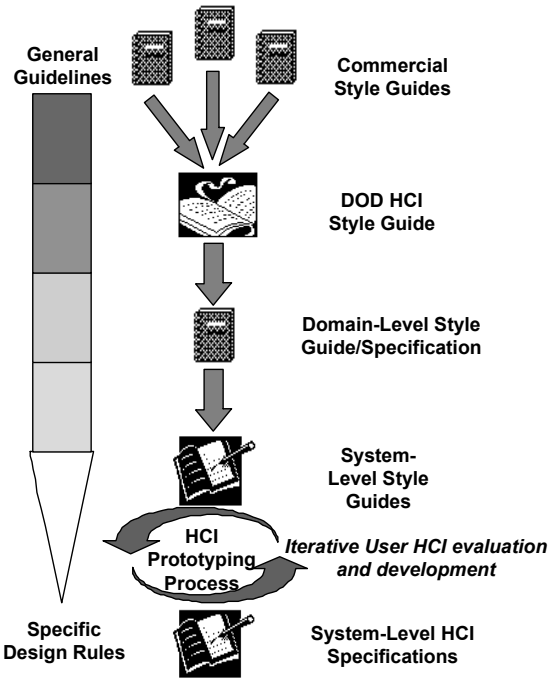


FIGURE 5-1. HIERARCHY OF STYLE GUIDES

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

- MIL-STD-1472E, Department of Defense Design Criteria Standard, Human Engineering, 23 August 1999.
- DoD HCI Style Guide, 30 April 1996.
- Selected commercial GUI style guide.
- Appropriate domain-level style guide.

5.2.2.1 Commercial Style Guides

A commercial GUI style will 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).

5.2.2.1.1 X Window Style Guides

If an X Windows-based environment is selected, the style guide corresponding to the selected version of Motif® is mandated. The following Motif® style guides are mandated:

- Open Group M027: CDE 2.1/Motif® 2.1 - Style Guide and Glossary, ISBN 1-85912-104-7, October 1997.
- Open Group M028: CDE 2.1/Motif® 2.1 - Style Guide Certification Check List, ISBN 1-85912-109-8, October 1997.

- Open Group M029: CDE 2.1/Motif® 2.1 - Style Guide Reference, ISBN 1-85912-114-4, October 1997.

5.2.2.1.2 Windows Style Guide

If a Windows-based environment is selected, the following is mandated:

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

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. 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 will therefore conform to the interface design criteria contained in the *DoD HCI Style Guide.*

The following standard is mandated:

- DoD HCI Style Guide, 30 April 1996.

Although the general principles given in this document applies 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 will 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 will 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 subdomain and/or a system level style guide.

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.

5.2.3 Symbology

The following standard is mandated:

- MIL-STD-2525B, Common Warfighting Symbology, 30 January 1999.

Note that MIL-STD-2525B 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.

5.3 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. The following standard is emerging:

- DoD HCI Style Guide, Version 4.0, 21 December 2000.

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.

Extensive work is currently being done on MIL-STD-2525B and is expected to be reissued as MIL-STD-2525C.

This page was intentionally left blank.

SECTION 6

INFORMATION SECURITY

6.1 INTRODUCTION

6.1.1 Purpose

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

6.1.2 Scope

The standards described in this section are drawn primarily from formally developed national and international standards. In order to be effective, security standards must be integrated into and used with the other information standards in the 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

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 AR 380-19. An appropriate protection profile will be developed for the system as defined by ISO 15408, the Common Criteria, which describes the set of functional security requirements for a Target of Evaluation (TOE). A list of approved protection profiles can be found at the following website:
<http://www.radium.ncsc.mil/tpep/library/protection_profiles/.>

For a more complete list see the following website: http://csrc.nist.gov/cc/pp/pplist.htm
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 will 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 will 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

This subsection identifies the mandatory standards, profiles, and practices for information processing security standards. Each mandated standard or practice is clearly identified on a separate bulleted line and includes a formal reference that can be included within Requests for Proposals (RFPs) or Statements of Work (SOWs). The Evaluation Criteria for Information Technology Security (Common Criteria) represents the outcome of efforts to develop criteria for evaluation of IT security that are widely useful within the international community. It is an alignment and development of a number of existing European, U.S., and Canadian criteria (ITSEC, TCSEC, and CTCPEC) respectively. The Common Criteria is a meta-standard (a standard of standards) as it is essentially a list of selectable security requirements (functional and assurance), plus definitions and requirements for how to document security capabilities and needs (as Security Targets and Protection Profiles respectively).

The following standard is mandated for (1) defining common security requirements across multiple commercial or governmental implementations, by defining a Protection Profile (PP), and for (2) defining evaluation documentation demonstrating that a given system implements PP requirements through its Security Target (ST):

- ISO/IEC 15408:1999, Information Technology - Security Techniques - Evaluation Criteria for Security (parts 1 through 3), 1 December 1999, also documented with the same technical content in Common Criteria (parts 1 through 3), Version 2.1.

It should be noted that the Common Criteria methodology provides general guidance to developers in information security areas where technical standards do not exist or have not been identified by the JTA-A.

6.2.1.1 Application Software Entity

If DMS services are used, the following are mandated:

- MD4002101-1.52, FORTEZZA Application Implementors' Guide, 5 March 1996.
- MD4000501-1.52b, FORTEZZA Cryptologic Interface Programmers' Guide, 20 October 1997.

6.2.1.2 Application Platform Entity

Authentication supports tracing security-relevant events to individual users. The following standard is mandated if the level of trust requires passwords and authentication:

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

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

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

6.2.2 Emerging Standards

6.2.2.1 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.

6.2.2.1.1 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.

6.2.2.2 Authentication Security Standards

IETF 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.

When Remote Dial In Authentication is required, the following standard may be used: IETF RFC-2138, “Remote Authentication Dial In User Service (RADIUS),” April 1997.

6.2.2.3 Generic Security Service Application Program Interface (GSS API)

The Generic Security Service Application Program Interface (GSS-API) (IETF 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 IETF 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 (IETF 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.

6.2.2.4 Security Management Protocols

The following standard for Secure Network Management is emerging:

- IETF RFC-2574, User-Based Security Model, V.3 of the Simple Network Management Protocol (SNMP V.3).

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

This subsection identifies the mandatory standards, profiles, and practices for information transfer security standards. Each mandated standard or practice is clearly identified on a separate bulleted line and includes a formal reference that can be included within Requests for Proposals (RFPs) or Statements of Work (SOWs).

The Evaluation Criteria for Information Technology Security (Common Criteria) represents the outcome of efforts to develop criteria for evaluation of IT security that are widely useful within the international community. It is an alignment and development of a number of existing European, U.S., and Canadian criteria (ITSEC, TCSEC, and CTCPEC) respectively. The

Common Criteria is a meta-standard (a standard of standards) as it is essentially a list of selectable security requirements (functional and assurance), plus definitions and requirements for how to document security capabilities and needs (as Security Targets and Protection Profiles respectively). The following standard is mandated for (1) defining common security requirements across multiple commercial or governmental implementations, by defining a Protection Profile (PP), and for (2) defining evaluation documentation demonstrating that a given system implements PP requirements through its Security Target (ST):

- ISO/IEC 15408:1999, Information Technology - Security Techniques - Evaluation Criteria fort Security (parts 1 through 3), 1 December 1999, also documented with the same technical content in Common Criteria (parts 1 through 3), Version 2.1.

It should be noted that the Common Criteria methodology provides general guidance to developers in information security areas where technical standards do not exist or have not been identified by the JTA-A.

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.

The Message Security Protocol (MSP) Version 4.0 has been revised to accommodate, in part, Allied requirements. All of MSP 4.0 features have been incorporated into ACP-120, Allied Communications Publication 120, and Common Security Protocol. The following messaging security protocol is mandated for DoD message systems that are required to exchange sensitive but unclassified and classified information:

- ACP-120, Allied Communications Publication 120, Common Security Protocol (CSP), Rev A, 7 May 1998.

6.3.1.2 DMS Interface

Host end-system security standards include security algorithms, security protocols, and evaluation criteria. The first-generation FORTEZZA Cryptographic Card is designed to protect information in messaging and other applications.

For systems required to interface with Defense Message System (DMS) for Organizational Messaging, the following standards are mandated:

- FORTEZZA Interface Control Document, Revision P1.5, 22 December 1994.
- FIPS PUB 140-1, Security Requirements for Cryptographic Modules, 11 January 1994.

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.
- MD4000501-1.52b, FORTEZZA Cryptologic Interface Programmers' Guide, 20 October 1997.

6.3.1.3 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 186-1, Digital Signature Standard (DSS) Digital Signature Algorithm (DSA), December 1998.
- FIPS PUB 185, SKIPJACK Algorithm, February 1994, NSA, R21-TECH-044-91, 21 May 1991.
- 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). There are no standards available yet, so these ICDs are mandated in this version of the JTA-Army. 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 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 46-3 Data Encryption Standard, 25 October 1999. The following standard applies:

- FIPS PUB 46-3, Data Encryption Standard, 25 October 1999.

6.3.1.4 Secure World Wide Web (WWW) Transactions

The Secure Sockets Layer (SSL) protocol allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, or message forgery. It is currently the de facto standard used by most browsers and popular e-mail packages that are associated with the browser. RFC 2246, The TLS Protocol Version 1.0, January 1999, is an Internet Engineering Task Force (IETF) Proposed Standard and is expected to supersede SSL as a mandated standard within 2 years. Since Netscape TM is supporting TLS development, it is expected that there will be no further development of the SSL protocol by Netscape TM. The following standard is mandated:

- Secure Sockets Layer (SSL) Protocol Version 3.0, 18 November 1996.

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

RFC 2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999, is an Internet Engineering Task Force (IETF)-Proposed Standard that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, or message forgery. It is based on the SSL 3.0 Protocol Specification as published by Netscape. The differences between this protocol and SSL 3.0 are not dramatic, but they are significant enough that TLS 1.0 and SSL 3.0 do not interoperate (although TLS 1.0 does incorporate a mechanism by which a TLS implementation can back down to SSL 3.0). TLS runs above the transport layer. TLS is expected to supersede SSL as a mandated standard within 2 years. Since Netscape is supporting TLS development, it is expected that there will be no further development of the SSL protocol by Netscape. The following standards are emerging:

- IETF-RFC 2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999.
- IETF-RFC 2487, SMTP Service Extension for Secure SMTP over TLS, January 1999.

6.3.2.3 Networking Security Standards

IETF RFC 2401, "Security Architecture for the Internet Protocol," S. Kent and R. Atkinson, November 1998, describes the security mechanisms for IP and the services that they provide. Each security mechanism is specified in a separate document. RFC-2401 also describes key management requirements for systems implementing those security mechanisms. It is not an overall Security Architecture for the Internet, but focuses on IP-layer security.

This RFC specifies the base architecture for IPsec-compliant systems. It also describes the security services offered by the IPsec protocols and how these services can be employed in the IP environment. IPsec is designed to provide interoperable, high-quality, cryptographically based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper-layer protocols. These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

The Internet Draft RFC 2402, "IP Authentication Header," S. Kent and R. Atkinson, November 1998, describes a mechanism for providing integrity and authentication for IP datagrams. An AH is normally inserted after an IP header and before the other information being authenticated. The AH is a mechanism for providing strong integrity and authentication for IP datagrams. It might also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed.

IETF RFC 2402 "IP Authentication Header," November 1998. The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams, and to provide protection against replays. AH may be applied alone, in combination with the IP Encapsulating Security Payload (ESP), or in a nested fashion through the use of tunnel mode. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. ESP may be used

to provide the same security services, and it also provides a confidentiality (encryption) service. The primary difference between the authentication provided by ESP and AH is the extent of the coverage. Specifically, ESP does not protect any IP header fields.

IETF RFC 2406, "IP Encapsulating Security Payload (ESP)," S. Kent and R. Atkinson, November 1998, discusses a mechanism for providing integrity and confidentiality to IP datagrams. In some circumstances, depending on the encryption algorithm and mode used, it can also provide authentication to IP datagrams. Otherwise, the IP AH may be used in conjunction with ESP to provide authentication. The mechanism works with both IPv4 and IPv6.

IETF RFC 2406 "IP Encapsulating Security Payload (ESP)," November 1998. The ESP header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, in combination with the IP AH [KA97b], or in a nested fashion, e.g., through the use of tunnel mode. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service, and limited traffic flow confidentiality. However, use of confidentiality without integrity/ authentication (either in ESP or separately in AH) may subject traffic to certain forms of active attacks that could undermine the confidentiality service.

IETF RFC 2104, "HMAC: Keyed-Hashing for Message Authentication," February 1997, H. Krawczyk (IBM), M. Bellare (UCSD), R. Canetti (IBM). This document describes HMAC, a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

IETF RFC 1829, "The ESP DES-CBC Transform," P. Karn (Qualcomm), P. Metzger (Piermont), W. Simpson (Daydreamer), August 1995. The Encapsulating Security Payload (ESP) provides confidentiality for IP datagrams by encrypting the payload data to be protected. This specification describes the ESP use of the Cipher Block Chaining (CBC) mode of the U.S. Data Encryption Standard (DES) algorithm (FIPS PUB 46, FIPS PUB 46-1, FIPS PUB 74, FIPS PUB 81). All implementations that claim conformance or compliance with the ESP specification must implement this DES-CBC transform. RFC 2451, "The ESP CBC-Mode Cipher Algorithms," R. Periera and R. Adams, November 1998 and RFC 2405, "The ESP CBC-Mode Cipher Algorithm with Explicit IV," C. Madson and N. Doraswamy, November 1998, are examples of encryption algorithms used for ESP.

The Domain Name System (DNS) has become a critical operational part of the Internet infrastructure, yet it has no strong security mechanisms to ensure data integrity or authentication. IETF RFC-2065, "DNS Security Extensions," D. Eastlake, C. Kaufman, January 1997, describes extensions to the DNS that provide these services to security-aware resolvers or applications through the use of cryptographic digital signatures. These digital signatures are included in secured zones as resource records. Security can still be provided even through non-security-aware DNS servers in many cases. The extensions also provide for the storage of authenticated public-keys in the DNS. This storage of keys can support general public key distribution service as well as DNS security.

IETF RFC 2408, "Internet Security Association and Key Management Protocol (ISAKMP)," Douglas Maughan, Mark Schertler, Mark Schneider, Jeff Turner, 21 February 1998, describes a protocol utilizing security concepts necessary for establishing Security Associations (SAs) and cryptographic keys in an Internet environment. It is expected that the IETF will adopt this protocol as the Internet standard for key and security association management for IPv6 security.

The IETF Draft, "The Resolution of ISAKMP with Oakley," D. Harkins, D. Carrel (Cisco Systems), February 1997, describes a proposal for using the Oakley Key Exchange Protocol in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec Domain of Interpretation (DOI). ISAKMP provides a framework for authentication and key exchange but does not define them. ISAKMP is designed to be key-exchange-independent; that is, it is designed to support many different key exchanges. Oakley describes a series of key exchanges—called "modes"—and details the services provided by each (e.g., perfect forward secrecy for keys, identity protection, and authentication).

IETF RFC 2407, "The Internet IP Security Domain of Interpretation for ISAKMP," D. Piper, November 1998, details the Internet IP Security DOI, which is defined to cover the IP security protocols that use ISAKMP to negotiate their security associations. The ISAKMP defines a framework for security association management and cryptographic key establishment for the Internet. This framework consists of defined exchanges and processing guidelines that occur within a given DOI. The following standards are emerging:

- IETF RFC 2401, Security Architecture for the Internet Protocol, November 1998.
- IETF RFC 2402, IP Authentication Header, November 1998.
- IETF RFC 2406, IP Encapsulating Security Payload (ESP), November 1998.
- IETF RFC 2104, HMAC: Keyed-Hashing for Message Authentication, February 1997.
- IETF RFC 1829, The ESP DES-CBC Transform, August 1995.
- IETF RFC 2451, The ESP CBC-Mode Cipher Algorithms, November 1998.
- IETF RFC 2405, The ESP CBC-Mode Cipher Algorithm with Explicit IV, November 1998.
- IETF RFC 2420, The PPP Triple-DES Encryption Protocol (3DESE) as a complement to FIPS PUB 46-3.
- IETF RFC 2065, DNS Security Extensions, January 1997.
- IETF RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP), 21 February 1998.
- IETF RFC 2407, Internet Draft, The Internet IP Security Domain of Interpretation for ISAKMP, November 1998.

Two IEEE LAN security standards are emerging:

- IEEE 802.10, IEEE Standards for Local and Metropolitan Area Networks (MANs): Interoperable LAN/MAN Security (SILS), 1998, discusses services, protocols, data formats, and interfaces to allow IEEE 802 products to interoperate, and discusses authentication, access control, data integrity, and confidentiality.
- IEEE 802.10a, Standard for Interoperable LAN Security -The Model, Draft January 1989, shows the relationship of SILS to OSI and describes required interfaces.

RFC-2228, File Transfer Protocol, October 1997, defines extensions to the FTP standard (STD9/ RFC 959). These extensions provide strong authentication, integrity, and confidentiality on both

the control and data channels. RFC-2228 also introduces new optional commands, replies, and file transfer encodings. The following standard is emerging:

- IETF RFC 2228, File Transfer Protocol, October 1997.

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

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).

6.3.2.6 Medium-Assurance Public-Key Infrastructure Security Standards

6.3.2.6.1 Background

A public-key infrastructure (PKI) comprises the people, policies, procedures, and computing/ telecommunications resources needed to manage public keys used by information systems. A PKI supports the following security services: authentication, data integrity, non-repudiation, confidentiality, and (optionally) authorization.

A PKI supports “X.509 public-key certificates,” as defined in International Telecommunications Union - Telecommunications (ITU-T) Recommendation X.509. A public-key certificate is a data structure that binds a subject (people, applications programs, machines, etc.) and the subject’s public key. A public-key certificate may contain additional attributes of the subject, such as address, phone number, and authorization (access control) data.

A PKI may support X.509 attribute certificates. An attribute certificate binds a subject and the subject’s authorization data, such as group membership, roles, clearances, privileges, and restrictions. The authorization data does not guarantee access to information resources, as the decision to grant or deny access is made by the application that uses the certificate. Attribute certificates do not contain public keys.

A private key is used to digitally sign data, such as messages, files, and transactions. The corresponding public key is used to verify the signature. A private key can also be used to decrypt data encrypted with the corresponding public key. In the DOD medium-assurance PKI, the public/ private-key pairs used for non-repudiation or digital signature services will be distinct from the pairs used for encryption/decryption services. Public/private-key pairs are also used in algorithms that automatically distribute symmetric, secret keys.

X.509 public-key certificates are signed and issued by a special user called a certification authority (CA). A CA may also revoke certificates. X.509 attribute certificates are signed, issued, and revoked by an attribute certificate issuer.

The DoD medium-assurance PKI is authorized to protect unclassified and certain types of sensitive but unclassified (SBU) information, in accordance with the DoD Class 3 level of information assurance. The DoD medium-assurance PKI may also be used for digital signature services, user authentication, and community of interest separation within certain types of classified networks protected by Type I cryptography. The U.S. DoD X.509 Certificate Policy specifies the permitted uses of a medium-assurance (Class 3) PKI in encrypted and unencrypted networks.

The standards listed below are the ones actually being used in the DoD medium-assurance pilot PKI. The standards are grouped according to the categories defined in the Internet Draft entitled "Internet X.509 Public Key Infrastructure PKIX Roadmap," <draft-ietf-pkix-roadmap-02.txt>, 23 June 1999, plus additional categories not mentioned in the Roadmap. Additional information on PKI policy can be found at <http://www-pki.itsi.disa.mil>.

6.3.2.6.2 Directory and Certificate Profile Standards

One of the critical components of the DOD PKI is the directory services that will support the public key enabled applications and functions across the enterprise. The emerging standard for the directory is as follows:

- ITU-T Rec. X.500 (ISO/IEC 9594-1), Directory Infrastructure.

The following emerging standard provides the certificate profile for the users of the DOD PKI:

- X.509 Certificate Policy for the United States Department of Defense, 13 November 2000, Version 5.2

The certificate profile identified in the X.509 Certificate Policy is based on the more generic open standard defined in, ITU-T Recommendation X.509, Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 as profiled by RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999.

6.3.2.6.3 Operational Protocols and Exchange Formats

Operational protocols deliver certificates and certificate revocation lists (CRLs) to certificate-using systems. The medium-assurance pilot uses RFC 2559, a profile of RFC 1777, Lightweight Directory Access Protocol, version 2, (LDAPv2), as its operational protocol. The following operational protocol is emerging:

- IETF RFC 2559, Internet X.509 Public Key Infrastructure Operational Protocols: LDAPv2, April 1999.

Certificates and CRLs are stored in LDAP servers, which are accessed by certificate-using systems through LDAPv2. RFC 2587 specifies the minimal schema required to support certificates and CRLs in an LDAP server. An emerging standard for LDAP PKI servers is:

- IETF RFC 2587, Internet X.509 Public Key Infrastructure LDAPv2 Schema, June 1999.

Certificates, private keys, and other personal data must be protected when they are moved between computers or removable media, such as smart cards or floppy disks. For secure or authenticated exchange of such personal data, the following standard is emerging:

- RSA Laboratories Public Key Cryptography Standard 12, Personal Information Exchange Syntax Standard, version 1.0 (Draft), 30 April 1997.

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

- FIPS PUB 196, Entity Authentication Using Public Key Cryptography, 18 February 1997.

6.3.2.6.4 Management Protocols

Management protocols support transactions involving management entities, such as CAs, Registration Authorities (RAs), and Local Registration Authorities (LRAs). Typical transactions are user registration, certificate enrollment, and certificate revocation. The following management protocols are emerging:

- IETF RFC 2315, Public Key Cryptography Standard (PKCS) #7, Cryptographic Message Syntax, Version 1.5, March 1998.
- IETF RFC 2314, PKCS #10, Certification Request Syntax, Version 1.5, March 1998.

Although RFC 2315 and 2314 are based upon de facto standards from RSA Laboratories, Inc., the IETF is incorporating them into open, consensus-based standards, such as the Internet draft for "Certificate Management Messages over Cryptographic Message Syntax (CMC)." As the CMC draft matures, it will be considered for adoption as an emerging standard.

6.3.2.6.5 Application Program Interfaces (APIs)

API standards allow programmers to incorporate PKI services into their applications in a manner that supports applications portability. The following standard is emerging:

- RSA Laboratories Public Key Cryptography Standard (PKCS) #11,Cryptographic Token Interface Standard, Version 1.0, 28 April 1995.

6.3.2.6.6 Cryptography

The following standards are emerging:

- RSA Laboratories Public Key Cryptography Standard (PKCS) #1, RSA Cryptography Standard, Version 2.0, 1 October 1998.
- FIPS PUB 140-1, Security Requirements for Cryptographic Modules, 11 January 1994. {DOD X.509 Certificate Policy specifies the FIPS 140-1 security levels required for PKI users, RAs, and CAs}.
- FIPS PUB 46-3, Data Encryption Standard, 25 October 1999.

The following standard is emerging for PKI Class 3 implementations:

- FIPS PUB 180-1, Secure Hash Algorithm, April 1995.

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), which will be cognizant of the germane security policies.

6.4 INFORMATION-MODELING, METADATA, AND INFORMATION-EXCHANGE SECURITY STANDARDS

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

6.4.1 Mandated Standards

None mandated at this time.

6.4.2 Emerging Standards

Emerging standards are as follows:

- ISO/IEC 10165 Series, Information Technology - Open Systems Interconnection- Structure of Management Information - Parts 1- 4, 1993 – 1994.
- DII 10164-9, SC21 N9390, Information Technology - Open Systems Interconnection - Systems Management - Part 9: Objects and Attributes for Access Control (Final Text), ISO/IEC JTC1 SC21/WG4, DII April 1993, target IS March 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, 30 April 1996.

TABLE 6-1 - NOTIONAL MAPPING OF PROTOCOLS AND SECURITY STANDARDS

Layer	Common Protocols	Security Standards/Protocols	
Application	**<u>Interactive Session:</u>** 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)"
Presentation **Session**	**<u>Non-Session:</u>** 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.

6.5.2 Emerging Standards

6.5.2.1 Entity Authentication

The entity authentication emerging standard is as follows:

- 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

The personal authentication emerging standard is as follows:

- 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.

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
AEAGD	Army Enterprise Architecture Guidance Document
AEP	Application Environment Support
AFSRB	Army Fused Safety Review Board
AIS	Automated Information Systems
AITI	Automated Interchange of Technical Information
AJ	Anti-Jam
ALE	Automatic Link Establishment
ALSP	Aggregate Level Simulation Protocol
AMC	Army Materiel Command
AMD	Air and Missile Defense
AMSO	Army Modeling and Simulation Office
ANSI	American National Standards Institute
API	Application Programming Interface
AR	Army Regulation
ARIADNE	Alliance of Remote Instructional Authoring and Distribution Networks for Europe
AS	Aerospace Standard
ASAS	All Source Analysis System
ASB	Army Science Board
ASD	Assistant Secretary of Defense
ASIC	Application-Specific Integrated Circuit
ATA	Army Technical Architecture
ATCCIS	Army Tactical Command and Control Information System
ATD	Advanced Technology Demonstration
ATM	Air Traffic Management
ATM	Asynchronous Transfer Mode
AVS	Aviation Systems
BCI	Battlefield Combat Identification
BER	Bit Error Rate
BGP	Border Gateway Protocol
BM	Ballistic Missile
BMD	Ballistic Missile Defense
BOOTP	Bootstrap Protocol
bps	bits per second
BRI	Basic Rate Interface
BUFR	Binary Universal Format for Representation
CAA	Civil Aviation Authorities
CAD	Computer-Aided Design
CADRG	Compressed ARC Digitized Raster Graphics
CALS	Continuous Acquisition & Life-Cycle Support

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
CD-ROM	Compact Disc-Read Only Memory
CFS	Center for Standards
CGI	Computer Generated Imagery
CGM	Computer Graphics Metafile
CHAP	Challenge Handshake Authentication Protocol
CI	Combat Identification
CIB	Controlled Image Base
CIDE	Communication Information Data Exchange
CINC	Commander-in-Chief
CIPSO	Common Internet Protocol Security Options
CIO/G-6	Chief Information Officer/G-6
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CLI	Call Level Interface
CMB	Configuration Management Board
CMI	Computer Managed Instruction
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CMMS	Conceptual Models of the Mission Space
CNR	Combat Net Radio
CNS	Communications, Navigation, and Surveillance
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
CS-S	Combat Support and Sustainment
CTRS	Conventional Terrestrial Reference System
C2	Command and Control
C2CDM	C2 Core Data Model
C3I	Command, Control, Communications, and Intelligence
C3S	Command, Control, and Communications Systems
C4I	Command, Control, Communications, Computers, and Intelligence
DAA	Designated Approving Authority
DAMA	Demand Assigned Multiple Access
DAP	Directory Access Protocol
DAT	Digital Audio Tape
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
DDA	Defense Data Model
DDNS	Dynamic Domain Name System
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
DIF	Data Interchange Format
DII	Defense Information Infrastructure
DIS	Distributed Interactive Simulation
DISA	Defense Information Systems Agency
DISAC	DISA Circular
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
DNI	Detailed Network Interface
DNS	Domain Name System
DoD	Department of Defense
DoDD	Department of Defense Directive
DPPDB	Digital Point Positioning Data Base
DSN	Defense Switched Network
DSS	Digital Signature Standard
DSSS	Direct Sequence Spread Spectrum
DTD	Document Type Definition
DTE	Data Terminal Equipment
DTED	Digital Terrain Elevation Data
DTOP	Digital Topographic Data
EC	Electronic Commerce
EDI	Electronic Data Interchange
EDISMC	EDI Standards Management Committee (
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
FED	Federation Execution Details
FESMCC	Federal EDI Standards Management Coordinating Committee
FIPS	Federal Information Processing Standards
FOA	Field Operating Agency
FOM	Federation Object Model
FoS	Family Of Systems
FPS	Frames Per Second
FTP	File Transfer Protocol
FTR	Federal Telecommunications Recommendation
FWG	Functional Working Group
GCCS	Global Command and Control System

GH	Generic Hub
GIF	Graphics Interchange Format
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
GVS	Ground Vehicle Systems
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
Hz	Hertz
IAB	Internet Architecture Board
IAW	In Accordance With
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Chip
ICCCM	Inter Client Communications Convention Manual
ICD	Interface Control Document
ICHIPB	Imagery Chip, Version B
ICMP	Internet Control Message Protocol
ICOM	Inputs, Controls, Outputs, and Mechanisms
ICP	Interface Change Proposal
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
IER	Information Exchange Requirements
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IF	Intermediate Frequency
IFF	Identification of Friends and Foes
IGES	Initial Graphics Exchange Specification
IGMP	Internet Group Management Protocol
IIOP	Internet Inter-ORB Protocol
ILMI	Integrated Local Management Interface
IMETS	Integrated Meteorological System
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPv6	IP Next Generation/Version 6
IS	Information System

ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	ISDN Security Program
ITU	International Telecommunications Union
I/EW	Intelligence and Electronic Warfare
I&A	Identification & Authentication
I&RTS	Integration & Runtime Specification
JCS	Joint Chiefs of Staff
JFIF	JPEG File Interchange Format
JIEO	Joint Interoperability and Engineering Organization
JPEG	Joint Picture Expert Group
JSA	Joint System Architecture
JTA	Joint Technical Architecture
JTA-Army	Joint Technical Architecture - Army
JTF	Joint Task Force
JTDLMP	Joint Tactical Data Link Management Plan
JTIDS	Joint Tactical Information Distribution System
JVM	Java Virtual Machine
kbits	kilobits
kbits/s	kilobits per second
kbps	kilobits per second
kb/s	kilobits per second
KEA	Key Exchange Algorithm
kHz	kilo-Hertz
KMP	Key Management Protocol
LAN	Local Area Network
LANE	Local Area Network Emulation
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol
LD-CELP	Low-Delay Code Excited Linear Prediction
LDR	Low Data Rate
LLC	Logical Link Control
LOM	Learning Object Metadata
LOS	Line-of-Sight
LPI	Low Probability of Intercept
LTSA	Learning Technology Systems Architecture
LWD	Littoral Warfare Data
M&S	Modeling & Simulation
MAC	Media Access Control
MACOM	Major Army Command
MAU	Medium-Access Unit
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
MHP	Mobile Host Protocol
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
MIME	Multipurpose Internet Mail Extensions
MISSI	Multilevel Information System Security Initiative
MLPP	Multi-Level Precedence and Preemption
MMP	MISSI Management Protocol
MOSPF	Multicast OSPF
MPEG	Motion Pictures Expert Group
MPOA	MultiProtocol Over ATM
MP@ML	Main Profile @ Main Level
MS	Missile Systems
MSMP	Modeling and Simulation Master Plan
MSP	Message Security Protocol
MUS	Munition Systems
NCSC	National Computer Security Center (see NSA)
NDI	Nondevelopmental Item
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
NTM	National Technical Means
NTP	Network Time Protocol
NV	Night Vision
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
OE	Operating Environment
OMA	Object Management Architecture
OMCSR	Object Model Content Standards Repository
OMG	Object Management Group
OML	Object Model Library
OMT	Object Model Template
OOA	Object Oriented Analysis
OOM	Object-oriented methods
OOP	Object Oriented Programming
OOT	Object Oriented Technology
OOTW	Operations-Other-Than-War
ORD	Operational Requirements Document
OS	Operating Systems
OSD	Office of the Secretary of Defense

OSI	Open Systems Interconnection
OSJTF	Open Systems Joint Task Force
OSPF	Open Shortest Path First
OTAR	Over-The-Air-Rekeying
PAPI	Personal and Performance Information
PC	Personal Computer
PCI	Peripheral Component Interface
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
PKI	Public Key Infrastructure
PM	Program/Product Manager
PMC	PCI Mezzanine Card
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
PSE51	Minimal Realtime System Profile
PSE52	Realtime Controller System Profile
PSE53	Dedicated Realtime System Profile
PSE54	Multi-Purpose Realtime System Profile
PTTI	Precise Time and Time Interval
QCIF	Quarter Common Intermediate Format
RADIUS	Remote Authentication Dial In User Service
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
RSTA	Reconnaissance and Target Acquisition
RTI	Runtime Infrastructure
RTP	Real Time Protocol
RT/NRT	Real-Time/Near-Real-Time

SA	Situational Awareness
SA	Systems Architecture
SAE	Society of Automotive Engineers
SAMP	Security Association Management Protocol
SATCOM	Satellite Communications
SBU	Sensitive But Unclassified
SCQL	Structured Card Query Language
SCSI	Small Computer Systems Interface
SDE	Support Data Extensions
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
SIDR	Secure Intelligence Data Repository
SIF	Standard Simulator Data Base (SSDB) Interchange Format
SILS	Standard for Interoperable LAN Security
SIPE	Soldier Integrated Protective Ensemble
SISO	Simulation Interoperability Standards Organization
SLP	Sensor Link Protocol
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
SOM	Simulation Object Model
SONET	Synchronous Optical Network
SP3	Security Protocol at Layer 3
SQL	Structured Query Language
SQL/MM	SQL Multimedia
SS	Soldier Systems
SSDB	Standard Simulator Data Base
SSL	Secure Sockets Layer (of HTTP)
STAMIS	Standard Army Management Information System
STANAG	Standardization Agreement
STD	Standard
STEP	Standards for the Exchange of Product Model Data
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
UML	Unified Modeling Language
UN	United Nations
UNI	User-Network Interface
URL	Uniform Resource Locator
USACE	Army Corps of Engineers
USD A&T	Under Secretary of Defense for Acquisition and Technology
USIGS	United States Imagery and Geospatial Information System
USMC	United States Marine Corps
USMTF	United States Message Text Format
USNO	U.S. Naval Observatory
USS	Uniform Symbology Specification
UTC	Coordinated Universal Time
UVMap	Urban Vector Map
VHDL	VHSIC Hardware Description Language
VHF	Very High Frequency
VISP	Video Imagery Standards Profile
VITD	Vector Interim Terrain Data
VLAN	Virtual LANs
VMap	Vector Map
VMap AD	VMap Aeronautical Data
VMF	Variable Message Format
VPF	Vector Product Format
VRML	Virtual Reality Modeling Language
VTC	Video Teleconferencing
WFMC	Workflow Management Coalition
WGS-84	World Geodetic System 84
WMO	World Meteorological Organization
WRM	Workflow Reference Model
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
XML	eXtensible Markup Language

XOS	Extended Operating System
XTI	X/Open Transport Interface
Y2K	Year 2000
3GL	Third Generation Language
4GL	Fourth Generation Languages

APPENDIX B - LIST OF REFERENCES

Appendix B contains all documents referenced in the JTA-Army, including the mandated and the emerging standards.

B.1 MILITARY

B.1.1 DoD References

TABLE B-1 - DOD REFERENCES

#	Reference	Title and Date	Section
1	DoD 5000.2-R	Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, 15 March 1996	2.2.2.1.1.1 Programming Languages
2	DoD-5015.2-STD	Design Criteria Standard for Electronic Records Management Software Applications, November 1997 (Sec 2.2.1-2.2.1.1 only)	2.3.1.1.2 Electronic Records Management
3	DoD 5200.28-STD	The Department of Defense Trusted Computer System Evaluation Criteria, December 1985	6.1.3 Background, 6.2.1.1 Application Software Entity, 6.2.1.2 Application Platform Entity, 6.3.1.6 Evaluation Criteria Security Standards
4	DoD 8320.1-M-1	Department of Defense Data Element Standardization Procedures, January 1993	4.2.5 DoD Data Definitions
5	DoD AIMS 97-900	Performance/Design And Qualification Requirements Mode 4 Input/Output Data, 18 March 1998	F.3.6.1.1 Mandates
6	DoD AIMS 97-1000	Performance/Design and Qualification Requirements Technical Standard For The ATCRBS/IFF/MARK XII Electronic Identification System and Military Mode S, 18 March 1998	F.3.6.1.1 Mandates
7	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 March 1994 (ITU-T X.741).	6.4.2 Emerging Standards
8	DoD Manual 8320.1-M-1	DoD Data Standardization Procedures, April 1998	4.2.4 DoD Data Model Implementation, 4.2.5 DoD Data Definitions
9	DoDD 5000.59	DoD Modeling and Simulation Management, dated January 4, 1994	G.1.2 Background
10	ICD-GPS-060	Precise Time and Time Interval (PTTI) Interface, Rev A	3.3.1 Emerging Host Standards
11	ICD-GPS-200C	NAVSTAR GPS Space Segment/Navigation User Interfaces, 16 October 1997	3.2.1.5 Global Position System (GPS) Standards
12	ICD-GPS-222A	NAVSTAR GPS UE Auxiliary Output Chip Interface (U), 26 April 1996	3.2.1.5 Global Position System (GPS) Standards

#	Reference	Title and Date	Section
13	ICD-GPS-225A	NAVSTAR GPS Selective Availability/Anti-Spoofing Host Application Equipment Design Requirements with the Precise Positioning Service Security Module (U), 12 March 1998	3.2.1.5 Global Position System (GPS) Standards
14	ICP TJ93-096	Space Track Message, Ballistic Missile Defense Organization, Interface Change Proposal (ICP), 26 September 1997	F.MS.2.4.2 Emerging Standards
15	Joint Pub 1-02	Department of Defense Dictionary of Military and Associated Terms, 23 March 1994	F.1 DOMAIN OVERVIEW
16	J-STD-008 (Draft)	PCS standard for CDMA	3.3.2 Emerging Network Standards
17	MD4000501-1.52b	FORTEZZA Cryptologic Interface Programmer's Guide, 20 October 1997	6.2.1.1 Application Software Entity, 6.3.1.2 DMS Interface
18	MD4002101-1.52	FORTEZZA Application Implementor's Guide, 5 March 1996	6.2.1.1 Application Software Entity, 6.3.1.2 DMS Interface
19	MIL-HDBK-1300A	National Imagery Transmission Format Standard (NITFS)	2.2.2.1.4.4 Still Imagery Data Interchange, E.2.3.1.1.1 Secondary Imagery Dissemination Standards
20	MIL-HDBK-28001	CALS SGML, 30 June 1995	D.2.2.1.1 Document Interchange
21	MIL-PRF-28000A w/AMD 1	Digital Representation for Communications of Product Data: IGES Application Subsets and IGES Application Protocols, 14 December 1992	D.2.2.1.3 Product Data Interchange
22	MIL-PRF-28000B	Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols (Draft), 1 July 1999	D.2.2.2.1 Product Data Interchange
23	MIL-PRF-28001C	Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text. (CALS SGML), 2 May 1997	D.2.2.1.1 Document Interchange
24	MIL-PRF-28002C	Performance Specification, Requirements for Raster Graphics Representation in Binary Format, 30 September 1997	D.2.2.1.2 Graphics Data Interchange
25	MIL-STD-882C	System Safety Program Requirements, 19 January 1993	F.MUS. 3.6.1 Mandates
26	MIL-STD-1389D	Design Requirements for Standard Electronic Module (SME), 30 March 1989	F.AVS.3.5.2 Emerging Standards
27	MIL-STD-1472E	Department of Defense Design Criteria Standard, Human Engineering, 23 August 1999	5.2.2 Style Guides
28	MIL-STD-1472F	Human Engineering Design Criteria for Military Systems, Equipment and Facilities	5.3 EMERGING STANDARDS
29	MIL-STD-1477C	Symbols for Army Air Defense System Displays (Metric).	F.MS.2.5.1.1 Symbology
30	MIL-STD-1553B	Interface Standard for Digital Time Division Command/Response Multiplex Data Bus, 21 September 1978, with Notice of Change 1, 12 February 1980, Notice of Change 2, 8 September 1986, Notice of Change 3, 31 January 1993, and Notice of Change 4, 15 January 1996	F.AVS.3.5.1.1 Serial Buses
31	MIL-STD-1553B	Standard for Medium Speed System Network Bus, 21 September 1978, with Notice of Change 1, 12	F.GVS.3.5.1.1 Serial Buses

#	Reference	Title and Date	Section
		February 1980; Notice of Change 2, 8 September 1986; Notice of Change 3, 31 January 1993; and Notice of Change 4, 15 January 1996	
32	MIL-STD-1582D	EHF LDR Uplinks and Downlinks, 30 September 1996; with Notice of Change 1, 14 February 1997, and Notice of Change 2, 17 February 1999	E.2.3.1.3.1.3.1 Low Data Rate (LDR)
33	MIL-STD-1760C	Department of Defense Interface Standard for Aircraft/Store Electrical Interconnection System, 20 March 1997	F.AVS.3.5.2.1 Serial Buses
34	MIL-STD-1773	Fiber Optics Mechanization of an Aircraft Internal Time Division Command/Response Multiplex Data Bus, 20 May 1988 with Notice of Change 1, 2 October 1989	F.AVS.3.5.1 Mandates
35	MIL-STD-1787C	Aircraft Display Symbology, 5 January 01	F.AVS.2.5.1.1 Symbology
36	MIL-STD-1821	Standard Simulator Data Base (SSDB) Interchange Format (SIF) Design Standard, 17 June 1993, with Change of Notice 1, 17 April 1994, and Notice of Change 2, 17 February 1996	G.2.4.1.3 Standard Simulator Database Interchange format (SIF)
37	MIL-STD-1840C	Automated Interchange of Technical Information (AITI), 26 June 1997	D.2.2.1.1 Document Interchange, D.2.2.1.3 Product Data Interchange
38	MIL-STD-188-110B	Interoperability and Performance Standards for Data Modems, 27 April 2000	E.2.3.1.3.2.1.3 Data Modems
39	MIL-STD-188-136A	EHF MDR Uplinks and Downlinks, 8 June 1998	E.2.3.1.3.1.3.2 Medium Data Rate (MDR)
40	MIL-STD-188-141B	Interoperability and Performance Standards for Medium and High Frequency Radio Systems, 1 March 1999	E.2.3.1.3.2.1.1 HF and Automatic Link Establishment (ALE)
41	MIL-STD-188-145	Digital Line-of-Sight (LOS) Microwave Radio Equipment, 7 May 1987; with Notice of Change 1, 28 July 1992	E.2.3.1.3.2.5 Super High Frequency (SHF)
42	MIL-STD-188-148A	Interoperability Standard Anti-Jam (AJ) Communication HF Band (2-30 MHz), 18 March 1992	E.2.3.1.3.2.1.2 Anti-jamming Capability
43	MIL-STD-188-161D	Interoperability and Performance Standards for Digital Facsimile Equipment, 10 January 1995	3.2.1.3.2 Digital Facsimile Standard
44	MIL-STD-188-164	Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995, with Notice of Change 1, 9 September 1998	E.2.3.1.3.1.2.1 Earth Terminals
45	MIL-STD-188-165	Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995, with Notice of Change 1, 9 September 1998	E.2.3.1.3.1.2.2 Phase Shift Keying (PSK) Modems
46	MIL-STD-188-181B	Interoperability Standard for Single Access 5-kHz and 25-kHz UHF Satellite Communications Channels, 20 March 1999	E.2.3.1.3.1.1.1 5-kilo-Hertz (kHz) and 25-kHz Serv
47	MIL-STD-188-182A	Interoperability Standard for 5 kHz UHF DAMA Terminal Waveform, 31 March 1997, with Notice of Change 1, 9 September 1998; and Notice of Change 2, 22 January 1999	E.2.3.1.3.1.1.2 5-kHz Demand Assigned Multiple Access (DAMA) Service

#	Reference	Title and Date	Section
48	MIL-STD-188-183A	Interoperability Standard for 25 kHz UHF/TDMA/DAMA Terminal Waveform, 20 March 1998; with Notice of Change 1, 9 September 1998	E.2.3.1.3.1.1.3 25-kHz Time Division Multiple Access (TDMA)/Demand Assigned Multiple Access (DAMA) Service
49	MIL-STD-188-184	Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993, with Notice of Change 1, 9 September 1998	E.2.3.1.3.1.1.4 Data Control Waveform
50	MIL-STD-188-185	DoD Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System, 29 May 1996, with Notice of Change 1, 1 December 1997; and Notice of Change 2, 9 September 1998	E.2.3.1.3.1.1.5 Demand Assigned Multiple Access (DAMA) Control System
51	MIL-STD-188-196	Bi-Level Image Compression for the National Imagery Transmission Format Standard, 18 June 1993	2.2.2.1.4.4 Still Imagery Data Interchange
52	MIL-STD-188-198A	Joint Photographic Experts Group (JPEG) Image Compression for the National Imagery Transmission Format Standard, 15 December 1993	2.2.2.1.4.4 Still Imagery Data Interchange
53	MIL-STD-188-199	Vector Quantization Decompression for the National Imagery Transmission Format Standard, 27 June 1994	2.2.2.1.4.4 Still Imagery Data Interchange
54	MIL-STD-188-220B	Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, January 20, 1998	3.2.2.2.3 Combat Net Radio (CNR) Networking
55	MIL-STD-188-242	Tactical Single Channel (VHF) Radio Equipment, 20 June 1985	E.2.3.1.3.2.2 Very High Frequency (VHF)
56	MIL-STD-188-243	Tactical Single Channel (UHF) Radio Communications, 15 March 1989	E.2.3.1.3.2.3 Ultra High Frequency (UHF)
57	MIL-STD-2045-18500	Message Handling System (MHS) Message Security Protocol (MSP) Profile, Parts 1-5, October 1993	6.3.1.1 Security Protocols
58	MIL-STD-2045-44500	National Imagery Transmission Format Standard (NITFS) Tactical Communications Protocol 2 (TACO2), 18 June 1993, with Notice of Change 1, 29 July 1994; and Notice of Change 2, 27 June 1996	E.2.3.1.1.1 Secondary Imagery Dissemination Standards
59	MIL-STD-2045-47001B	Connectionless Data Transfer Application Layer Standard, January 20, 1998	4.2.6.2.1 Bit-Oriented Formatted Messages
60	MIL-STD-2301A	Computer Graphics Metafile (CGM) Implementation Standard for the National Imagery Transmission Format Standard, 18 June 1993, with Notice of Change 1, 12 October 1994, profiled by ANSI/ISO 8632:1992 Computer Graphics Metafile (CGM) for the Storage and Transfer of Picture Description Information	2.2.2.1.4.4 Still Imagery Data Interchange
61	MIL-STD-2401	Department of Defense World Geodetic System (WGS 84), 11 January 1994	2.2.2.1.4.3 Geospatial Data Interchange
62	MIL-STD-2407	Interface Standard for Vector Product Format (VPF), 28 June 1996	2.2.2.1.4.3 Geospatial Data Interchange
63	MIL-STD-2411	Raster Product Format, 6 October 1994; with Notice of Change, Notice 1, 17 January 1995	2.2.2.1.4.3 Geospatial Data Interchange
64	MIL-STD-2500B	National Imagery Transmission Format (Version 2.1) for the National Imagery Transmission	2.2.2.1.4.4 Still Imagery Data Interchange

#	Reference	Title and Date	Section
		Format Standard, 22 August 1997 with Notice 1, 2 October 1998	
65	MIL-STD-2525B	Common Warfighting Symbology, 30 January 1999	4.2.7 Modeling and Simulation Information and Data Exchange Standards , 5.2.3 Symbology, F.MS.2.5.1.1 Symbology
66	MIL-STD-2549	Department of Defense Interface Standard, Configuration Management Data Interface, 30 June 1997	D.2.2.1.6 Configuration Management Data Interchange
67	MIL-STD-6016A	Tactical Digital Information Link (TADIL) J Message Standard, 30 April 1999	4.2.6.2.1 Bit-Oriented Formatted Messages, F.MS.2.4.2 Emerging Stand
68	MIL-STD-6016	TADIL-J/Link-16	F.MS.2.4.2 Emerging Standards
69	MIL-STD-6040	United States Message Text Format (USMTF), 31 March 2000	4.2.6.2.2 Character-based Formatted Messages
70	NCSC-TG-005, Version 1	Trusted Network Interpretation, July 1987	6.3.1.5 Transport Mechanisms, 6.3.1.6 Evaluation Criteria Security Standards
71	NCSC-TG-021, Version 1	Trusted Database Management System Interpretation, April 1991	6.2.1.1 Application Software Entity
72	SSDCB79S4000	JTIDS System Segment Specification (Class 2 Terminal) (SECRET document).	E.2.3.1.3.2.6 Joint Tactical Information Distribution System (JTIDS)/Multifunctional Information Distribution System (MIDS) Transmission Media, Link 16 Transmission Standards
73	STANAG 4175, Edition 1	Technical Characteristics of the Multifunctional Information Distribution System (MIDS), 29 August 1992	E.2.3.1.3.2.4 Link 16 Transmission Standards
74	STANAG 4246, Edition 2	HAVE QUICK UHF Secure and Jam-resistant Communications Equipment, 17 June 1987; with Amendment 3, August 1991	E.2.3.1.3.2.4 Anti-jamming Capability
75	STANAG 4404, Edition 1	Safety Requirements and Guidelines for Munition Systems Related Safety Critical Systems, Draft, 29 August 1997	F.MUS. 3.6.2 Emerging Standards
76	STANAG 4452, Edition 1	Safety Assessment of Munition-Related Computing Systems, Draft, 1 June 1997	F.MUS. 3.6.2 Emerging Standards
77	STANAG 4579	Battlefield Target Identification Devices, 22 March 2000	F.3.6.2 Emerging Standards
78	STANAG 5516, Edition 1	Tactical Data Exchange - LINK 16, Ratified 2 15 January 1997	4.2.6.2.1 Bit-Oriented Formatted Messages
79	X.509	Certificate Policy for the United States Department of Defense, 13 November 2000, Version 5.2	6.3.2.6.2 Directory and Certificate Profile Standards
80	(No Number)	ASD Memorandum Development, Procurement, and Employment of DoD Global Position System User Equipment, 30 April 1992	3.2.1.5 Global Position System (GPS) Standards
81	(No Number)	Defense Data Dictionary System (DDDS)	4.2.5 DoD Data Definitions, 4.2.6.2.4 Database to Database Exchange
82	(No Number)	Defense Information Infrastructure Common Operating Environment, Integration and Runtime	2.2 Mandates

#	Reference	Title and Date	Section
		Specification (I&RTS), Version 4.1, 3 October 2000.	
83	(No Number)	Department of Defense (DoD) Modeling and Simulation Master Plan (MSMP),	G.1.2 Background
84	(No Number)	Department of Defense Joint Technical Architecture (JTA), Version 1.0, 22 August 1996	1.1.4 Background
85	(No Number)	Department of Defense Joint Technical Architecture (JTA), Version 2.0, 30 November 1998	1.1.4 Background
86	(No Number)	Department of Defense Joint Technical Architecture (JTA), Version 3.0, 15 November 1999	1.1.4 Background
87	(No Number)	DoD ATM Addressing Plan, 17 April 1998	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
88	(No Number)	DoD Defense Data Model (DDA), http://www-datadmn.itsi.disa.mil/ddm.html	4.2.2 Data Modeling
89	(No Number)	DoD HCI Style Guide, 30 April 1996	5.2.1.1 Character-based Interfaces, 5.2.2 Style Guides, 5.2.2.3 Domain-level Style Guides, 6.5.1.1 Security Banners and Screen Labels
90	(No Number)	DoD HCI Style Guide, Version 4.0, 21 December 2000	5.3 Emerging Standards
91	(No Number)	DoD HLA Mandated Baseline Definition, September 10, 1996	G.2.2.1.4 High Level Architecture (HLA) for Simulations
92	(No Number)	DoD Memorandum, Subject: Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement, 13 October 1993	1.1.4 Background
93	(No Number)	DoD Memorandum, Subject: Specifications and Standards -- A New Way of Doing Business, 29 June 1994	1.1.4 Background
94	(No Number)	DoD Technical Reference Model Version 1.0, 5 November 1999	2.1.3 Background, 2.2.1 Application Software Entity
95	(No Number)	DoD/IC/USIGS Video Imagery Standards Profile (VISP), Version 1.4, 8 June 1999	2.2.2.1.4.7.1 Video Imagery and Audio
96	(No Number)	Federation Execution Details Data Interchange Format Version 1.3, February 1998	G.2.4.1.1 Federation Execution Details Data Interchange Format (FED DIF)
97	(No Number)	FORTEZZA Crypto Card Interface Control Document (ICD), Version P1.5, 22 December 1994	6.3.1.3 MISSI Cryptographic Algorithms
98	(No Number)	FORTEZZA Interface Control Document, Revision P1.5, 22 December 1994	6.3.1.2 DMS Interface
99	(No Number)	FORTEZZA Plus Crypto Card Interface Control Document (ICD), Release 3.0, 01 June 1995, FOUO	6.3.1.3 MISSI Cryptographic Algorithms
100	(No Number)	Joint Range Extension Application Protocol (JREAP) for Encapsulation into Joint Technical	F.MS.2.3.2.1 Joint Range Extension (JRE) Application

#	Reference	Title and Date	Section
		Architecture (JTA) Compliant Protocols, Joint Range Extension Application Protocol Working Group, Version 1.0, 19 July 2000	Protocol (JREAP)
101	(No Number)	High Level Architecture (HLA) Management Plan, Version 1.6, 17 July 1995	G.1.2 Background
102	(No Number)	Joint Software System Safety Handbook, Draft, 30 September 1997	F.MUS. 3.6.2 Emerging Standards
103	(No Number)	Secure Intelligence Data Repository (SIDR)	4.2.5 DoD Data Definitions
104	(No Number)	Synthetic Environment Data Representation and Interchange Specification (SEDRIS).	G.2.4.2.1 SEDRIS
105	(No Number)	The Under Secretary of Defense for Acquisition and Technology, DoD High Level Architecture (HLA) for Simulations, 10 September 1996	G.1.2 Background
106	(No Number)	Time Division Multiple Access (TDMA) Protocol, Control, and Signaling Standard for Soldier Radios	F.SS.2.3.2 Emerging Standards
107	(No Number)	User Interface Specifications for the Defense Information Infrastructure (DII), Version 4.0, October 1999	E.2.5.1.1 Domain-level Style Guides
108	(No Number)	VMF Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 5, 21 January 2002	4.2.6.2.1 Bit-Oriented Formatted Messages

B.1.2 Army References

TABLE B-2 - ARMY REFERENCES

#	Reference	Title and Date	Section
1	ACCS-A3-407-008E	Interface Specification for the Army Data Distribution System (ADDS) Interface, 3 May 1998	3.2.2.2.6 X.25
2	AR 5-11	Management of Army Models and Simulations, dated 10 July 1997	G.1.2 Background
3	AR 380-19	Army Regulation, Information System Security, 1 August 1990	6.1.3 Background
4	FM 101-5-1	Operational Terms and Graphics	4.2.5 Modeling and Simulation Information and Data Exchange Standards, 5.2.1.3 Symbology
5	(No Number)	Achieving Interoperability Among Army Systems, 4 October 2001	1.1.3 Scope
6	(No Number)	Army Enterprise Architecture Guidance Document (AEAGD), The Department of the Army, 23 December 1998	1.1.2 Architectures Defined
7	(No Number)	Army Model and Simulation Master Plan, dated October 1997	G.1.2 Background
8	(No Number)	Army Technical Architecture Implementation, Mark-On-The-Wall Message, Department of the Army, 6 June 1996	1.1.3 Scope
9	(No Number)	Aviation Human-Computer Interface Style Guide, Version 2.2, May 1998	F.AVS.2.5.1.2 Aviation Systems Subdomain Style Guide
10	(No Number)	Command and Control (C2) Core Data Model (C2CDM) - C2 Core Data Model (C2CDM) a.k.a C3 Functional View of the DDA Tactical Systems, http://www-datadmn.itsi.disa.mil/ddm.html	4.2.2 Data Modeling

#	Reference	Title and Date	Section
11	(No Number)	Department of the Army C4I Technical Architecture, Version 3.1, 31 March 1995	1.1.4 Background
12	(No Number)	Department of the Army Technical Architecture, Version 4.0, 30 January 1996	1.1.4 Background
13	(No Number)	Department of the Army Technical Architecture, Version 4.5, 12 November 1996	1.1.4 Background
14	(No Number)	HQDA Memorandum, Subject: 1994 Army Science Board (ASB) Study: Technical Architecture for Army C4I, 28 July 1994	1.2 TECHNICAL ARCHITECTURE
15	(No Number)	Human Computer Interface Style Guide for the Ground Vehicle Domain, Draft Version 0.3, 12 December 1996	F.GVS.2.5.2 Emerging Standards
16	(No Number)	Joint Technical Architecture – Army (JTA-Army), Department of the Army, Version 5.0, 11 September 1997	1.1.4 Background
17	(No Number)	Joint Technical Architecture – Army (JTA-Army), Department of the Army, Version 5.5, 23 December 1998	1.1.4 Background
18	(No Number)	Map Data Loading Standard (MDLS), Revision 1.0; February 26, 1998	F.2.3.1.1 Map Data Loading
19	(No Number)	Soldier/Aircrew Machine Interface Style Guide	F.AVS.2.5.2.1 Aviation Systems Subdomain Style Guide
20	(No Number)	The Army Enterprise Implementation Plan, 8 August 1994	1.1.4 Background
21	(No Number)	The Army Enterprise Strategy, the Vision, 20 July 1993	1.1.4 Background
22	(No Number)	U.S. Army Weapon Systems Application Program Interface (API) GuideBook: Volume II - API Specification Style Guide, February 2, 1999	F.2.4.1 Mandates
23	(No Number)	U.S. Army Weapon Systems Human-Computer Interface (WSHCI) Style Guide, Version 3.0, December 1999	F.2.5.1.1 Domain-level Style Guide
24	(No Number)	Weapon System Mapping Services (WSMS) Application Programmer's Interface (API), WSTAWG Doc# WSTA-AS-03-01, January 28, 2001	F.2.2.1.2 Mapping Services F.2.2.2.2 Mapping Services

B.1.3 Other Government Agency References

TABLE B-3 - OTHER GOVERNMENT AGENCY REFERENCES

#	Reference	Title and Date	Section
1	ACP-120	Allied Communications Publication 120, Common Security Protocol (CSP), Rev A, 7 May 1998	6.3.1.1 Security Protocols
2	ACP 123	Common Messaging Strategy and Procedures, November 1994	3.2.1.1.1.1 Electronic Mail
3	ACP 123, U.S. Supplement No. 1	Common Messaging Strategy and Procedures, November 1995	3.2.1.1.1.1 Electronic Mail
4	BMD-P-SD-92-000002-A	Ballistic Missile Defense (BMD) Navigation Standard, Ballistic Missile Defense Organization, 23 June 1993	F.MS.2.2.2.1 Navigation Standard
5	DCID 1/16	Director of Central Intelligence Directive (DCID)	6.6 SECURITY RELATED

#	Reference	Title and Date	Section
			DOCUMENTS
6	DIS 9075-4,	Database Language SQL, Part 4: Persistent Stored Modules (SQL/PSM).	2.3.2 Service Area Standards
7	DISAC 310-225-1	Defense Switched Network (DSN) User Services Guide, DISA Circular, 2 April 1998	3.2.2.2.4 Integrated Services Digital Network (ISDN)
8	DOT FAA 1010.51A	US National Aviation Standard for the Mark X (SIF) Air Traffic Control Radar Beacon system (ATCRBS) Characteristics, 8 March 1971	F.3.6.1.1 Mandates
9	FIPS PUB 4-1	Representation For Calendar Date And Ordinal Date For Information Interchange, 27 January 1988	4.2.6 Date Data Format
10	FIPS PUB 10-4	Countries, Dependencies, Areas of Special Sovereignty, and Their Principal Administrative Divisions, April 1995	2.2.2.1.4.3 Geospatial Data Interchange
11	FIPS PUB 46-2	Data Encryption Standard, December 1993	6.6 SECURITY RELATED DOCUMENTS
12	FIPS PUB 46-3	Data Encryption Standard, Draft, 25 October 1999	6.3.1.3 Cryptographic Algorithms 6.3.2.6.6 Cryptography
13	FIPS PUB 112	Password Usage, National Institute of Standards and Technology (NIST), 30 May 1985	6.2.1.2 Application Platform Entity
14	FIPS PUB 128-2	Computer Graphics Metafile (CGM), 17 April 1996	2.2.2.1.4.2 Graphics Data Interchange
15	FIPS PUB 140-1	Security Requirements for Cryptographic Modules, 11 January 1994	6.3.1.2 DMS Interface, 6.3.2.6.6 Cryptography
16	FIPS PUB 161-2	Electronic Data Interchange (EDI), 22 May 1996,	D.2.2.1.4 Electronic Data Interchange
17	FIPS Pub 172-1	VHSIC Hardware Description Language (VHDL), 27 January 1995	D.2.2.1.3 Product Data Interchange
18	FIPS Pub 173	Spatial Data Transfer Standard (SDTS), 10 June 1994	D.2.2.1.5 Geospatial Data Interchange
19	FIPS PUB 180-1	Secure Hash Algorithm, NIST, April 1995	6.3.1.3 MISSI Cryptographic Algorithms
20	FIPS PUB 184	Integration Definition For Information Modeling (IDEF1X), December 1993	4.2.2 Data Modeling
21	FIPS PUB 185	SKIPJACK algorithm, February 1994, NSA, R21-TECH-044-91, 21 May 1991	6.3.1.3 MISSI Cryptographic Algorithms
22	FIPS PUB 186-1	Digital Signature Standard (DSS) Digital Signature Algorithm (DSA), December 1998	6.3.1.3 MISSI Cryptographic Algorithms
23	FIPS PUB 189	Information Technology - Portable Operating System Interface (POSIX®) - Recommendations (Section 12) and Implementation Guidance (Section 13), 1994	2.2.2.1.7 Operating System Services
24	FIPS PUB 196	Entity Authentication Using Public Key Cryptography, 18 February 1997	6.3.1.1 Security Protocols, 6.3.2.6.3 Operational Protocols and Exchange Formats
25	ICD-SLP-200	Interface Control Document (ICD) Title: Sensor Link Protocol, September 14, 1998	F.SS.2.3.2 Emerging Standards
26	NIMAL 805-1A	NIMA GGI&S List of Products and Services, January 1997	2.2.2.1.4.3 Geospatial Data Interchange
27	NISTIR 90-4250	Secure Data Network System (SDNS) program	6.3.1.1 Security Protocols
28	N-0106-97	Bandwidth Compression Standards and Guidelines Document, 25 August 1998 with Change Notice 1,	F.AVS.2.2.1.1 Still Imagery Data Interchange

#	Reference	Title and Date	Section
		01 March 2001	
29	Presidential Executive Order 12906	Presidential Executive Order 12906, April 1994	D.2.2.1.5 Geospatial Data Interchange
30	R21-Tech-23-94	NSA-developed Type II Key Exchange Algorithm (KEA), NSA, 12 July 1994	6.3.1.3 MISSI Cryptographic Algorithms
31	SDN.301, revision 1.5	Secure Data Network System (SDNS) Security Protocol 3 (SP3), 1989	6.3.1.1 Security Protocols
32	SDN.703	MISSI Management Protocol (MMP), Revision 1.0, 7 June 1996	6.2.2.5 Security Management Protocols
33	SDN.903, revision 3.2	Secure Data Network System (SDNS) Key Management Protocol (KMP), 1 August 1989	6.3.1.1 Security Protocols
34	STDI-0002	Airborne Support Data Extension (ASDE), Version 1.0, 13 January 1999; as documented in Section 8 of The Compendium of Controlled Extensions (CE) for the National Imagery Transmission Format (NITF) Version 2.0, 4 March 1999	E.2.2.1.1 Still-Imagery Data Interchange
35	STDI-0002	HISTOA Extension, 25 August 1998; as documented in Section 15 of The Compendium of Controlled Extensions (CE) for the National Imagery Transmission Format (NITF) Version 2.0, 4 March 1999	E.2.2.1.1 Still-Imagery Data Interchange
36	STDI-0002	ICHIPB Support Data Extension for the National Imagery Transmission Format, Version 1.0, 16 November 1998; as documented in Section 5 of The Compendium of Controlled Extensions (CE) for the National Imagery Transmission Format (NITF) Version 2.0, 4 March 1999	E.2.2.1.1 Still-Imagery Data Interchange
37	STDI-0002	National Imagery Transmission Format Profile for Image Access Extensions (PIAE), Version 3.0, 25 September 1997; as documented in Section 6 of The Compendium of Controlled Extensions (CE) for the National Imagery Transmission Format (NITF) Version 2.0, 4 March 1999	E.2.2.1.1 Still-Imagery Data Interchange
38	(No Number)	Battlefield Combat Identification System (BCIS) Specification #A3191205A	F.3.6.2.2 Emerging Standards
39	(No Number)	Defense Information Infrastructure (DII) Common Operating Environment (COE), Integration and Runtime Specification (I&RTS), Version 4.1, 3 October 2000.	2.2 MANDATES, 2.2.1 Application Software Entity
40	(No Number)	National Security Agency (NSA)-developed Type II confidentiality algorithm (SKIPJACK).	6.3.1.3 MISSI Cryptographic Algorithms
41	(No Number)	Weapon System Mapping Services (WSMS) Application Programmer's Interface (API), Revision 1.1, April 30, 1998	F.2.2.2.2 Mapping Services

B.2 COMMERCIAL REFERENCES

TABLE B-4 - COMMERCIAL REFERENCES

#	Reference	Title and Date	Section
1	AICC AGR 006	Computer Managed Instruction (CMI), V1.1, Feb	2.3.1.1 Environment

#	Reference	Title and Date	Section
		1, 1997 (see <http://www.aicc.org/pages/down-docs-index.htm>)	Management
2	ANSI/AIAA R-004-1992	Recommended Practice for Atmospheric and Space Flight Vehicle Coordinate Systems	F.MS.2.2.2.1 Geospatial Data Interchange
3	ANSI ASC X12	Electronic Data Interchange (ASC X12S 97-372 is latest edition).	D.2.2.1.4 Electronic Data Interchange
4	ANSI ASC X12.58	Security Structures, 1997	D.2.6 Information Systems Security Standards
5	ANSI HL7	Health Level Seven Standard Version 2.4 Application Protocol for Electronic Data Exchange in Healthcare Environments, October 6, 2000	D.2.2.1.4 Electronic Data Interchange
6	ANSI NCITS 256,	Non-Contact Information Technology Standard 256, 1999	D.2.2.2.1 Product Data Interchange
7	ANSI/NCITS 288	Information Technology - Fibre Channel - Generic Services - 2 (FC-GS-2), 1999	F.AVS.3.5.1.1 Serial Buses
8	ANSI/NCITS 321	Fibre Channel Switched Fabric and Switched Control Requirements (FC-SW), 1998	F.AVS.3.5.1.1 Serial Buses
9	ANSI/NCITS 332	Fibre Channel Arbitrated Loop (FC-AL-2), 1999	F.AVS.3.5.1.1 Serial Buses
10	ANSI S4.40-1992/AES3-1992	AES (Audio Engineering Society) Recommended Practice for Digital Audio Engineering - Serial transmission format for two-channel linearly represented digital audio data, 1992 (reaffirmed and amended 1997).	2.2.2.1.4.7.1.1 Audio for Video Imagery
11	ANSI T1.101	Telecommunications - Synchronization Interface Standard, 1999	3.2.3.3 Synchronous Optical Network (SONET) Transmission Facilities
12	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	3.2.3.3 Synchronous Optical Network (SONET) Transmission Facilities
13	ANSI T1.107	Digital Hierarchy - Formats Specifications, 1995	3.2.3.3 Synchronous Optical Network (SONET) Transmission Facilities
14	ANSI T1.117	Digital Hierarchy - Optical Interface Specifications (SONET) (Single Mode - Short Reach), 1991 (R1997)	3.2.3.3 Synchronous Optical Network (SONET) Transmission Facilities
15	ANSI T1.204	OAM&P - Lower Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements, 1997	3.2.5.2 Telecommunications
16	ANSI T1.208	OAM&P - Upper Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements, 1997	3.2.5.2 Telecommunications
17	ANSI T1.403.01	ISDN Primary Rate - Customer Installation Metallic Interfaces (Layer 1 Specification), 1999	3.2.2.2.4 Integrated Services Digital Network (ISDN)
18	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	3.2.2.2.4 Integrated Services Digital Network (ISDN)
19	ANSI T1.602	Data Link Signaling Specification for Application at the User Network Interface, 1996	3.2.2.2.4 Integrated Services Digital Network (ISDN)
20	ANSI T1.605	ISDN Basic Access Interface for S and T Reference Points - Layer 1 Specification, 1991	3.2.2.2.4 Integrated Services Digital Network (ISDN)

#	Reference	Title and Date	Section
		(R1999)	
21	ANSI T1.607	Digital Subscriber Signaling System No. 1 (DSS1) - Layer 3 Signaling Specification for Circuit Switched Bearer Service, 1998	3.2.2.2.4 Integrated Services Digital Network (ISDN)
22	ANSI T1.610	DSS1 - Generic Procedures for the Control of ISDN Supplementary Services, 1998	3.2.2.2.4 Integrated Services Digital Network (ISDN)
23	ANSI T1.619	Multi-Level Precedence and Preemption (MLPP) Service, ISDN Supplementary Service Description, 1992	3.2.2.2.4 Integrated Services Digital Network (ISDN)
24	ANSI T1.619a	Supplement, 1994	3.2.2.2.4 Integrated Services Digital Network (ISDN)
25	ANSI T1.630	ATM Adaptation Layer for Constant Bit Rate (CBR) Services Functional and Specification, (i.e. AAL1), 1993	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
26	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).	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
27	ANSI X3.30	Information Technology - Representation of Date for Information Interchange, 1997	4.2.6 Date Data Format
28	ANSI X3.100	Interface between DTE and DCE for Operation with PSDN, or between Two DTEs, by Dedicated Circuit, 1989	3.2.2.2.6 X.25
29	ANSI X3.100a	Supplement to ANSI X3.100, 1991	3.2.2.2.6 X.25
30	ANSI X3.131	Information Systems - Small Computer Systems Interface - 2 (SCSI-2), 1994	F.GVS.3.5.1.2.3 Peripheral Bus, F.MUS.3.5.1.1.2 Peripheral Buses
31	ANSI X3.229	Fibre Distributed Data Interface (FDDI) - Station Management (SMT).	3.2.2.2.7 Fiber Distributed Data Interface (FDDI)
32	ANSI X3.230-1994	Information Technology – Fibre Channel – Physical and Signaling Interface (FC-PH).	E.3.1.2.1.1 Fibre Channel F.AVS.3.5.1.1 Serial Buses
33	ANSI X3.230-1994/AM 1-1996	Information Technology – Fibre Channel – Physical and Signaling Interface (FC-PH) – Amendment 1	E.3.1.2.1.1 Fibre Channel
34	ANSI/NCITS X3.230-1994	Amendment 1:1996, Amendment 1 to ANSI/NCITS X3.230-1994 Fibre Channel Physical and Signaling Interface (FC-PH), 1996	F.AVS.3.5.1.1 Serial Buses
35	ANSI/NCITS X3.230-1994	Amendment 2:1999, Amendment 2 to ANSI/NCITS X3.230-1994, Fibre Channel Physical and Signaling Interface (FC-PH), 1999	F.AVS.3.5.1.1 Serial Buses
36	ANSI X3.272	Fibre Channel Arbitrated Loop (FC-AL), 1996	F.AVS.3.5.1.1 Serial Buses
37	ANSI X3.289	Fiber Channel Fabric Generic (FC-FG), 1996	F.AVS.3.5.1.1 Serial Buses
38	ANSI X3.297	Information Technology - Fibre Channel Physical and Signaling Interface 2 (FC-PH-2), 1997	F.AVS.3.5.1.1 Serial Buses
39	ANSI X3.303	Fibre Channel Physical and Signaling Interface 3 (FC-PH-3) 1998.	F.AVS.3.5.1.1 Serial Buses
40	ANSI/AIAA R-004-1992	Recommended Practice for Atmospheric and Space Flight Vehicle Coordinate Systems	F.MS.2.2.2.2 Geospatial Data Interchange
41	ANSI/AIM BC-1-1995	Uniform Symbology Specification - Code 39, 16 August 1995CXc	D.2.2.1.3 Product Data Interchange
42	ANSI/AIM BC-8	Uniform Symbology Specification PDF 417, July 1994.	D.2.2.1.3 Product Data Interchange
43	ANSI/ISO/IEC 8632	Information Technology - Computer Graphics - Metafile for the Storage and Transfer of Picture	D.2.2.1.2 Graphics Data Interchange

#	Reference	Title and Date	Section
		Description Information [part 1:1992 Functional Specifications (with amendment 1:1994 Rules for Profiles and with amendment 2:1995 Application Structuring Extensions)] and [part 3:1992 Binary Coding (with amendment 1:1994 Rules for Profiles and with amendment 2:1995 Application Structuring Extensions)] as profiled by MIL-PRF-28003A dated 15 November 1991 with Amendment 1 dated 14 August 1992, Performance Specification, Digital Representation for Communications of Illustration Data: CGM Application Profile.	
44	ANSI/ISO/IEC 9636-1,2,3,4,5,6:1991 (R1997)	Information Technology Computer Graphics Interfacing (CGI) Techniques for Dialogue with Graphics Devices	2.2.2.1.5 Graphic Services
45	ANSI/ISO/IEC 14882-1998	Information Technology - Programming Languages - C++	2.2.2.1.1.1 Programming Languages
46	ANSI/PC-D-350D	Printed Board Description in Digital Form, July 1, 1992	D.2.2.1.3 Product Data Interchange
47	ARINC 429	Mark 33 Digital Information Transfer System (DITS), 1999	F.AVS.3.5.1.1 Serial Buses
48	ARINC 629	Multi-Transmitter Data Bus, 1999	F.AVS.3.5.1.1 Serial Buses
49	ANSI/SMPTE 12M-1998	Time and Control Code for Video and Audio Tape for 525 Line/60 Field Television Systems	2.2.2.1.4.7.1 Video Imagery
50	ANSI/SMPTE 259M-1997	Television - 10 bit 4:2:2 Component (Serial Digital Interface)	2.2.2.1.4.7.1 Video Imagery
51	ANSI/SMPTE 292M-1998	Television - Bit-Serial Digital Interface for High-Definition Television Systems	2.2.2.1.4.7.1 Video Imagery
52	ANSI/SMPTE 293M-1996	Television - 720 x 483 Active Line at 59.94-Hz Progressive Scan Production - Digital Representation	2.2.2.1.4.7.1 Video Imagery
53	ANSI/SMPTE 296M-1997	Television - 1270 x 720 Scanning, Analog and Digital Representation and Analog Interface	2.2.2.1.4.7.1 Video Imagery
54	ANSI/SMPTE 274M-1995	Television - 1920 x 1080 Scanning and Interface	2.2.2.1.4.7.1 Video Imagery
55	ANSI/SMPTE 309M-1998	Transmission of Date and Time Zone Information in Binary Groups of Time and Control Code	2.2.2.1.4.7.1 Video Imagery
56	ANSI/US PRO-100-1996	Initial Graphics Exchange Specification (IGES), V5.3, 23 September 1996	D.2.2.1.3 Product Data Interchange
57	ANSI/VITA 1	VME64 Specification, 1994	F.AVS.3.5.1.2.1 Backplane Buses, F.GVS.3.5.1.2.1 Backplane Buses
58	ANSI/VITA 1.1	VME64 Extensions, 1997	F.AVS.3.5.1.2.1 Backplane Buses, F.GVS.3.5.1.2.1 Backplane Buses
59	ATM Forum, af-ilmi-0065.000	Integrated Local Management Interface (ILMI) Specification, Version 4.0, September 1996	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
60	ATM Forum, af-lane-0050.000	LAN Emulation Over ATM Version 1.0 Addendum, December 1995	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
61	ATM Forum, af-lane-0057.000	LANE Servers Management Spec v1.0, March 1996	3.2.2.2.5 Asynchronous Transfer Mode (ATM)

#	Reference	Title and Date	Section
62	ATM Forum, af-lane-0084.000	LANE Emulation Over ATM Version 2.0 LUNI Specification, July 1997	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
63	ATM Forum, af-lane-0093.000	LAN Emulation Client Management Specification Version 2.0, October 1998	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
64	ATM Forum, af-lane-0112.000	LAN Emulation Over ATM Version 2 - LNNI Specification	3.3.2 Emerging Network Standards
65	ATM Forum, af-mpoa-0087.000	MultiProtocol Over ATM (MPOA) Version 1.0, July 1997	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
66	ATM Forum, af-mpoa-0114.000	Multi-Protocol Over ATM Version 1.1, May 1999	3.3.2 Emerging Network Standards
67	ATM Forum, af-phy-0015.000	ATM Physical Medium Dependent Interface Specification for 155 Mb/s over Twisted Pair Cable, September 1994	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
68	ATM Forum, af-phy-0016.000	DS1 Physical Layer Specification, September 1994	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
69	ATM Forum, af-phy-0040.000	Physical Interface Specification for 25.6 Mb/s over Twisted Pair Cable, November 1995	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
70	ATM Forum, af-phy-0043.000	A Cell-based Transmission Convergence Sublayer for Clear Channel Interfaces, November 1995	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
71	ATM Forum, af-phy-0046.000,	622.08 Mb/s Physical Layer Specification, January 1996	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
72	ATM Forum, af-phy-0054.000	DS3 Physical Layer Interface Specification, January 1996	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
73	ATM Forum, af-phy-0064.000	E-1 Physical Layer Interface Specification, September 1996	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
74	ATM Forum, af-phy-0086.000	Inverse Multiplexing for ATM (IMA) Specification Version 1.0, July 1997	3.2.2.2.5 Asynchronous Transfer Mode (ATM) 3.3.2 Emerging Network Standards
75	ATM Forum af-phy-0086.001	Inverse Multiplexing for ATM (IMA) Specification Version 1.1, March 1999	3.3.2 Emerging Network Standards
76	ATM Forum, af-pnni-0055.000	Private Network to Network Interface (PNNI) Specification, Version 1.0, March 1996	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
77	ATM Forum, af-pnni-0066.000	PNNI Specification V1.0 Addendum (Soft PVC MIB), September 1996	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
78	ATM Forum, af-saa-0124.000	Gateway for H.323 Media Transport Over ATM, July 1999	3.3.2 Emerging Network Standards
79	ATM Forum, af-sig-0061.000	ATM UNI Signaling Specification, Version 4.0, July 1996	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
80	ATM Forum, af-sig-0076.000	Addendum to UNI Signaling V4.0 for ABR Aparameter Negotiation, January 1997	3.3.2 Emerging Network Standards
81	ATM Forum, af-tm-0056.000	Traffic Management Specification, Version 4.0, April 1996	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
82	ATM Forum, af-tm-0077.000	Traffic Management ABR Addendum	3.3.2 Emerging Network Standards
83	ATM Forum, af-tm-0121.000	Traffic Management Specification Version 4.1, March 1999	3.3.2 Emerging Network Standards
84	ATM Forum, af-uni-0010.002	ATM UNI Specification V 3.1, (Section 2.1, 2.4, and Section 4: ILMI for UNI 3.1), September 1994	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
85	ATM Forum, af-vtoa-0078.000	Circuit Emulation Service Interoperability Specification 2.0, January 1997	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
86	ATM Forum, af-	ATM Trunking Using AAL2 for Narrowband	3.3.2 Emerging Network

#	Reference	Title and Date	Section
	vtoa-0113.000	Services	Standards
89	ATM Forum, af-vtoa-0119.000	Low Speed Circuit Emulation Service (LSCES), May 1999	3.3.2 Emerging Network Standards
90	ATSC Doc. A/52	Digital Audio Compression Standard (AC-3), 20 December 1995	2.3.2.1.1.5 Motion-Imagery Data Interchange
91	ATSC Document A/53	ATSC Digital Television Standard, 16 September 1995	F.3.5.2 Emerging Standards
92	BTD-Security-01	ATM Security Specification, April 1997	6.3.2.3 Networking Security Standards
93	C310	DCE 1.1: Time Services Specification, X/Open CAE Specification, November 1994	2.2.2.2.4.1 Remote Procedure Computing
94	C311	DCE 1.1: Authentication and Security Services, Open Group CAE Specification, August 1997	2.2.2.2.4.1 Remote Procedure Computing
95	C320	Motif Toolkit API, Open Group Technical Standard, ISBN 1-85912-024-5, April 1995	2.2.2.1.2 User Interface Services
96	C323	Common Desktop Environment (CDE) Version 1.0, X/Open CAE Specification, April 1995	F.MUS.2.2 Information Processing Standards
97	C323	XCDE Services and Applications, Open Group Technical Standard, ISBN 1-85912-074-1, April 1995	2.2.2.1.2 User Interface Services
98	C324	XCDE Definitions and Infrastructure, Open Group Technical Standard, ISBN 1-85912-070-9, April 1995	2.2.2.1.2 User Interface Services
99	C507	Window Management (X11R5): X Window System Protocol, X/Open CAE Specification, April 1995	2.2.2.1.2 User Interface Services
100	C508	Window Management (X11R5): Xlib - C Language Binding, X/Open CAE Specification, April 1995	2.2.2.1.2 User Interface Services
101	C509	Window Management (X11R5): X Toolkit Intrinsics, X/Open CAE Specification, April 1995	2.2.2.1.2 User Interface Services
102	C510	Window Management (X11R5): File Formats and Application Conventions, Open Group Technical Standard, ISBN 1-85912-090-3, May 1995	2.2.2.1.2 User Interface Services
103	C705	DCE 1.1: Directory Services, Open Group CAE Specification, August 1997	2.2.2.2.4.1 Remote Procedure Computing
104	C706	DCE 1.1: Remote Procedure Call, Open Group CAE Specification, August 1997	2.2.2.2.4.1 Remote Procedure Computing
105	C903	X Window System (X11R6): Protocol, Open Group Technical Standard, July 1999	2.2.2.1.2 User Interface Services
106	C904	X Window System (X11R6): C-Language Library (Xlib), Open Group Technical Standard, December 1999	2.2.2.1.2 User Interface Services
107	C905	X Window System (X11R6): Toolkit, Open Group Technical Standard, December 1999	2.2.2.1.2 User Interface Services
108	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)	6.3.3 Summary of Standards
110	draft-ietf-cat-gssv2-05.txt	GSS-API, Version 2, J. Linn, 20 February 1996	6.2.2.4 Generic Security Service Application Program Interface (GSS API)

#	Reference	Title and Date	Section
111	draft-ietf-cat-idup-gss-04.txt	Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)," C. Adams, 18 February 1996	6.2.2.4 Generic Security Service Application Program Interface (GSS API)
112	draft-ietf-pkix-ipki-part1-08.txt	IETF Internet-Draft: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, June 16,1998	6.3.2.6.1 Background, 6.3.2.6.2 Certificate Profiles
113	EIA 170	Electrical Performance Standards - Monochrome Television Studio Facilities, November 1957	F.SS.3.5.1 Mandates
114	EIA 232F	Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, October 1997	3.2.2.2.2 Point to Point Standards, 3.2.2.2.6 X.25
115	EIA-422B	Electrical characteristics of balanced voltage digital interface circuits, 1994	3.2.1.2 Video Teleconferencing (VTC) Standards
116	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	3.2.2.2.2 Point to Point Standards, 3.2.2.2.6 X.25, 3.2.1.2 Video Teleconferencing (VTC) Standards
117	EIA 530A	High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment, December 1998, Including Alternate 26-Position Connector, 1992	3.2.2.2.2 Point to Point Standards, 3.2.2.2.6 X.25
118	ESD-TR-86-278	Guidelines for Designing User Interface Software, Smith and Mosier 1986	5.2.1.2 Character-based Interfaces
119	FM 92-X	Ext. GRIB WMO No. 306, Manual on Codes, International Codes, Volume I.2 (Annex II to WMO Technical Regulations) Parts B and C	2.2.2.1.4.9 Atmospheric and Oceanographic Data Interchange
120	FM 94-X	Ext. BUFR WMO No. 306, Manual on Codes, International Codes, Volume I.2 (Annex II to WMO Technical Regulations) Parts B and C.	2.2.2.1.4.9 Atmospheric and Oceanographic Data Interchange
121	FTR 1080A-1998	Appendix A, Video Teleconferencing Profile, October 1998	3.2.1.2 Video Teleconferencing (VTC) Standards
122	IEEE 610.12	IEEE Standard Glossary of Software Engineering Terminology, 1990	1.1.2 Architectures Defined
123	IEEE 802.10	IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS), IEEE, 1992	6.3.2.3 Networking Security Standards
124	IEEE 802.10a	Standard for Interoperable LAN Security-The Model, IEEE, Draft January 1989	6.3.2.3 Networking Security Standards
125	IEEE 802.10b	Standard for Interoperable LAN Security-Part B: Secure Data Exchange, IEEE, 1992	6.3.2.3 Networking Security Standards
126	IEEE 802.10c/D6	Standard for Interoperable LAN Security-Part C: Key Management, IEEE, Draft 6 issued 1994	6.2.2.5 Security Management Protocols
127	IEEE 802.11a-1999	Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, High Speed PHY in the GHz Band	3.3.2 Emerging Network Standards
128	IEEE 802.11b - 1999	Supplement to Information Technology - Telecommunications and Information Exchange Between Systems - Local and metropolitan area networks - Specifications requirements - Part 11:	3.2.2.2.6 Wireless LAN

#	Reference	Title and Date	Section
		Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band.	
129	IEEE 802.1Q	Multi-switch Ethernet VLANs	3.3.2 Emerging Network Standards
130	IEEE 802.2	Local and Metropolitan Area Networks, Part 2: Logical Link Control, 1994	3.2.2.2.7 Fiber Distributed Data Interface (FDDI)
131	IEEE 802.3-1998	Edition Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications (includes IEEE 802.3z-1998)	3.2.2.2.1 Ethernet
132	IEEE 802.3ab-1999	Supplement to IEEE 802.3-1998: Physical Layer Parameters and Specifications for 1000 Mb/s Operation over 4-Pair of Category 5 Balanced Copper Cabling, Type 1000BASE-T	3.2.2.2.1 Ethernet
133	IEEE 802.3u-1995	Supplement to ISO/IEC 8802-3:1993, Local and Metropolitan Area Networks: Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100 Mbps Operation, Type 100BASE-T (Clauses 21-30)	3.2.2.2.1 Ethernet
134	IEEE 1003.2d	POSIX® - Part 2: Shell and Utilities - Amendment: Batch Environment, 1994	2.2.2.1.7 Operating System Services
135	IEEE 1003.5: 1992	IEEE Standard for Information Technology - POSIX® Ada Language Interfaces - Part 1: Binding for System Application Program Interface (API) with Interpretations, March 1994	2.2.2.1.1.2 Language Bindings and Object Linking, 2.2.2.1.7 Operating System Services
136	IEEE 1003.5b: 1996	IEEE Standard for Information Technology - POSIX® Ada Language Interfaces - Part 1: Binding for System Application Program Interface (API) - Amendment 1: Real-time Extensions. (Incorporates IEEE 1003.5:1992).	2.2.2.1.7 Operating System Services
137	IEEE 1003.5g: 1999	IEEE Standard for Information Technology - POSIX® Ada Language Interfaces - Part 1: Binding for System Application Program Interface (API) - Amendment g: Realtime Extensions	2.2.2.1.7 Operating System Services
138	IEEE 1003.13:1998	IEEE Standard for Information Technology - Standardization Applications Environment Profile - POSIX® Realtime Application Support	2.2.2.1.7 Operating System Services, F.2.2.1.1 Operating System Services
139	IEEE 1073	Protocol for Medical Device Communications, 1996	D.2.3.2 Emerging Standards
140	ANSI/IEEE 1076	IEEE Standard VHDL Language Reference Manual, 1993	F.2.4.2 Emerging Standards, D.2.2.1.3 Product Data Interchange
141	IEEE 1076.2	VHDL Mathematical Package, 1996	F.2.4.2 Emerging Standards
142	IEEE 1076.3	Standard VHDL Synthesis Packages, 1997	F.2.4.2 Emerging Standards
143	IEEE 1076.4	VITAL Application-Specific Integrated Circuit (ASIC) Modeling Specification, 1995	F.2.4.2 Emerging Standards

#	Reference	Title and Date	Section
144	IEEE 1101.2	Standard for Mechanical Core Specifications for Conduction-Cooled Eurocards (ANSI), 1992	F.GVS.3.5.1.2.2 Single Board Computer (SBC) Expansion Buses, F.MS.3.5.1.1.1 Single Board Computer (SBC) Expansion Buses
145	IEEE 1320.1-1998	IEEE Standard for Functional Modeling Language-Syntax and Semantics for IDEF0	4.2.1 Activity Modeling
146	IEEE 1394: 1995	IEEE Standard for a High Performance Serial Bus	E.3.1.2.1.2 FireWire, F.AVS.3.5.1.1 Serial Buses F.SS.3.5.1.1 Serial Buses
147	IEEE 1394a: 2000	Amendment 1	F.AVS.3.5.1.1 Serial Buses F.SS.3.5.1.1 Serial Buses
148	IEEE 1394b	Standard for a High Performance Serial Bus, 2001	F.AVS.3.5.2 Emerging Standards F.SS.3.5.2.1 Serial Buses
149	IEEE 1445-1998	Standard for Digital Test Interchange Format (DTIF).	D.2.2.1.7.2 Digital Test Data Formats
150	IEEE 1484.1	Architecture and Reference Model Working Group Document: Learning Technology Systems Architecture (LTSA), Draft 5, 1999-12-08.	2.3.1.1.1 Learning Technology
151	IEEE P996.1/D1	Compact Embedded PC Modules, October 1993	F.3.5.2 Emerging Standards
152	IEEE P1003.1D	Real-Time Extensions	2.3.2 Service Area Standards
153	IEEE P1003.1e	POSIX® Part 1: System API - Protection, Audit, and Control Interfaces [C Language], Draft 15, reballot March 1996	6.2.2.2 Application Platform Entity
154	IEEE P1003.1e/D15	POSIX®: Protection Audit And Control Interface (C Language), December 1995	F.2.2.2.1 Operating System Services
155	IEEE P1003.1G	Protocol Independent Interfaces	2.3.2 Service Area Standards
156	IEEE P1003.1H	Services for Reliable, Available, Serviceable Systems	2.3.2 Service Area Standards
157	IEEE P1003.1J	Advanced Real-Time Extensions	2.3.2 Service Area Standards
158	IEEE P1003.2c	POSIX® Part 2: Shell and Utilities - Protection and Control Interfaces, Draft 15, reballot March 1996	6.2.2.2 Application Platform Entity
159	IEEE P1003.2L	Real-Time Distributed Systems Communication	2.3.2 Service Area Standards
160	IEEE P1003.5B	Ada Bindings for Real-Time Extensions	2.3.2 Service Area Standards
161	IEEE P1003.5c/D3	POSIX®-Part 1: Binding for API - Amendment 2: Protocol Independent Interfaces, October 1997	F.2.2.2.1 Operating System Services
162	IEEE P1003.5f	POSIX®: Ada Binding to 1003.21, January 1997	F.2.2.2.1 Operating System Services
163	IEEE P1003.22/D6	POSIX®-Open System Security Framework, August 1995	F.2.2.2.1 Operating System Services
164	IEEE P1386.1/D2.4	Physical/Environmental layers for Peripheral Component Interface (PCI) Mezzanine Cards (PMC), January 12, 2001	F.3.5.2.1.1 Single Board Computers (SBCs) and Expansion Cards
165	IEEE P1484.2	Learner Model Working Group Document: Public and Private Information (PAPI) for Learners, Draft Version 6, 2000-06-23	2.3.1.1.1 Learning Technology
166	IEEE 1484.11	Computer Managed Instruction (CMI) Working Group Document: Computer-Managed Instruction (CMI), Draft 3.3, 1999-02	2.3.1.1.1 Learning Technology
167	IEEE P1484.12	Learning Object Metadata (LOM), Working	2.3.1.1.1 Learning Technology

#	Reference	Title and Date	Section
		Group Document: Learning Object Metadata, Draft 4, 2000-02-05	
168	IEEE P1516	Modeling and Simulation (M&S) High Level Architecture (HLA) - Framework and Rules, Version 1.3, 23 April 1999	G.2.2.1.1 HLA Framework and Rules
169	IEEE P1516.1	Modeling and Simulation (M&S) High Level Architecture (HLA) Federate Interface Specification, Version 2, 23 April 1999	G.2.2.1.2 HLA Interface Specification
170	IEEE P1516.2	Modeling and Simulation (M&S) High Level Architecture (HLA) Object Model Template (OMT) Specification, Version 1.3, 23 April 1999	G.2.2.1.3 HLA Object Model Template (OMT)
171	IETF RFC-951	Bootstrap Protocol, September 1, 1985	3.2.1.1.1.7 Bootstrap Protocol (BOOTP), 3.2.2.1 Router Standards
172	IETF RFC-1285	Fiber-optic Data Distribution Interface (FDDI) MIBs	3.3.2 Emerging Network Standards
173	IETF RFC-1305	Network Time Protocol (V3), 9 April 1992	3.2.1.1.1.6 Network Time
174	IETF RFC-1332	PPP Internet Protocol Control Protocol (IPCP), May 26, 1992	3.2.2.2.2 Point to Point Standards
175	IETF RFC-1356	Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode, August 1992	3.2.2.2.4 Integrated Services Digital Network (ISDN), 3.2.2.2.6 X.25
176	IETF RFC-1381, 1382, and 1461	X.25 MIBs	3.3.2 Emerging Network Standards
177	IETF RFC-1471 through 1474	Point-to-Point Protocol (PPP) MIBs	3.3.2 Emerging Network Standards
178	IETF RFC-1508	Generic Security Service Application Program Interface (GSS-API), September 1993	6.2.2.4 Generic Security Service Application Program Interface (GSS API)
179	IETF RFC-1510	The Kerberos Network Authentication Service, V.5, 10 September 1993	6.2.1.2 Application Platform Entity
180	IETF RFC-1512	FDDI Management Information Base, September 1993	3.3.2 Emerging Network Standards
181	IETF RFC-1514	Host Resources MIB, September 1993	3.2.5.1 Data Communications
182	IETF RFC-1533	Dynamic Host Configuration Protocol (DHCP) Options and BOOTP Vendor Extensions, October 8, 1993	3.2.1.1.1.7 Bootstrap Protocol (BOOTP), 3.2.2.1 Router Standards
183	IETF RFC-1541	Dynamic Host Configuration Protocol (DHCP), October 27, 1993	3.2.1.1.1.8 Dynamic Host Configuration Protocol (DHCP)
184	IETF RFC-1542	Clarifications and Extensions for the Bootstrap Protocol, October 27, 1993	3.2.1.1.1.7 Bootstrap Protocol (BOOTP), 3.2.2.1 Router Standards
185	IETF RFC-1567	X.500 MIB	3.3.2 Emerging Network Standards
186	IETF RFC-1570	PPP Link Control Protocol (LCP) Extensions, January 11, 1994	3.2.2.2.2 Point to Point Standards
187	IETF RFC-1577	Protocol elements of LDAP	3.3.1 Emerging Host Standards
188	IETF RFC-1583	Open Shortest Path First Routing Version 2, March 23, 1994	3.2.2.1.2.1 Interior Routers
189	IETF RFC-1611	Domain Name Service (DNS) MIBs, May 1994	3.3.2 Emerging Network Standards
190	IETF RFC-1612	DNS Resolver MIB Extensions, May 1994	3.3.2 Emerging Network Standards

#	Reference	Title and Date	Section
191	IETF RFC-1618	PPP over ISDN, May 1994	3.2.2.2.4 Integrated Services Digital Network (ISDN)
192	IETF RFC-1657	Border Gateway Protocol version 4 (BGP-4) MIB	3.3.2 Emerging Network Standards
193	IETF RFC-1695	Asynchronous Transfer Mode (ATM) MIB	3.3.2 Emerging Network Standards
194	IETF RFC-1738	Uniform Resource Locators, December 20, 1994	3.2.1.1.1.9.2 Uniform Resource Identifier (URI)
195	IETF RFC-1757	Remote Network Monitoring Management Information Base, (RMON Version 1), February 1995	3.2.5.1 Data Communications
196	IETF (Informational) RFC-1770	IPv4 Option for Sender Directed Multi-Destination Delivery, 28 March 1995	3.2.1.1.2.1.4 Internet Protocol (IP), 3.2.2.1.1 Internet Protocol (IP)
197	IETF RFC-1771	Border Gateway Protocol 4, March 21, 1995	3.2.2.1.2.2. Exterior Routers
198	IETF RFC-1772	Application of BGP-4 In the Internet, March 21, 1995	3.2.2.1.2.2. Exterior Routers
199	IETF RFC-1777	LDAP, March 1995	3.2.1.1.1.2.2 Lightweight Directory Access Protocol (LDAP)
200	IETF RFC-1808	Relative Uniform Resource Locators, June 14, 1995	3.2.1.1.1.9.2 Uniform Resource Locator (URL)
201	IETF RFC-1812	Requirements for IP Version 4 Routers, June 22, 1995.	3.2.2.1 Router Standards
202	IETF RFC-1825	Security Architecture for the Internet Protocol	6.3.2.3 Networking Security Standards
203	IETF RFC-1826	IP Authentication Header	6.3.2.3 Networking Security Standards
204	IETF RFC-1827	IP Encapsulating Security Payload (ESP)	6.3.2.3 Networking Security Standards
205	IETF RFC-1828	IP Authentication using Keyed MD5	6.3.2.3 Networking Security Standards
206	IETF RFC-1829	The ESP DES-CBC Transform	6.3.2.3 Networking Security Standards
207	IETF RFC-1850	Open Shortest Path First (OSPF) Version 2 Management Information Base, November 1995	3.2.5.1 Data Communications
208	IETF RFC-1883	Internet Protocol, Version 6 (IPv6) Specification. 1995	3.3.1 Emerging Host Standards
209	IETF RFC-1885	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6), 1995	3.3.1 Emerging Host Standards
210	IETF RFC-1886	DNS Extensions to support IP version 6, 1995	3.3.1 Emerging Host Standards
211	IETF RFC-1938	A One-Time Password System	6.2.2.3 Authentication Security Standards
212	IETF RFC-1952	GZIP File Format Specification, Version 4.3, 23 May 1996.	2.2.2.1.4.10 File Compression
213	IETF RFC-1989	PPP Link Quality Monitoring, August 1996	3.2.2.2.2 Point to Point Standards
214	IETF RFC-1990	The PPP Multilink Protocol, August 96	3.2.2.2.2 Point to Point Standards
215	IETF RFC-1994	PPP Challenge Handshake Authentication Protocol (CHAP), August 1996	3.2.2.2.2 Point to Point Standards
216	IETF RFC-2001	TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms, 24	3.2.1.1.2.1.1 Transmission Control Protocol (TCP)

#	Reference	Title and Date	Section
		January 1997	
217	IETF RFC-2002	IP Mobility Support	3.3.1 Emerging Host Standards
218	IETF RFC-2006	The Definitions of Managed Objects for IP Mobility Support using SMIv2, October 1996	3.3.2 Emerging Network Standards
219	IETF RFC-2011	SNMPv2 Management Information Base for the Internet Protocol using SMIv2, November 1996	3.3.2 Emerging Network Standards
220	IETF RFC-2012	Transmission Control Protocol (TCP) MIB	3.3.2 Emerging Network Standards
221	IETF RFC-2013	User Datagram Protocol (UDP) MIB	3.3.2 Emerging Network Standards
222	IETF RFC-2021	Remote Network Management Monitoring Version 2 (RMON2) MIB	3.3.2 Emerging Network Standards
223	IETF RFCs 2045-2049	Multipurpose Internet Mail Extensions (MIME) Parts 1-5, November 1996	TABLE 2-1, 3.2.1.1.1.1 Electronic Mail
224	IETF RFC-2068	Hypertext Transfer Protocol (HTTP/1.1)	3.3.1 Emerging Host Standards
225	IETF RFC 2083	Portable Network Graphics (PNG) Specification, Version 1.0, January 1997	2.2.2.1.4.2 Graphics Data Interchange
226	IETF RFC 2104	"HMAC: Keyed-Hashing for Message Authentication," February 1997	6.3.2.3 Networking Security Standards
227	IETF RFC-2131	Dynamic Host Configuration Protocol, March 1997	3.2.1.1.1.8 Dynamic Host Configuration Protocol (DHCP), 3.2.2.1 Router Standards
228	IETF RFC-2132	DHCP Options and BOOTP Vendor Extensions, March 1997	3.2.1.1.1.7 Bootstrap Protocol (BOOTP), 3.2.2.1 Router Standards
229	IETF RFC-2136	Dynamic Updates in the Domain Name System, April 1997	3.2.1.1.1.2.3 Domain Name System (DNS)
230	IETF RFC-2138	Remote Authentication Dial In User Service (RADIUS), April 1997	6.2.2.3 Authentication Security Standards
231	IETF RFC 2205	Resource ReSerVation Protocol RSVP-Version 1	3.3.1 Emerging Host Standards
232	IETF RFC 2207	RSVP Extensions for IPSEC Data Flows	3.3.1 Emerging Host Standards
233	IETF RFC 2228	File Transfer Protocol, October 1997	6.3.2.3 Networking Security Standards
234	IETF RFC-2236	Internet Group Management Protocol, Version 2, November 1997	3.2.1.1.2.1.4 Internet Protocol (IP), 3.2.2.1.1 Internet Protocol (IP)
235	IETF-RFC 2246	The Transport Layer Security (TLS) Protocol Version 1.0, January 1999	6.3.2.2 Secure World Wide Web (WWW) Transactions
236	IETF RFC-2251	Lightweight Directory Access Protocol 3 (LDAP v3)	3.3.1 Emerging Host Standards
237	IETF RFC 2314	PKCS #10, Certification Request Syntax, Version 1.5, March 1998	6.3.2.6.4 Management Protocols
238	IETF RFC 2315	Public Key Cryptography Standard (PKCS) #7, Cryptographic Message Syntax, Version 1.5, March 1998	6.3.2.6.4 Management Protocols
239	IETF RFC-2373	IPv6 Addressing Architecture, July 1998	3.3.1 Emerging Host Standards
240	IETF RFC 2374	IPv6 Aggregatable Global Unicast Address Format	3.3.1 Emerging Host Standards
241	IETF RFC 2380	RSVP over ATM Implementation Requirements	3.3.1 Emerging Host Standards
242	IETF RFC 2396	Uniform Resource Identifiers (URI), Generic Syntax, August 1998	3.2.1.1.1.9.2 Uniform Resource Identifier (URI)
243	IETF RFC 2401	"Security Architecture for the Internet Protocol," S. Kent and R. Atkinson, November 1998	6.3.2.3 Networking Security Standards

#	Reference	Title and Date	Section
244	IETF RFC 2402,	"IP Authentication Header," S. Kent and R. Atkinson, November 1998	6.3.2.3 Networking Security Standards
245	IETF RFC 2406	"IP Encapsulating Security Payload (ESP)," November 1998	6.3.2.3 Networking Security Standards
246	IETF RFC 2407	"The Internet IP Security Domain of Interpretation for ISAKMP," November 1998	6.3.2.3 Networking Security Standards
247	IETF RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP), 21 February 1998	6.3.2.3 Networking Security Standards
248	IETF RFC 2452	IPv6 MIB for the TCP	3.3.1 Emerging Host Standards
249	IETF RFC 2454	IPv6 MIB for the UDP	3.3.1 Emerging Host Standards
250	IETF RFC 2460	IPv6 Specification	3.3.1 Emerging Host Standards
251	IETF RFC 2461	Neighbor Discovery for IPv6	3.3.1 Emerging Host Standards
252	IETF RFC 2462	IPv6 Stateless Address Auto-Configuration	3.3.1 Emerging Host Standards
253	IETF RFC 2463	ICMPv6 for the IPv6 Specification	3.3.1 Emerging Host Standards
254	IETF RFC 2464	Transmission of Ipv6 Packet Over Ethernet Networks	3.3.1 Emerging Host Standards
255	IETF RFC 2466	MIB for IPv6:ICMPv6 Group	3.3.1 Emerging Host Standards
256	IETF RFC 2472	IPv6 Over PPP	3.3.1 Emerging Host Standards
257	IETF-RFC 2487	SMTP Service Extension for Secure SMTP over TLS, January 1999	6.3.2.2 Secure World Wide Web (WWW) Transactions
258	IETF RFC 2492	IPv6 Over ATM Networks	3.3.1 Emerging Host Standards
259	IETF RFC 2515	Definitions of Managed Objects for ATM Management	3.3.2 Emerging Network Standards
260	IETF RFC 2559	Internet X.509 Public Key Infrastructure Operational Protocols: LDAPv2, April 1999	6.3.2.6.3 Operational Protocols and Exchange Formats
261	IETF RFC 2571	An Architecture for Describing SNMP Management Frameworks	3.3.2 Emerging Network Standards
262	IETF RFC 2572	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	3.3.1 Emerging Host Standards
263	IETF RFC 2573	SNMP Applications	3.3.1 Emerging Host Standards
264	IETF RFC 2574	User-based Security Model (USM) Version 3 of the Simple Network Management Protocol (SNMPv3)	3.3.1 Emerging Host Standards 6.2.2.4 Security Management Protocols
265	IETF RFC 2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)	3.3.2 Emerging Network Standards
266	IETF RFC-2581	TCP Congestion Control, April 1999	3.2.1.1.2.2 Transmission Control Protocol (TCP)
267	IETF RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema, June 1999	6.3.2.6.3 Operational Protocols and Exchange Formats
268	IETF RFC 2605	Directory Server Monitoring MIB	3.3.2 Emerging Network Standards
269	IETF RFC-2616	Hypertext Transfer Protocol - HTTP /1.1, June 1999	3.2.1.1.1.9.1 Hypertext Transfer Protocol (HTTP)
270	IETF Standard 3	(IETF RFC-1122 and IETF RFC-1123), Requirements for Internet Hosts, October 1989	3.2.1.1 Host Standards
271	IETF Standard 5	Internet Protocol, September 1981, (Also IETF RFC-791/IETF RFC-950/IETF RFC-919/IETF RFC-922/IETF RFC-792/IETF RFC-1112)	3.2.1.1.2.1.4 Internet Protocol (IP), 3.2.2.1.1 Internet Protocol (IP)
272	IETF Standard 6	User Datagram Protocol, August 1980, (Also IETF RFC-768)	3.2.1.1.2.3 User Datagram Protocol (UDP), 3.2.2.1 Router Standards

#	Reference	Title and Date	Section
273	IETF Standard 7	Transmission Control Protocol, September 1981, (Also IETF RFC-793)	3.2.1.1.2.1.1 Transmission Control Protocol (TCP), 3.2.2.1 Router Standards
274	IETF Standard 8	TELNET Protocol, May 1983, (Also IETF RFC-854/IETF RFC-855)	3.2.1.1.1.4 Remote Terminal, 3.2.2.1 Router Standards
275	IETF Standard 9	File Transfer Protocol, October 1985, with the following FTP commands mandated for reception: Store unique (STOU) and Abort (ABOR). (Also IETF RFC-959)	3.2.1.1.1.3 File Transfer
276	IETF Standard 10	Simple Mail Transfer Protocol (SMTP) Service Extensions, November 1995, (Also IETF RFC-821/IETF RFC-1869/IETF RFC-1870)	3.2.1.1.1.1 Electronic Mail
277	IETF Standard 11	Standard for the Format of ARPA Internet Text Messages, August 1982, (Also IETF RFC-822/IETF RFC-1049)	3.2.1.1.1.1 Electronic Mail
278	IETF Standard 13	Domain Name System, November 1987, (Also IETF RFC-1034/IETF RFC-1035)	3.2.1.1.1.2.3 Domain Name System (DNS), 3.2.2.1 Router Standards
279	IETF Standard 15	Simple Network Management Protocol (SNMP), May 1990, (Also IETF RFC-1157)	3.2.5.1 Data Communications
280	IETF Standard 16	Structure and Identification of Management Information for TCP/IP-based Internets, May 1990, (Also IETF RFC-1212, Concise MIB Definitions, March 1991, IETF RFC-1155)	3.2.2.1 Router Standards, 3.2.5.1 Data Communications
281	IETF Standard 17	Management Information Base for network management of TCP/IP-based Internets: MIB-II, March 1991, (Also IETF RFC-1213)	3.2.5.1 Data Communications
282	IETF Standard 33	Trivial FTP (TFTP), July 1992, (Also IETF RFC-1350) to be used for initialization only	3.2.2.1 Router Standards
283	IETF Standard 35	ISO Transport Service on top of the TCP, May 1987, (Also IETF RFC-1006)	3.2.1.1.2.5 Open Systems Interconnection (OSI)/Internet Interworking Protocol
284	IETF Standard 36	Transmission of IP and ARP over FDDI Networks, January 1993, (Also IETF RFC-1390)	3.2.2.2.7 Fiber Distributed Data Interface (FDDI)
285	IETF Standard 37	An Ethernet Address Resolution Protocol, November 1982, (Also IETF RFC-826)	3.2.2.2.1 Ethernet
286	IETF Standard 41	Standard for the Transmission of IP Datagrams Over Ethernet Networks, April 1984, (Also IETF RFC-894)	3.2.2.2.1 Ethernet
287	IETF Standard 50	Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994, (Also IETF RFC-1643)	3.2.5.1 Data Communications
288	IETF Standard 51	Point-to-Point Protocol (PPP), July 1994, (Also IETF RFC-1661/IETF RFC-1662)	3.2.2.2.2 Point to Point Standards
289	IETF Standard 54	Open Short Path First Routing Version 2, April 1998	3.2.2.1.2.1 Interior Routers
290	IS-41-C	Signaling protocol for CDMA and TDMA mobile cellular	3.3.2 Emerging Network Standards
291	IS-95-A	Mobile Cellular standard for CDMA	3.3.2 Emerging Network Standards
292	ISDN Security Program (ISP)-421	Revision 1.0: The ISP Security Association Management Protocol (SAMP), 15 May 1994	6.3.2.1 Security Association Management

#	Reference	Title and Date	Section
293	ISO 10181	OSI Security Frameworks	6.1.3 Background
294	ISO 13818-4	1.5Mbps - 6.0 Mbps, MPEG-2	2.3.2 Service Area Standards
295	ISO 7498-2	Information processing systems - Open Systems Interconnection - Basic Reference, 1989	6.1.3 Background
296	ISO 7776	Data Communication High-Level Data Link Control Procedures - Description of the X.25 LAPB-compatible DTE Data Link Procedures, 1986	3.2.2.2.6 X.25
297	ISO 8208	Data Communications - X.25 Packet Layer Protocol for Data Terminating Equipment, 1989	3.2.2.2.6 X.25
298	ISO 8601:1988	Data elements and interchange formats, Information interchange, Representation of dates and times	4.2.5.1 DoD Date Standards
299	ISO 8632:1992 with Amendment 1:1994 and Amendment 2:1995	Computer Graphics Metafile (CGM)- Interchange format for vector graphics data	2.2.2.1.4.2 Graphics Data Interchange, 2.2.2.1.4.4 Still Imagery Data Interchange, D.2.2.1.2 Graphics Data Interchange
300	ISO 8879: 1986	Information processing -- Text and office systems --Standard Generalized Markup Language (SGML)	2.2.2.1.4.1 Document Interchange, D.2.2.1.1 Document Interchange
301	ISO 9314-1	Fibre Distributed Data Interface (FDDI) - Pt 1: Token Ring Physical Layer (PHY)	3.2.2.2.7 Fiber Distributed Data Interface (FDDI)
302	ISO 9314-2	Fibre Distributed Data Interface (FDDI) - Pt 2: Token Ring Media Access Control (MAC).	3.2.2.2.7 Fiber Distributed Data Interface (FDDI)
303	ISO 9314-3	Fibre Distributed Data Interface (FDDI) - Pt 3: Physical Layer Medium Dependent (PMD).	3.2.2.2.7 Fiber Distributed Data Interface (FDDI)
304	ISO 9660:1988	Information processing - Volume and file structure of CD-ROM for information interchange	2.2.2.1.4.8 Data Interchange Storage Media
305	ISO 10303	Industrial Automation Systems and Integration - Product Data Representation and Exchange; Part 1, Overview and fundamental concepts, 1994; Part 11, Description methods: The EXPRESS language reference manual, 1994; Part 12, Description methods: The EXPRESS-I language reference manual, 1997; Part 21, Implementation methods: Clear text encoding of the exchange structure, 1994; Part 22, Implementation	D.2.2.2.1 Product Data Interchange
306	ISO UN/EDIFACT	UN/EDIFACT	D.2.2.1.4 Electronic Data Interchange
307	ISO WG21/ANSI X3J16	"Programming Language C++", 2 December 1996	2.3.2 Service Area Standards
308	ISO/IEC 7816	Identification Cards - Integrated Circuit(s) cards with contacts	D.3.1.1.1 Smart Card Technology Standards for Electronic Business/Electronic Commerce
309	ISO/IEC 8632:1992	Computer Graphics Metafile (CGM) for the Storage and Transfer of Picture Description Information, as profiled by MIL-STD-2301A, Computer Graphics Metafile (CGM) Implementation Standard for the National Imagery Transmission Format Standard, 5 June 1998	2.2.2.1.4.4 Still Imagery Data Interchange

#	Reference	Title and Date	Section
310	ISO/IEC 8652	Ada Reference Manual, Language and Standard Libraries, (Ada 95), 1995	2.2.2.1.1.1 Programming Languages
311	ISO/IEC 8802-3: 1996	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 10BASE-T Medium-Access Unit (MAU)	3.2.2.2.1 Ethernet
312	ISO/IEC 8802-3: 1996 (E)	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. (ANSI/IEEE Std 802.3, 1996 edition)	3.2.2.2.1 Ethernet
313	ISO/IEC 8802-3: 1996	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification, 10BaseT Medium access Unit (MAU) 2.3.1.1.1 Learning Technology	3.2.2.2.1 Ethernet
314	ISO/IEC 8802-11: 1999	(ISO/IEC) (IEEE standard 802.11-1999) Information Technology-Telecommunications and Information Exchange Between Systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.	3.2.2.2.1 Ethernet
315	ISO/IEC 8859-1	Information Technology - 8-Bit Single-Byte Coded Graphic Character Sets - Part 1: Latin Alphabet No. 1, 1988	2.2.2.1.8 Internationalization Services
316	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)	2.2.2.1.3 Data Management Services
317	ISO/IEC 9075-3	Information Technology - Database Languages - SQL - Part 3: Call Level Interface (SQL/CLI), 1995	2.2.2.1.3 Data Management Services
318	ISO/IEC 9579:2000	Information Technology - Remote Database Access for SQL with security enhancement	2.3.2.2 Data Management
319	ISO/IEC 9595: 1998	Information Technology-Open Systems Interconnection Common Management Information Services (CMIS	3.2.5.2 Telecommunications
320	ISO/IEC 9596-1: 1998	Information Technology - Open Systems Interconnection- Common Management Information Protocol (CMIP) - Part 1: Specification	3.2.5.2 Telecommunications, 6.2.2.5 Security Management Protocols
321	ISO/IEC 9596-2	Information technology -- Open Systems Interconnection -- Common Management Information Protocol: Protocol Implementation Conformance Statement (PICS) proforma, 1993	3.2.5.2 Telecommunications
322	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).	6.5.2.1 Entity Authentication
323	ISO/IEC 9945-	(Real-time Extensions) to ISO/IEC 9945-1:1996,	2.2.2.1.7 Operating System

#	Reference	Title and Date	Section
	1:1996	Information Technology - Portable Operating System Interface (POSIX®) - Part 1: System Application Program Interface (API) [C language] (Real-time Optional Services).	Services
324	ISO/IEC 9945-1:1996	(Thread Extensions) to ISO/IEC 9945-1:1996, Information Technology - Portable Operating System Interface (POSIX®) - Part 1: System Application Program Interface (API) [C language] (Thread Optional Services).	2.2.2.1.7 Operating System Services
325	ISO/IEC 9945-2:1993	Information Technology Portable Operating System Interface (POSIX®) - Part 2: Shell and Utilities, Information Technology - Portable Operating System Interface (POSIX®) - Recommendations (Section 12) and Implementation Guidance (Section 13).	2.2.2.1.7 Operating System Services
326	ISO/IEC 9899:1999	Information Technology -Programming Language C.	2.2.2.1.1.1 Programming Languages
327	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).	6.3.2.5 Other
328	ISO/IEC 10038: 1993	Information technology-Telecommunications and information exchange between systems-Local area networks-Media access control (MAC) bridges, (Also ANSI/IEEE Std 802.1D, 1993 Edition)	3.2.2.2.1 Ethernet
329	ISO/IEC 10164-7	Information Technology-Open System Interconnection -Systems Management - Part 7: Security Alarm Reporting Function, (ITU-T X.736) 1992	6.2.2.1.1 Security Alarm Reporting
330	ISO/IEC 10165	Information Technology - Open Systems Interconnection- Structure of Management Information - Parts 1- 4, 1993 - 1994	6.3.3 Summary of Standards, 6.4.2 Emerging Standards
331	ISO/IEC 10536	Identification Cards - Contactless integrated circuit(s) card	D.3.1.1.1 Smart Card Technology Standards for Electronic Business/Electronic Commerce
332	ISO/IEC 10646-1	Information Technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane, 2000	2.2.2.1 Internationalization Services
333	ISO/IEC 10918-1	Joint Photographic Experts Group (JPEG) as profiled by MIL-STD-188-198A, Joint Photographic Experts Group (JPEG) Image Compression for the National Imagery Transmission Format Standard, 15 December 1993	2.2.2.1.4.4 Still Imagery Data Interchange
334	ISO/IEC 11172-1	Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s - Part 1: Systems, 1993; with Technical Corrigendum 1:1995	2.2.2.1.4.7.2 Video Support
335	ISO/IEC 11172-1: 1993/Cor. 1:1995	Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s - Part 1: Systems, 1993; with Technical Corrigendum 1:1995	2.2.2.1.4.6 Audio Data Interchange, 2.2.2.1.4.7.2 Video Support

#	Reference	Title and Date	Section
336	ISO/IEC 11172-2	Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s - Part 2 Video; 1993	2.2.2.1.4.7.2 Video Support
337	ISO/IEC 11172-3: 1993	Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Megabits per second (Mbit/s) - Part 3 (Audio Layer-3 only); with Technical Corrigendum 1:1996	2.2.2.1.4.7.2 Video Support
338	ISO/IEC 11172-3/Cor. 1	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), 1996	2.2.2.1.4.6 Audio Data Interchange
339	ISO/IEC 13584:1998	Industrial Automation Systems and Integration - Parts Library - Part 20; Logical Resource: Logical Model of Expressions; Part 42: Description Methodology: Methodology for Structuring Part Families	D.2.2.2.1 Product Data Interchange
340	ISO/IEC 13818-1: 1996	Information Technology - Generic Coding of Moving Pictures and Associated Audio Information - Part 1: Systems (MPEG-2); 1996, with Amendment 1:1997	2.2.2.1.4.7.1 Video Imagery, 2.2.2.1.4.7.2 Video Support
341	ISO/IEC 13818-2	Generic Coding of Moving Pictures and Associated Audio Information - Part 2: Video (MPEG-2); 1996, with Amendment 1:1997 and Amendment 2:1997. (The identical text is also published as ITU-T Rec. H.262).	2.2.2.1.4.7.1 Video Imagery, 2.2.2.1.4.7.2 Video Support
342	ISO/IEC 13818-3:1995	Information technology - Generic coding of moving pictures and associated audio information, with Amendment 1:1996. Used for compressed digital audio systems, MPEG-2 Part 3: Audio	2.2.2.1.4.7.1.1 Audio for Video Imagery
343	ISO/IEC 13818-4:1996	Information Technology - Generic Coding of Moving Pictures and Associated Audio Information - Part 4: Conformance testing; 1996	2.2.2.1.4.7.1 Video Imagery
344	ISO/IEC 14519:1999	Information Technology - POSIX® Ada Language Interfaces -Binding for System Application Program Interface (API) - Realtime Extensions.	2.2.2.1.7 Operating System Services
345	ISO/IEC 14772-1:1998	Information Technology - Computer Graphics and Image Processing -The Virtual Reality Modeling Language - Part 1: Functional specification and UTF-8 encoding	2.3.2.1.1.2 Virtual Reality Modeling Language
346	ISO/IEC 15408:1999	Information Technology - Security Techniques - Evaluation Criteria for Security (parts 1 through 3), 1 December 1999, also documented with the same technical content in Common Criteria (parts 1 through 3), Version 2.1	6.2.1 Mandated Standards, 6.3.1 Mandates
347	ISO/IEC 15444-1	Information Technology - JPEG 2000 Image Coding System - Part 1: Core Coding System.	2.3.2.1.1.4 Still-Imagery Data Interchange
348	ISO/IEC 15802-2: 1995	Information Technology-Telecommunications And Information Exchange Between Systems-Local And Metropolitan Area Networks - Common Specifications-Part 2: LAN/MAN Management (ANSI), (Also ANSI/IEEE Std	3.2.2.2.1 Ethernet

#	Reference	Title and Date	Section
		802.1B, 1995 Edition)	
349	ISO/IEC 15816:2001	Information Technology - Security Techniques - Security Information Objects for Access Control	6.3.1.1 Security Protocols
350	ISO/IEC 15948:2000	Portable Network Graphics (PNG): Functional Specification Final Committee Draft (FCD).	2.3.2.1.1.1 Graphic Data Interchange
351	ISO/IEC DIS 9075-1:1999	Information technology - Database languages - SQL - Part 1: Framework (SQL/Framework).	2.3.2.2 Data Management Services
352	ISO/IEC DIS 9075-2:1999	Information technology - Database languages - SQL - Part 2: Foundation (SQL/Foundation).	2.3.2.2 Data Management Services
353	ISO/IEC DIS 9075-3:1999	Information technology - Database languages - SQL - Part 3: Call-Level Interface (for SQL3).	2.3.2.2 Data Management Services
354	ISO/IEC DIS 9075-4:1999	Information technology - Database languages - SQL - Part 4: Persistent Stored Modules (SQL/PSM).	2.3.2.2 Data Management Services
355	ISO/IEC DIS 9075-5	Information technology - Database languages - SQL - Part 5: Host Language Bindings (SQL/Bindings).	2.3.2.2 Data Management Services
356	ISO/IEC DIS 9075-10	Information technology - Database languages - SQL - Part 10: Object Language Bindings (SQL/OLB).	2.3.2.2 Data Management Services
357	ISO/IEC DIS 13249-3:1999	Information Technology - Database languages - SQL Multimedia and Application Packages - Part 3: Spatial	2.3.2.2 Data Management Services
358	ISP-421, Revision 1.0	The ISP Security Association Management Protocol (SAMP), ISDN Security Program (ISP), 15 May 1994	6.3.2.1 Security Association Management
359	ITU Recommendation G.726	40, 32, 24, 16 kbps Adaptive Differential Pulse Code Modulation (ADPCM), December 1990	F.2.2.1.2 Audio Data Interchange
360	ITU-R BT.601-4	Encoding Parameters of Digital Television for Studios, 1994	2.2.2.1.4.7.1 Video Imagery
361	ITU-R TF.460-4	Standard-frequency and Time-signal Emissions, International Telecommunications Union, July 1986	2.2.2.1.4.12 Time of Day Data Interchange
362	ITU-T E.164	Numbering Plan for the ISDN Era, May 1997	3.2.2.2.4 Integrated Services Digital Network (ISDN)
363	ITU-T G.711	Pulse code modulation 3.1 KHz to 48, 56, and 64 (narrowband speech mode), November, 1988	3.2.1.2 Video Teleconferencing (VTC) Standards
364	ITU-T G.728	Audio CODEC 3.1 KHz at 16 Kbps (narrowband speech mode), September, 1992	3.2.1.2 Video Teleconferencing (VTC) Standards
365	ITU-T H.221	Frame structure for 64 to 1920 Kbit/s channel in audio visual services, May 1999	3.2.1.2 Video Teleconferencing (VTC) Standards
366	ITU-T H.222/0	Information technology - Generic coding of moving pictures and associated audio information: Systems	3.3.1 Emerging Host Standards
367	ITU-T H.222/1	Information technology - Generic coding of moving pictures and associated audio information: Systems	3.3.1 Emerging Host Standards
368	ITU-T H.224	A Real Time Control Protocol for Simplex Applications using H.221 LSD/HSD/MLP channels, November 1994	3.2.1.2 Video Teleconferencing (VTC) Standards
369	ITU-T H.230	Frame-synchronous control and indication signals for audio visual systems, May, 1999	3.2.1.2 Video Teleconferencing (VTC) Standards

#	Reference	Title and Date	Section
370	ITU-T H.231	Multipoint control unit functional description, July, 1997	3.2.1.2 Video Teleconferencing (VTC) Standards
371	ITU-T H.242	System for establishing communication between audio visual terminals using digital channels up to 2 Mbits/s, May, 1999	3.2.1.2 Video Teleconferencing (VTC) Standards
372	ITU-T H.243	Procedure for establishing communication between three or more audio visual terminals using digital channels up to 2 Mbit/s, July, 1997	3.2.1.2 Video Teleconferencing (VTC) Standards
373	ITU-T H.244	Synchronized Aggregation of Multiple 64 or 56 kbps channels, July 1995	3.2.1.2 Video Teleconferencing (VTC) Standards
374	ITU-T H.261	Video CODEC for audiovisual services at px64 Kbps, March, 1993	3.2.1.2 Video Teleconferencing (VTC) Standards
375	ITU-T H.281	A Far-End Camera Protocol for Videoconferencing Using H.224, November 1994	3.2.1.2 Video Teleconferencing (VTC) Standards
376	ITU-T H.310	Includes underlying standards for video (MPEG2) and audio (MPEG1, MPEG2). H.310 can be used for high-quality VTC requiring > 2 Mbps infrastructure, but does not currently have much industry support	3.3.1 Emerging Host Standards
377	ITU-T H.320	Narrowband Visual Telephone Systems and Terminal Equipment, May, 1999	3.2.1.2 Video Teleconferencing (VTC) Standards
378	ITU-T H.321	Specifies the operation of H.320 codecs over ATM using AAL-1 or AAL-5. H.321 uses Quality of Service to manage videoconferencing quality. It lacks industry wide support	3.3.1 Emerging Host Standards
379	ITU-T H.323	ITU-T H.323, Packet-based Multimedia Communications Systems, January 1998	3.2.1.2 Video Teleconferencing (VTC) Standards
380	ITU-T H.324	Terminal for Low Bit Rate Multimedia Communications, January 1998	3.2.1.2 Video Teleconferencing (VTC) Standards
381	ITU-T I.363.1	B-ISDN ATM Adaptation Layer Specification: Type 1 ATM Adaptation Layer (AAL1), August 1996	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
382	ITU-T I.363.5	B-ISDN ATM Adaptation Layer Specification: Type 5 ATM Adaptation Layer (AAL5), August 1996	3.2.2.2.5 Asynchronous Transfer Mode (ATM)
383	ITU-T M.3207.1	TMN management service: maintenance aspects of B-ISDN management, 1996	3.2.5.2 Telecommunications
384	ITU-T M.3211.1	TMN management service: Fault and performance management of the ISDN access, 1996	3.2.5.2 Telecommunications
385	ITU-T M.3400	TMN Management Functions, 1997	3.2.5.2 Telecommunications
386	ITU-T Rec. X.500	Directory Infrastructure, (Also ISO/IEC 9594-1)	6.3.2.6.2 Directory and Certificate Profile Standards, 6.3.1.4 MISSI Digital Signature Infrastructure
387	ITU-T Rec. X.509 Version 3	The Directory: Authentication Framework, 1997, that is DMS compliant, (Also ISO/IEC 9594-8.2),	6.3.1.4 MISSI Digital Signature Infrastructure
388	ITU-T T.4	Group 3 facsimile – hardcopy representation, July, 1996	3.2.1.2 Video Teleconferencing (VTC) Standards
389	ITU-T T.82	Softcopy image compression (Joint Bi-level Image Experts Group [JBIG]), March, 1993	3.2.1.2 Video Teleconferencing (VTC) Standards
390	ITU-T T.81	Softcopy color image compression (Joint Photographic Experts Group [JPEG]), September, 1992	3.2.1.2 Video Teleconferencing (VTC) Standards

#	Reference	Title and Date	Section
391	ITU-T T.120	Transmission Protocols for Multimedia Data, July 1996	3.2.1.2 Video Teleconferencing (VTC) Standards
392	ITU-T T.122	Multipoint Communications Service for Audiographic and Audio Visual Conferencing Service Definition, March 1993	3.2.1.2 Video Teleconferencing (VTC) Standards
393	ITU-T T.123	Protocol Stacks for Audiographic and Audiovisual Teleconferencing Applications, May, 1999	3.2.1.2 Video Teleconferencing (VTC) Standards
394	ITU-T T.124	Generic Conference Control for Audiographic and Audiovisual Terminals and Multipoint Control Units, January, 1998	3.2.1.2 Video Teleconferencing (VTC) Standards
395	ITU-T T.125	Multipoint Communications Service Protocol Specification, February, 1998	3.2.1.2 Video Teleconferencing (VTC) Standards
396	ITU-T T.126	Multipoint Still Image and Annotation Conferencing Protocol Specification, July, 1997	3.2.1.2 Video Teleconferencing (VTC) Standards
397	ITU-T T.127	Multipoint Binary File Transfer Protocol, August 1995	3.2.1.2 Video Teleconferencing (VTC) Standards
398	ITU-T T.128	Multipoint application sharing, January, 1998	3.2.1.2 Video Teleconferencing (VTC) Standards
399	ITU-T X.25	Interface Between DTE and DCE for Terminals Operating in the Packet Mode on Public Data Networks.	3.2.2.2.6 X.25
400	ITU-T X.500	The Directory - Overview of Concepts, Models, and Services - Data Communication Networks Directory, 1993	3.2.1.1.1.2.1 X.500 Directory Services
401	ITU-T X.736	Information Technology-Open System Interconnection -Systems Management - Part 7: Security Alarm Reporting Function, 1992	6.2.2.2.1 Security Alarm Reporting
402	NEMA/ACR DICOM V3.0	Digital Imaging and Communication in Medicine, 1993	D.2.2.1.2 Graphics Data Interchange
403	M021	CDE 2.1/Motif® 2.1 User's Guide, ISBN 1-85912-173-X, October 1997.	2.2.2.1.2 User Interface Services
404	M027	CDE 2.1/Motif® 2.1 - Style Guide and Glossary, ISBN 1-85912-104-7, October 1997	2.2.2.1.2 User Interface Services, 5.2.2.1.1 X-Window Style Guides
405	M028	CDE 2.1/Motif® 2.1 - Style Guide Certification Check List, ISBN 1-85912-109-8, October 1997	2.2.2.1.2 User Interface Services, 5.2.2.1.1 X-Window Style Guides
406	M029	CDE 2.1/Motif® 2.1 - Style Guide Reference, ISBN 1-85912-114-4, October 1997	2.2.2.1.2 User Interface Services, 5.2.2.1.1 X-Window Style Guides
407	M213	Motif® 2.1 - Programmer's Guide, ISBN 1-85912-134-9, October 1997	2.2.2.1.2 User Interface Services
408	M214A	Motif® 2.1 - Programmer's Reference, Volume 1, ISBN 1-85912-119-5, October 1997	2.2.2.1.2 User Interface Services
409	M214B	Motif® 2.1 - Programmer's Reference, Volume 2, ISBN 1-85912-124-1, October 1997	2.2.2.1.2 User Interface Services
410	M214C	Motif® 2.1 - Programmer's Reference, Volume 3, ISBN 1-85912-164-0 October 1997	2.2.2.1.2 User Interface Services
411	M216	Motif® 2.1 - Widget Writer's Guide, ISBN 1-85912-129-2, October 1997	2.2.2.1.2 User Interface Services

#	Reference	Title and Date	Section
412	ODMG-9x	SQL3	2.3.2 Service Area Standards
413	OMG Document bom/99-03-01	Workflow Management Facility, 9 March 1999	2.3.1.2 Business Processing
414	OMG Document formal/99-10-07	Common Object Request Broker: Architecture and Specification, Version 2.3.1, October 1999.	2.2.2.1.11 Distributed Computing Services
415	OMG Document formal/2000-05-02	Workflow Management Facility Specification, V1.2 April 2000	2.3.1.2 Business Processing
416	Open Group 1992	Open Group /Motif® Style Guide, Revision 1.2	5.2.2.1 Commercial Style Guides
417	RTCA DO-181A	Minimum Operational Performance Standards for Air Traffic Control Radar Beacon System/Mode Select (ATCRBS/Mode S), Airborne Equipment, 14 January 1992, Change 1 errata 14 January 1993	F.AVS.3.6.2 Emerging Standards
418	RTCA DO-210C	Minimum Operational Performance Standards For Aeronautical Mobile Satellite Services (AMSS), 16 January 1996	F.AVS.3.6.2 Emerging Standards
419	RTCA DO-212	Minimum Operational Performance Standards for Airborne Automatic Dependent Surveillance (ADS) Equipment, 26 October 1992	F.AVS.3.6.2 Emerging Standards
420	RTCA DO-219	Minimum Operational Performance Standards for ATC Two-Way Data Link Communications, 27 August 1993	F.AVS.3.6.2 Emerging Standards
421	RTCA DO-224 – Change 1	Signal-in-Space Minimum Aviation Systems Performance Standards (MASPS) Advanced VHF Digital Data, Communications Including Capability with Digital Voice Technique, 30 April 1998	F.AVS.3.6.2 Emerging Standards
422	SAE J1587	Joint SAE/TMC Electronic Data Interchange Between Microcomputer Systems in Heavy-Duty Vehicle Applications	F.GVS.3.5.2.1 Serial Buses
423	SAE J1708	Serial Data Communications Between Microcomputer Systems in Heavy-Duty Vehicle Applications	F.GVS.3.5.2.1 Serial Buses
424	SAE J1850	Class B Data Communication Network Interface, 1 July 1995	F.GVS.3.5.1.1 Serial Buses
425	SAE J1939	Truck and Bus Control and Communications Network	F.GVS.3.5.2.1 Serial Buses
426	SMPTE 170M	Television - Composite Analog Video Signal - NTSC for Studio Applications, 1994	F.SS.3.5.1 Mandates
427	SLP-MSG-210	Revision, Sensor Link Protocol Message Set, 26 March 2001	E.2.4.1.1 Sensor Link Protocol (SLP) Message Set F.GVS.2.4.2.1 Tactical Information Exchange Standards F.MUS.2.4.2.1 Tactical Information Exchange Standards F.SS.2.4.2.1.1 Sensor Link Protocol (SLP) Message Set
428	T11/Project 1237-	D/1.4(Draft) Information Technology -Fibre Channel - Audio Video (FC-AV)	F.AVS.3.5.2 Emerging Standards
429	T11/Project 1332	T11/Project 1332-D/Rev 1.6(Draft) Fibre Channel - Virtual Interface (FC-VI)	F.AVS.3.5.2 Emerging Standards
430	TIA/EIA 465-A	Group 3 Facsimile Apparatus for Document	3.2.1.3.1 Analog Facsimile

#	Reference	Title and Date	Section
		Transmission, 21 March 1995	Standard
431	TIA/EIA-466-A	Procedures for Document Facsimile Transmission, 27 September 1996	3.2.1.3.1 Analog Facsimile Standard
432	UNIX® 1998	Open Group's Single UNIX® Specification (SUS), X/Open, 1998	2.2.2.2.4.1 Remote Procedure Computing, 2.3.2 Service Area Standards
433	VPP-2	VXIplug&play System Alliance System Frameworks Specification, Revision 4.0, 29 January 1996	D.3.1.1.2 System Framework Standards for ATS
434	VPP-3.2	VXIplug&play Systems Alliance Instrument Driver Functional Body Specification, Revision 4.0, 2 February 1996	D.2.2.1.7.1 Instrument Driver API Standards
435	VPP-4.3	VXIplug&play (VPP) Systems Alliance Virtual Instrument Standard Architecture (VISA) Library, 22 January 1997	D.2.3.1.1 Instrument Communication Manager Standards for ATS
436	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.	6.5.2.2 Personal Authentication
437	WFMC-TC-1009	Workflow Management Application Programming Interface (Interface 2&3) Specification, July 1998	2.3.1.2 Business Processing
438	WFMC-TC-1013	Workflow Management Coalition, Workflow Client Application (Interface 2) Application Programming Interface (WAPI), Naming Conventions, 1 November 1997	2.3.1.2 Business Processing
439	WFMC-TC-1016-P	Workflow Management Coalition, Interface 1: Process Definition Interchange, Process Model, 12 November 1998	2.3.1.2 Business Processing
440	WFMC-TC-1018	Workflow Management Coalition, Workflow Standard - Interoperability, Internet e-mail MIME Binding, 25 September 1998	2.3.1.2 Business Processing
441	WFMC-TC-1023	Workflow Management Coalition, Workflow Standard - Interoperability WF-XML Binding, 20 April 1999	2.3.1.2 Business Processing
442	W3C REC-html40-19980424	HTML 4.0 Specification, W3C Recommendation, April 24, 1998	2.2.2.1.4.1 Document Interchange
443	W3C REC-png.html	PNG (Portable Network Graphics) Specification	2.2.2.1.4.2 Graphics Data Interchange
444	W3C REC-xml-19980210	Extensible Markup Language (XML) 1.0. W3C Recommendation, 10 February 1998	2.2.2.1.4.1 Document Interchange
445	(No Number)	Aeronautical Telecommunications: Appendix 10 to the Convention on International Civil Aviation, volume IV (Surveillance radar and Collision Avoidance Systems), Edition 1, International Civil Aviation Organization (ICAO): Montreal, 1995, with Supplements (31 May 1996 and 10 November 1997).	F.3.6.1.1 Mandates
446	(No Number)	ATM Forum's, Protocol Implementation Extra Information for Testing (Pixit) pro forma	3.3.2 Emerging Network Standards
447	(No Number)	ATM Forum's, Protocol Information Conformance Statement (PICS) pro forma	3.3.2 Emerging Network Standards
448	(No Number)	BioAPI Specification, Version 1.1, March 16,	2.2.1.1 Biometric Technology

#	Reference	Title and Date	Section
		2001	Services
449	(No Number)	Common Desktop Environment (CDE) 2.1	2.3.2 Service Area Standards, 5.3 EMERGING STANDARDS
450	(No Number)	CORBAservices Specification, July 4, 1997 - Common Object Services Specification	2.3.2 Service Area Standards
450	(No Number)	Document Object Model (DOM) Level 2 Core Specification Version 1.0 W3C Recommendation, 13 November 2000	4.3.8.2 XML Parsing and Manipulating
451	(No Number)	Event Service Specification: March 1995, contained in CORBAservices: Common Object Services Specification, December 1998.	2.2.2.2.4.2 Distributed-Object Computing
452	(No Number)	Extensible Markup Language (XML) 1.0 (Second Edition) W3C Recommendation 6 October 2000'<http://www.w3.org/TR/2000/REC-xml-20001006>	4.2.8 XML-Based Information Exchange
453	(No Number)	Extensible Stylesheet Language (XSL) Version 1.0, W3C Candidate Recommendation, 21 November 2000' <http://www.w3.org/TR/2000/WD-xsl-20000327>	4.3.8.1 XML Transformation
454	(No Number)	Graphics Interchange Format (GIF), Version 89a, 31 July 1990, CompuServe Incorporated	2.2.2.1.4.2 Graphics Data Interchange
455	(No Number)	HTML 4.01 Specification, W3C Recommendation, revised on 24-Dec-1999, REC-html401-19991224 <http://www.w3.org/TR/1999/REC-html401-19991224>	2.2.2.1.4.1 Document Interchange
456	(No Number)	IETF Transport Layer Security Protocol (TLSP) V1, dated 24 March 1997	6.3.2.2 Secure World Wide Web (WWW) Transactions
457	(No Number)	International Civil Aviation Organization (ICAO), Annex 10, Volume III concerning Standards and Recommended Practices (SARPs) for High Frequency Data Link (HFDL), July 1995	F.AVS.3.6.2 Emerging Standards
458	(No Number)	JPEG File Interchange Format (JFIF), Version 1.02, C-Cube Microsystems, 1 September 1992	2.2.2.1.4.2 Graphics Data Interchange
459	(No Number)	Life Cycle Service Specification: November 1996, contained in CORBAservices: Common Object Services Specification, December 1998.	2.2.2.2.4.2 Distributed-Object Computing
460	(No Number)	MNG (Multiple-Image Network Graphics) Format Version 1.0, January 2001	2.3.2.1.1.1 Graphic Data Interchange
461	(No Number)	Naming Service Specification: March 1995, contained in CORBAservices: Common Object Services Specification: December 1998.	2.2.2.2.4.2 Distributed-Object Computing
462	(No Number)	Object Model Template Data Interchange Format (OMT DIF), Version 1.3, February 1998	G.2.4.1.2 Object Model Template Data Interchange Format
463	(No Number)	Object Transaction Service, November 1997, contained in CORBAservices Specification, July 4, 1997 - Common Object Services Specification	2.3.2 Service Area Standards
464	(No Number)	OMG Facility for Distributed Simulation Systems, Version 1.0, dated 10 November 1998	G.2.2.1.2 HLA Interface Specification
465	(No Number)	Open Data Base Connectivity (ODBC), ODBC 3.0	G.2.2.1.5 Data Management Services
466	(No Number)	Open Group Distributed Computing Environment	6.2.1.2 Application Platform

#	Reference	Title and Date	Section
		(DCE) Version 1.1	Entity
467	(No Number)	PCI Industrial Computer Manufacturer's Group (PICMG): Compact PCI Specification, R2.1, September 1997	F.GVS.3.5.1.2.1 Backplane Buses, F.MUS.3.5.1 Mandates, F.MUS.3.5.1.1.1 Backplane Buses
468	(No Number)	Personal Computer Memory Card International Association (PCMCIA), PC Card Standard, March 1997	F.3.5.1 Mandates
469	(No Number)	Portable Network Graphics (PNG) Specification, Version 1.0, World Wide Web Consortium, 1 October 1996	2.3.2 Service Area Standards
470	(No Number)	RSA Laboratories Public Key Cryptography Standard (PKCS) #1, RSA Cryptography Standard, Version 2.0, 1 October 1998	6.3.2.6.6 Cryptography
471	(No Number)	RSA Laboratories Public Key Cryptography Standard (PKCS) #11,Cryptographic Token Interface Standard, Version 1.0, 28 April 1995	6.3.2.6.5 Application Program Interfaces (APIs)
472	(No Number)	RSA Laboratories Public Key Cryptography Standard 12, Personal Information Exchange Syntax Standard, version 1.0 (Draft), 30 April 1997	6.3.2.6.3 Operational Protocols and Exchange Formats
473	(No Number)	SAX, The Simple API for XML, Version 2.0, 28 December 2000.	4.3.8.2 XML Parsing and Manipulating
474	(No Number)	Secure Sockets Layer (SSL) Protocol Version 3.0, 18 November 1996	6.3.1.7 Secure World Wide Web (WWW) Transactions
475	(No Number)	The Common Object Request Broker: Architecture and Specification, Version 2.2, OMG Group, Inc. document formal, 1 February 1998	2.2.2.2.4.2 Distributed-Object Computing
476	(No Number)	The Java Virtual Machine (JVM) is defined in "The Java Virtual Machine Specification" by Tim Lindholm and Frank Yellin, Addison-Wesley, 1997, ISBN 0-201-63452-X	2.3.2.3 Virtual Machines
477	(No Number)	The Object Database Standard: ODMG 3.0, Edited by R.G.G. Cattell et al. The Morgan Kaufmann Series in Data Management, 2000, ISBN 1-55860-647-4	2.3.2.2 Data Management Services
478	(No Number)	The OpenGL Graphics System: A Specification (Version 1.2.1), 1 April 1999	2.2.2.1.5 Graphic Services
479	(No Number)	The Windows® Interface Guidelines for Software Design, Microsoft® Press, 1995	5.2.2.1.2 Windows Style Guide
480	(No Number)	Time Service Specification: July 1997, contained in CORBAservices: Common Object Services Specification, December 1998.	2.2.2.2.4.2 Distributed-Object Computing
481	(No Number)	Trading Object Service Specification: March 1997, contained in CORBAservices: Common Object Services Specification, December 1998.	2.2.2.2.4.2 Distributed-Object Computing
482	(No Number)	Transaction Service Specification: November 1997, contained in CORBAservices: Common Object Services Specification, December 1998.	2.2.2.2.4.2 Distributed-Object Computing
483	(No Number)	Trusted Systems Interoperability Group (TSIG) Trusted Information Exchange for Restricted Environments (TSIX(RE)) 1.1	6.3.2.4 Security Protocols

#	Reference	Title and Date	Section
484	(No Number)	The Uniform Modeling Language (UML) version 1.3 of June 1999 as adopted by the Object Management Group (OMG).	4.2.3 Object Modeling
485	(No Number)	User Interface Specifications for the Defense Information Infrastructure (DII), Version 4.0, October 1999	D.2.5 Human-Computer Interface Standards
486	(No Number)	W3C Recommendation, XML Schema Part 1: Structures, 2 May 2001,< http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/>	4.2.8.1 XML Schema
487	(No Number)	W3C Recommendation, XML Schema Part 2: Datatypes, 2 May 2001, <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>	4.2.8.1 XML Schema
489	(No Number)	Win32 APIs, as specified in the Microsoft Platform SDK, which can be found on the Microsoft Developer Network. Win32 APIs, as specified in the Microsoft Platform SDK.	2.2.2.1.2 User Interface Services, 2.2.2.1.7 Operating System Services
490	(No Number)	XForms 1.0: Data Model W3C Working Draft, 06 April 2000	2.3.2.1.1.6 Document Interchange
491	(No Number)	XForms Requirements, W3C Working Draft, 29 March 2000	2.3.2.1.1.6 Document Interchange
492	(No Number)	XML Metadata Interchange (XMI), Version 1.1, ad/99-10-22, 25 October 1999.	4.3.3.1 Object Metadata Exchange
493	(No Number)	XML Metadata Interchange (XMI), Version 1.1 - Appendices, ad/99-10-13, 25 October 1999.	4.3.3.1 Object Metadata Exchange
494	(No Number)	XSL Transformations (XSLT) Version 1.0, W3C Recommendations, 16 November 1999 <http://www.w3.org/TR/1999/REC-xslt-19991116>.	4.3.8.1 XML Transformation

B.3 CANDIDATES FOR REMOVAL FROM THE JTA-ARMY

Table B-5 contains mandated standards that are candidates for removal in the next version of the JTA-Army. Generally, these standards are used in current systems, but they are discouraged for use in new systems or in systems being upgraded.

Also, Table B-5 contains mandated ICDs. ICDs are mandated since no standards are available yet. As standards are developed, the ICDs will be replaced.

TABLE B-5 - CANDIDATES FOR REMOVAL FROM THE JTA-ARMY

#	Reference	Title and Date	Section
1	EIA 232E	Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, July 1991.	3.2.2.2.6 X.25
2	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.)	3.2.2.2.6 X.25

#	Reference	Title and Date	Section
3	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.)	3.2.2.2.6 X.25
4	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.)	3.2.2.2.6 X.25
5	ICD-GPS-200C	NAVSTAR GPS Space Segment/Navigation User Interfaces, 16 Oct 97.	3.2.1.5 Global Position System (GPS) Standards
6	ICD-GPS-222A	NAVSTAR GPS UE Auxiliary Output Chip Interface (U), 26 Apr 96.	3.2.1.5 Global Position System (GPS) Standards
7	ICD-GPS-225A	NAVSTAR GPS Selective Availability/Anti-Spoofing Host Application Equipment Design Requirements with the Precise Positioning Service Security Module (U), 12 Mar 98.	3.2.1.5 Global Position System (GPS) Standards
8	IEEE 802.2	Local and Metropolitan Area Networks, Part 2: Logical Link Control, 1994.	3.2.2.2.7 Fiber Distributed Data Interface (FDDI)
9	IETF STD-36/IETF RFC-1390	Transmission of IP and ARP over FDDI Networks, January 1993.	3.2.2.2.7 Fiber Distributed Data Interface (FDDI)
10	ISO 7776	Data Communication High-Level Data Link Control Procedures - Description of X.25 LAPB-compatible DTE Data Link Procedures, 1986.	3.2.2.2.6 X.25
11	ISO 8208	Data Communications - X.25 Packet Layer Protocol for Data Terminating Equipment, 1989.	3.2.2.2.6 X.25
12	ISO 9314-1	Fibre Distributed Data Interface (FDDI) - Pt 1: Token Ring Physical Layer (PHY).	3.2.2.2.7 Fiber Distributed Data Interface (FDDI)
13	ISO 9314-2,	Fibre Distributed Data Interface (FDDI) - Pt 2: Token Ring Media Access Control (MAC).	3.2.2.2.7 Fiber Distributed Data Interface (FDDI)
14	ISO 9314-3	Fibre Distributed Data Interface (FDDI) - Pt 3: Physical Layer Medium Dependent (PMD).	3.2.2.2.7 Fiber Distributed Data Interface (FDDI)
15	ITU-T X.25	Interface Between DTE and DCE for Terminals Operating in the Packet Mode on Public Data Networks.	3.2.2.2.6 X.25
16	IEEE 1320.1-1998,	IEEE Standard for Functional Modeling Language-Syntax and Semantics for IDEF0.	4.2.1 Activity Modeling
17	(No Number)	FORTEZZA Crypto Card ICD, Version P1.5, 22 December 1994.	6.3.1.3 MISSI Cryptographic Algorithms
18	(No Number)	FORTEZZA Plus Crypto Card ICD, Release 3.0, 1 June 1995.	6.3.1.3 MISSI Cryptographic Algorithms

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. (DoD TRM)

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. (DoD TRM)

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 -- (1) Has been sold, leased, or licensed to the general public; or,

(2) Any item that has been offered for sale, lease, or license to the general public (a more complete definition is provided in FAR --Part 2; Definition of Words and Terms; (FAC 97-14); 1 October 1999).

(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 competitively, in substantial quantities, in the commercial 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 service 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.

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.

Engagement Domain

An environment that is primarily based on the command and control of weapons systems and designed to facilitate rapid identification and judgment based on the need to engage or not to engage.

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)

Force Domain

An environment that is primarily based on the command and control (management of the battlespace) of units and forces.

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 will 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 will 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 Open Group/Motif® style guide. Motif® 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.

(a) Any previously developed item of supply used exclusively for governmental purposes by a Federal agency, a State or local government, or a foreign government with which the United States has a mutual defense cooperation agreement;

(b) Any item described in paragraph (a) of this definition that requires only minor modification or modifications of a type customarily available in the commercial marketplace in order to meet the requirements of the procuring.

Open Group

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.

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)

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)

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. (DoD TRM)

Time Criticality

Systems where no perceptible 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).

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 – COMBAT SUPPORT AND SUSTAINMENT DOMAIN

D.1 DOMAIN OVERVIEW

D.1.1 Purpose

This appendix builds on the JTA- Army core mandates by identifying additional standards specifically for the Combat Support and Sustainment (CS-S) Domain (see Section 1.2.2 for the Core vs. Domain standards relationship). It is being developed to help CS-S elements plan and migrate toward a common technical architecture to move, interface and share information.

D.1.2 Background

There are numerous elements using their own communications, systems and applications to support Warfighter activities. To have compatibility and interoperability, DoD and Army information technology managers are establishing standards to be implemented in new and existing architectures for CS-S information systems.

D.1.3 Domain Description

The Combat Support and Sustainment Domain addresses those specific elements necessary for the production, use, or exchange of information within and among systems supporting personnel, logistics, and other functions required to maintain operations or combat. The Combat Support and Sustainment Domain consists of automated systems that perform combat service support and administrative business functions, such as acquisition, finance, human resources management, legal, logistics, transportation and medical functions.

D.1.4 Scope and Applicability

The Combat Support and Sustainment Domain appendix identifies standards applicable to DoD Combat Support and Sustainment Elements, e.g., Logistics, EDI, Continuous Acquisition & Life-Cycle Support (CALS), Medical, Transportation.

D.1.5 Technical Reference Model

This domain uses the DoD Technical Reference Model (TRM) cited in Section 2.1.3 as its framework. Combat Support and Sustainment Application Platform Entity service areas are addressed in Appendix D.2 as domain specific standards. Additional Application Software Entity service areas required to support Combat Support and Sustainment Domain systems are addressed in Appendix D.3 as Domain Specific Service Areas.

D.1.6 Appendix Organization

The Combat Support and Sustainment Domain appendix consists of three sections. Appendix D.1 contains the overview. Appendix D.2 contains those information technology standards that are domain specific standards related to the core, and Appendix D.3 is reserved for those mandates for combat support and sustainment that are domain specific because they do not map directly to the core service areas.

D.2 DOMAIN SPECIFIC STANDARDS

D.2.1 Introduction

The Combat Support and Sustainment Domain embraces the principles established in Section 2. Only those paragraphs from the core that have domain specific standards are included below.

D.2.2 Information Processing Standards

D.2.2.1 Mandates

D.2.2.1.1 Document Interchange (Refer to Section 2.2.2.1.4.1 Document Interchange)

Continuous Acquisition and Life-Cycle Support (CALS) has developed a set of standards that apply to this service area. CALS SGML profiles the ISO standard (8879) by selecting a particular Document Type Definition (DTD) and other parameters that help standardize the development of technical manuals for DoD. CALS also developed a handbook for applying CALS SGML (MIL-HDBK-28001, 30 June 1995). Although Hypertext Mark-up Language (HTML) is also a subset of SGML, it is not sufficiently robust enough for TM development. (eXtensible Mark-up Language (XML) may replace both CALS SGML and HTML in the future.) CALS also has a standard for archiving documents (1840C). The mandated standards for the CALS Document Interchange BSA are:

- MIL-PRF-28001C, Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text. (CALS SGML), 2 May 1997.
- MIL-STD-1840C, Automated Interchange of Technical Information (AITI), 26 June 1997.

D.2.2.1.2 Graphics Data Interchange (Refer to Section 2.2.2.1.4.2 Graphics Data Interchange)

CALS has developed a metadata standard, MIL-PRF-28003A, which profiles the ISO Computer Graphics Metafile (CGM) standard (ISO 8632). Also, a CALS Raster Standard, MIL-PRF-28002C, puts raster graphics into a binary format. The mandated standards for the CALS Graphics Data Interchange service area are:

- ANSI/ISO/IEC 8632 Information Technology - Computer Graphics - Metafile for the Storage and Transfer of Picture Description Information [part 1:1992 Functional Specifications (with amendment 1:1994 Rules for Profiles and with amendment 2:1995 Application Structuring Extensions)] and [part 3:1992 Binary Coding (with amendment 1:1994 Rules for Profiles and with amendment 2:1995 Application Structuring Extensions)] as profiled by MIL-PRF-28003A dated 15 November 1991 with Amendment 1 dated 14 August 1992, Performance Specification, Digital Representation for Communications of Illustration Data: CGM Application Profile.
- MIL-PRF-28002C, Performance Specification, Requirements for Raster Graphics Representation in Binary Format, 30 September 1997.

The Medical Community has developed a standard for digital image transfer. The following mandatory standard applies to the Medical Imagery Data Interchange BSA:

- NEMA/ACR Digital Imaging and Communications in Medicine (DICOM), PS 3.1-1999 through PS 3.14-1999..

D.2.2.1.3 Product Data Interchange (Refer to Section 2.2.2.1.5.5 Product Data Interchange)

Several standards exist for exchanging product data. The ANSI/US PRO/IPO-100-1996 and MIL-PRF-28000B standards for Initial Graphics Exchange Specification (IGES), define a neutral data format that allows the digital exchange of information between computer-aided design (CAD) and computer-aided manufacturing (CAD/CAM) systems. IGES supports digital design and manufacturing information about an object sufficient to support manufacturing and construction only. MIL-PRF-28000A contains applications subsets and protocols that form profiles of IGES Version 4.0. The following standards are mandated:

- ANSI/US Product Data Association (PRO)-100-1996, Initial Graphics Exchange Specification (IGES), V5.3, 23 September 1996.
- MIL-PRF-28000A with Amendment 1, Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols, 14 December 1992.

A standard for circuit board description in digital form is ANSI/IPC-D-350D. An associated standard for describing hardware product data in an unambiguous way is FIPS PUB 172-1; which adopts ANSI/IEEE 1076 and includes valuable interpretations of the adopted standard. Other product data can be stored digitally using MIL-STD-1840C. The following standards are mandated:

- ANSI/PC-D-350D, Printed Board Description in Digital Form, July 1, 1992.
- FIPS Pub 172-1, VHSIC Hardware Description Language (VHDL), 27 January 1995.
- ANSI/IEEE 1076, 1993, IEEE Standard VHDL Language Reference Manual.
- MIL-STD-1840C, Automated Interchange of Technical Information, 26 June 1997.

Bar code standards are used to identify packages and products. They can be used to help identify products being shipped and stocked. MIL-STD-1189B was canceled, but the notice directed the user to AIM BC-1, a linear bar code standard. The following linear (one dimensional) standard is mandated:

- ANSI/AIM BC-8, Uniform Symbology Specification PDF 417, July 1994.

In 1995, the DoD mandated the use of two-dimensional bar code symbology for certain logistics applications. More recently two-dimensional bar codes have been used for certain logistics applications. More recently two-dimensional bar codes have been used on ID cards. In order to standardize two dimensional barcode usages the following standard is mandated for Army business system use:

- ANSI/AIM BC-8, Uniform Symbology Specification PDF 417, July 1994.

D.2.2.1.4 Electronic Data Interchange (Refer to Section 2.2.2.1.4.11 Electronic Commerce Data Interchange)

Electronic Data Interchange (EDI) is a new service area specializing in the computer-to-computer exchange of business information using a public standard. EDI is a central part of Electronic Commerce (EC). EC is the paperless exchange of business information. FIPS Pub 161-2 establishes the Federal EDI Standards Management Coordinating Committee (FESMCC) to harmonize the development of EDI transaction sets and message standards among Federal agencies, and the adoption of Government-wide implementation conventions. The Federally

approved implementation conventions may be viewed on the Web at: <http://www.antd.nist.gov/fededi/l>.

The DoD EDI Standards Management Committee (EDISMC) was established for the purpose of coordinating EDI standardization activities within DoD. The EDISMC supports the development, adoption, publication, and configuration management of EDI implementation conventions for DoD. The DoD EDISMC manages the efforts of several functional working groups (FWG). DoD FWGs have been established in the following areas: logistics, finance, healthcare, transportation, procurement, and communications, command and control. EDISMC-approved implementation conventions are submitted to the FESMCC for approval as Federal implementation conventions. DoD-approved implementation conventions may be viewed on the Web at: <http://www-edi.itsi.disa.mil>.

FIPS PUB 161-2, 22 May 1996, Electronic Data Interchange (EDI) adopts, with specific conditions, ANSI ASC X12, UN/EDIFACT and ANSI HL7. The following standards are mandated as profiled by FIPS PUB 161-2:

- ANSI ASC X12 Electronic Data Interchange (ASC X12S 97-372 is latest edition).
- ISO UN/EDIFACT.

Health Level Seven (HL7) is the EDI standard for healthcare environments. The HL7 version in FIPS 161-2 is obsolete. The following HL7 Standard is mandated for medical EDI:

- ANSI HL7 Health Level Seven Standard Version 2.4 Application Protocol for Electronic Data Interchange in Healthcare Environments, October 6, 2000.

D.2.2.1.5 Geospatial Data Interchange (Reference Section 2.2.2.1.4.3 Geospatial Data Interchange)

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 and 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.2.2.1.6 Configuration Management Data Interchange

A new standard, MIL-STD-2549, has been developed to provide for electronic exchange of configuration management data. It is meant to replace MIL-STD-973 when procuring configuration management information. The following standard is mandated for use:

- MIL-STD-2549, Department of Defense Interface Standard, Configuration Management Data Interface, 30 June 1997.

D.2.2.1.7 Data Interchange Services for Automatic Test Systems (ATS)

D.2.2.1.7.1 Instrument Driver API Standards

The DRV is the interface between the generic instrument class serving the test procedure and the instrument driver. The calls made available at this interface include calls oriented to software housekeeping, such as initializing the driver itself; and calls that cause the instrument to perform a function, such as arm and measure commands. The service requests crossing this interface are communications between generic ATS assets (e.g., digital multimeter) and specific ATS assets (e.g., vendor XYZ model 123 digital multimeter). The instruments are ATS assets, but the calls to the driver are either direct or close-to-direct consequences of action requests in the Test Procedure, which is a Test Program Sets (TPS) asset. Some instrument functions are available from a variety of instruments. However, the driver calls to access these functions vary from instrument to instrument. This interferes with TPS portability. Historically, cross-platform incompatibilities—in the way drivers for the same instrument implement the same function—have been a recurring ATS integration problem. In common commercial practice, the driver is acquired with the instrument from the instrument's original equipment manufacturer. The DRV API interface allows software developed by different organizations to work together. The following standard is mandated:

- VPP-3.2, VXIplug&play Systems Alliance Instrument Driver Functional Body Specification, Revision 4.0, 2 February 1996.

D.2.2.1.7.2 Digital Test Data Formats

Digital Test Data Formats (DTFs) describe the sequence of logic levels necessary to test a digital Units Under Test (UUT). Digital test data is generally divided into four parts: patterns, timing, levels, and circuit models and component models used for the fault dictionary. In addition, certain diagnostic data may exist that is closely associated with the digital test data. This interface is intended to be used for capturing the output of digital automatic test pattern generators. A standard for describing DTF, known as LSRTAP, has become a de facto industry standard. The following standard is mandated:

- IEEE 1445-1998, Standard for Digital Test Interchange Format (DTIF).

D.2.2.2 Emerging Standards

D.2.2.2.1 Product Data Interchange

ISO10303, commonly called Standard for the Exchange of Product Model Data (STEP), is a standard for the computer-interpretable representation and exchange of product data. STEP provides a neutral mechanism capable of exchanging product data between different computer-aided engineering (CAE), and CAD/CAM applications. STEP supports the entire life cycle of a product, independent from any particular system and supports 3D geometry, including 3D wireframe and 3D solid geometry. The following portions of STEP, ISO 10303, Industrial Automation Systems and Integration - Product Data Representation and Exchange are emerging:

- ISO 10303, Industrial Automation Systems and Integration - Product Data Representation and Exchange; Part 1, Overview and fundamental concepts, 1994; Part 11, Description methods: The EXPRESS language reference manual, 1994; Part 12, Description methods: The EXPRESS-I language reference manual, 1997; Part 21, Implementation methods: Clear text encoding of the exchange structure, 1994; Part 22, Implementation.

methods: Standard data access interface specification, 1998; Part 31, Conformance testing methodology and framework: General concepts, 1994; Part 32, Conformance testing methodology and framework: Requirements on testing laboratories and clients, 1998; Part 41, Integrated generic resources: Fundamentals of product description and support, 1994; Part 42, Integrated generic resources: Geometric and topological representation, 1994; Part 43, Integrated generic resources: Representation structure, 1994; Part 44, Integrated generic resources: Product structure configuration, 1994; Part 45, Integrated generic resources: Materials, 1998; Part 46, Integrated generic resources: Visual presentation, 1994; Part 47, Integrated generic resources: Shape variation tolerances, 1997; Part 49, Integrated generic resources: Process structure and properties, 1998; Part 101, Integrated application resources: Draughting,1994; Part 105, Integrated application resources: Kinematics, 1996; Part 201, Application protocol: Explicit draughting (equivalent to IGES), 1994; Part 202, Application protocol: Associative draughting, 1996; Part 203, Application protocol: Configuration controlled design, 1994; Part 224, Application protocol: Mechanical product definition for process planning using machining features, 1999.

Effective use of STEP to share product model data for systems requires a companion standard, ISO/IEC 13584 to exchange CAD Part Libraries (PLIB). The PLIB supplies a data model of the supplier part library, supplier identification, and part geometry. The following standard is emerging:

- ISO/IEC 13584:1998, Industrial Automation Systems and Integration - Parts Library - Part 20; Logical Resource: Logical Model of Expressions; Part 42: Description Methodology: Methodology for Structuring Part Families.

MIL-PRF-28000B - A profile of IGES 5.3. This CALS profile is based on the Y2K-compliant version of IGES and will require all IGES data files to be submitted in a Y2K-compliant format. The following standard is emerging for IGES:

- MIL-PRF-28000B, Digital Representation for Communication of Product Data: IGES Application Subsets and IGES Application Protocols (Draft), 1 July 1999.

The DoD is using Radio Frequency Identification (RFID) to track logistics shipments and other business process used. In order to support interoperability and affordability among RFID vendors, a standard for an Application Programming Interface (API) for RFID software command sets has been developed and is used by several equipment vendors. The following standard is emerging for RFID:

- ANSI NCITS 256, Non-Contact Information Technology Standard 256, 1999.

D.2.3 Information Transfer Standards

D.2.3.1 Mandates

D.2.3.1.1 Instrument Communication Manager Standards for ATS

The Instrument Communication Manager (ICM) interface includes bus-specific options for communicating from the instrument driver to a supporting input/output (I/O) library. Until recently, vendors of IEEE-488 and VME Extensions for Instrumentation (VXI) bus hardware provided software drivers for their buses that were different according to the hardware bus protocol or operating system (OS) used. This situation interfered with the plug-and-play capabilities that users thought they were going to get from buying different instruments that all communicated by common hardware protocols. The same functions of the same instruments were not accessed through software in the same way across buses and host platforms. Different manufacturers of IEEE-488 cards had proprietary and unique software calls. Furthermore,

leading vendors of VXI Slot 0 cards and embedded controllers used different I/O calls to access instruments. This impeded the transporting of instrument drivers, Application Development Environments (ADEs), and test programs from one set of hardware to another. Without a standard ICM interface, vendors cannot provide interoperable or portable instrument drivers because different vendors would use different I/O drivers at the very lowest layer of the software. This forces instrument drivers to be tailored to specific I/O calls for each test station and lowers the likelihood that instrument drivers will be commercially available for each configuration. In addition, standard I/O software allows one to place parameters such as bus addresses and instrument addresses in the instrument driver instead of the test program. A standard ICM interface enables higher-level software to be interoperable and portable between vendors and across different platforms. This improves the interoperability of test software and the ability to re-host test software from one test system to another. The following standard is mandated:

- VPP-4.3, VXIplug&play (VPP) Systems Alliance Virtual Instrument Standard Architecture (VISA) Library, 22 January 1997.

D.2.3.2 Emerging Standards

There are no domain specific emerging standards for the Combat Support and Sustainment Information Transfer Standards section.

D.2.4 Information-Modeling, Metadata, and Information-Exchange Standards.

There are no domain specific mandates or emerging standards for the Combat Support and Sustainment Information-Modeling, Metadata, and Information-Exchange Standards section.

D.2.5 Human-Computer Interface Standards

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 CS-S 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 (DII), Version 4.0, October 1999.

D.2.6 Information Systems Security Standards

EC/EDI have security services associated with ANSI ASC X12 transactions. ANSI ASC X12.58 is a description of that security but is not mandated.

D.3 DOMAIN SPECIFIC SERVICE AREAS

D.3.1 Introduction

D.3.1.1 Mandated Standards

D.3.1.1.1 Smart Card Technology Standards for Electronic Business/Electronic Commerce

Smart Card standards are derived from identification-card standards and detail the physical, electrical, mechanical and application programming interface. ISO 7816 series is for contact Smart Cards while ISO 10536 specifies the standards for various types of contactless Smart Cards. Smart-Card standards are essential for interoperability between multivendor cards and readers. The following ISO/IEC Series Standards for Smart Cards are mandated:

- ISO/IEC 7816 Identification Cards - Integrated Circuit(s) cards with contacts; Part 1, Physical characteristics, October 1998; Part 2, Dimensions and location of the contacts, March 1999; Part 3, Electronic signals and transmission protocols, December 1997; Part 4, Interindustry commands for interchange, September 1995; Part 5, Numbering system and registration procedure for application identifiers, June 1994; Part 6, Interindustry Data Elements, May 1996; Part 7, Interindustry commands for Structured Card Query Language (SCQL), March 1999.
- ISO/IEC 10536 Identification Cards - Contactless integrated circuit(s) card; Part 1, Physical characteristics, September 1992; Part 2, Dimensions and location of coupling areas, December 1995; Part 3, Electronic signals and reset procedures, December 1996.

D.3.1.1.2 System Framework Standards for ATS

System frameworks provide a common interface for developers of software modules, ensuring that they are portable to other computers that conform to the specified framework. By defining system frameworks, suppliers can focus on developing programming tools and instrument drivers that can be used with any ADE that is compliant with the framework. System frameworks contain, but are not limited to, the following components:

1. Compatible ADEs.
2. Instrument Drivers.
3. Operating System.
4. Required Documentation and Installation Support.
5. Requirements for the Control Computer Hardware.
6. Soft Front Panel.
7. VISA Interface and I/O Software.
8. VXI Instruments, VXI slot0, System Controller, VXI Mainframe.

A system designed using a VXIplug&play system framework ensures that the ADE, DRV, GIC, ICM, and other FRM components are compatible and interoperable with each other. Following the system framework requirements also ensures that all necessary system components have been included, resulting in a complete and operational system. System frameworks increase the likelihood that ADEs will be available on multiple platforms, greatly enhancing the ability to move test software between platforms. While this does not ensure total portability of TPSs, it

does eliminate the need to translate or rewrite the source code when it is ported. The following standard is mandated:

- VPP-2, VXIplug&play System Alliance System Frameworks Specification, Revision 4.0, 29 January 1996.

D.3.1.2 Emerging Standards

There are no emerging standards for this section.

This page was intentionally left blank.

APPENDIX E - COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C3I) DOMAIN

E.1 DOMAIN OVERVIEW

E.1.1 Purpose

This appendix builds on the JTA-Army core mandates by identifying C3I Domain specific standards to include information standards and analogous standards applicable to C3I (see Section 1.2.2 for relationships between core and domain standards).

E.1.2 Background

E.1.3 Domain Description

The C3I domain consists of those integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications whose primary focus is on one or more of the following functions:

1. Support properly designated commanders in the exercise of authority and direction over assigned and attached forces across the range of military operations.
2. Collect, process, integrate, analyze, evaluate, or interpret available information concerning the area of operations.

This appendix will specifically address the information technology aspect of the C3I domain.

E.1.4 Scope and Applicability

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

E.1.5 Technical Reference Model

There is no separate Technical Reference Model established for the C3I Domain.

E.1.6 Appendix Structure

This appendix is divided into three sections: the Domain Overview in Appendix E.1, the Domain Specific Standards in Appendix E. 2, and the Domain Specific Services Areas in Appendix E. 3.

E.2 DOMAIN SPECIFIC STANDARDS

E.2.1 Introduction

E.2.2 Information Processing Standards

There are no domain specific mandates or emerging standards to the standards in the main body of the JTA-Army.

E.2.2.1 Mandates

E.2.2.1.1 Still-Imagery Data Interchange

There are no information processing standards mandated in the C3I domain.

E.2.2.2 Emerging Standards

There are no emerging information processing standards for the C3I Domain.

E.2.3 Information Transfer Standards

E.2.3.1 Mandates

E.2.3.1.1 End System Standards

E.2.3.1.1.1 Secondary Imagery Dissemination Standards (Refer to Section 3.2.1.4 Imagery Dissemination Communications Standards)

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 is 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, with Notice of Change 1, 29 July 1994; and Notice of Change 2, 27 June 1996.

E.2.3.1.2 Network Standards

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

E.2.3.1.3 Transmission Media (Refer to Section 3.2.3 Transmission Media)

E.2.3.1.3.1 Military Satellite Communications (MILSATCOM) (Refer to Section 3.2.3.1 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 consist 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.2.3.1.3.1.1 Ultra High Frequency (UHF) Satellite Terminal Standards

E.2.3.1.3.1.1.1 5-kilo-Hertz (kHz) and 25-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-188-181B, Interoperability Standard for Single Access 5-kHz and 25-kHz UHF Satellite Communications Channels, 20 March 1999.

E.2.3.1.3.1.1.2 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-188-182A, Interoperability Standard for 5 kHz UHF DAMA Terminal Waveform, 31 March 1997, with Notice of Change 1, 9 September 1998; and Notice of Change 2, 22 January 1999.

E.2.3.1.3.1.1.3 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-188-183A, Interoperability Standard for 25 kHz UHF/TDMA/DAMA Terminal Waveform, 20 March 1998; with Notice of Change 1, 9 September 1998.

E.2.3.1.3.1.1.4 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, with Notice of Change 1, 9 September 1998.

E.2.3.1.3.1.1.5 Demand Assigned Multiple Access (DAMA) Control System

For the minimum mandatory interface requirements for MILSATCOM equipment that control access to DAMA UHF 5-kHz and 25-kHz MILSATCOM channels, the following standard is mandated:

- MIL-STD-188-185, DoD Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System, 29 May 1996, with Notice of Change 1, 1 December 1997; and Notice of Change 2, 9 September 1998.

E.2.3.1.3.1.2 Super High Frequency (SHF) Satellite Terminal Standards

E.2.3.1.3.1.2.1 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, with Notice of Change 1, 9 September 1998.

E.2.3.1.3.1.2.2 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, with Notice of Change 1, 9 September 1998.

E.2.3.1.3.1.3 Extremely High Frequency (EHF) Satellite Payload and Terminal Standards

E.2.3.1.3.1.3.1 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-1582D, EHF LDR Uplinks and Downlinks, 30 September 1996; with Notice of Change 1, 14 February 1997, and Notice of Change 2, 17 February 1999.

E.2.3.1.3.1.3.2 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-188-136A, EHF MDR Uplinks and Downlinks, 8 June 1998.

E.2.3.1.3.2 Radio Communications (Refer to Section 3.2.3.2 Radio Communications)

E.2.3.1.3.2.1 High Frequency (HF)

E.2.3.1.3.2.1.1 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-188-141B, Interoperability and Performance Standards for Medium and High Frequency Radio Systems, 1 March 1999.

E.2.3.1.3.2.1.2 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.2.3.1.3.2.1.3 Data Modems

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

- MIL-STD-188-110B, Interoperability and Performance Standards for Data Modems, 27 April 2000.

E.2.3.1.3.2.2 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.2.3.1.3.2.3 Anti-Jamming Capability

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

- STANAG 4246, Edition 2, HAVE QUICK UHF Secure and Jam-resistant Communications Equipment, 17 June 1987; with Amendment 3, August 1991.

E.2.3.1.3.2.4 Link 16 Transmission Standards

When communicating with the Joint Tactical Information Distribution System (JTIDS)/Multi-Functional Information Distribution System (MIDS) radios, the following standards are mandated:

- STANAG 4175, Edition 1, Technical Characteristics of the Multifunctional Information Distribution System (MIDS), lt 29 August 1992, (U).

E.2.3.2 Emerging Standards

There are no domain specific emerging standards.

E.2.4 Information-Modeling, Metadata, and Information-Exchange Standards

E.2.4.1 Tactical Information Exchange Standards (Bit Oriented Formatted Messages)

E.2.4.1.1 Sensor Link Protocol (SLP) Message Set

The Sensor Link Protocol (SLP) was developed for use as a common interface between electro-optical sensor systems and a diverse set of host computer systems. The SPL message set is decoupled from lower layer protocols to allow implementers the flexibility to select from a number of open standards such as RS-232/485, FireWire or USB. The SLP message set is used in conjunction with the SLP Interface Control Document to develop a common digital data exchange mechanism between sensors and host computing devices that offer full remote operation and control of those sensors by a host-computing device in both a point-to-point and networked environment. The following emerging standard defines the SLP message set:

- SLP-MSG-210, Revision, Sensor Link Protocol Message Set, 26 March 2001.

E.2.5 Human-Computer Interfaces

There are no additional domain specific mandates or emerging standards to the standards in the main body of the JTA-Army.

E.2.5.1 Mandates

There are no domain specific mandated standards.

E.2.5.1.1 Domain-Level Style Guides (Refer to Section 5.2.2.3 Domain-level Style Guides)

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 (DII), Version 4.0, October 1999.

E.2.5.2 Emerging Standards

There are no domain specific emerging standards.

E.2.6 Information Security

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

E.3 DOMAIN SPECIFIC SERVICE AREAS

E.3.1 Introduction

E.3.1.1 Mandated Standards

There are no domain specific mandated standards.

E.3.1.2 Emerging Standards

E.3.1.2.1 Internal Communications

Internal communications provide information-transfer capabilities between the platform and the onboard C3I systems, subsystems, and components. This section identifies the standards necessary to facilitate interoperability within and between these entities.

E.3.1.2.1.1 Fibre Channel

Fibre Channel is an ANSI standard, high-speed, reliable, data transfer technology that operates over copper wire and fiber optic cabling. Fibre Channel can operate at up 1G bps at a distance of up to 10 kilometers; making it a suitable candidate for bandwidth-intensive applications such as data warehousing, imaging, integrated audio/video, real-time computing, and collaborative planning. Fibre Channel is capable of carrying multiple existing protocols including IP, SCSI and ATM and can connect several topologies such as point-to-point, arbitrated-loop, and switching thereby enabling it to support LANs, WANs and enterprise networks as well as legacy networks. C3I systems that have requirements for real-time data exchange, storage based networks (Storage Area Networks), Redundant Arrays of Independent Disks (RAID) and digital audio/video networks should consider Fibre Channel technology. The emerging standards are:

- ANSI X3.230-1994, Information Technology – Fibre Channel – Physical and Signaling Interface (FC-PH).
- ANSI X3.230-1994/AM 1-1996, Information Technology – Fibre Channel – Physical and Signaling Interface (FC-PH) – Amendment 1.

E.3.1.2.1.2 FireWire

FireWire is a commercial standard, high-speed, plug-and-play, serial bus that provides a low cost alternative to parallel and serial I/O ports contained in a computer. FireWire can be used to connect cards (on the same backplane or on other backplanes) or up to 63 external peripheral devices like digital cameras and audio devices, digital videocassette recorder (VCRs), optical drives, hard disk drives, and sensors, providing speeds between 100M and 400M bps. The following emerging standard is applicable:

- IEEE 1394-1995, IEEE Standard for a High Performance Serial Bus.

This page was intentionally left blank.

APPENDIX F - WEAPON SYSTEMS DOMAIN (WSD)

F.1 INTRODUCTION

A Weapon System is defined as 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. (Joint Pub 1-02)

A domain is defined as a distinct functional area that can be supported by a family of systems (FoS) with similar requirements and capabilities. The Weapon Systems Domain (WSD) encompasses the family of systems whose primary function is that of supporting attack and/or defense against an adversary, and that are intentionally designed to interoperate with other weapon systems and/or with systems external to the (WSD).

Weapon Systems have special attributes (e.g. timeliness, embedded nature, space and weight limitations), adverse environmental conditions, and critical requirements (e.g., survivability, low power/weight, and dependable hard real-time processing) that drive highly interdependent and interrelated system hardware and software. Weapon systems operations can be identified as operations in the Force Domain and operations in the Engagement Domain. Engagement Domain operations are real-time or near real time. Force Domain operations are involved in the support of the operation, and are typically non-real-time or near real time. Figure F-1 provides an example of the unique and varying regimes of real-time processing requirements for typical weapon system operations, but does not necessarily represent the sequencing of functions.

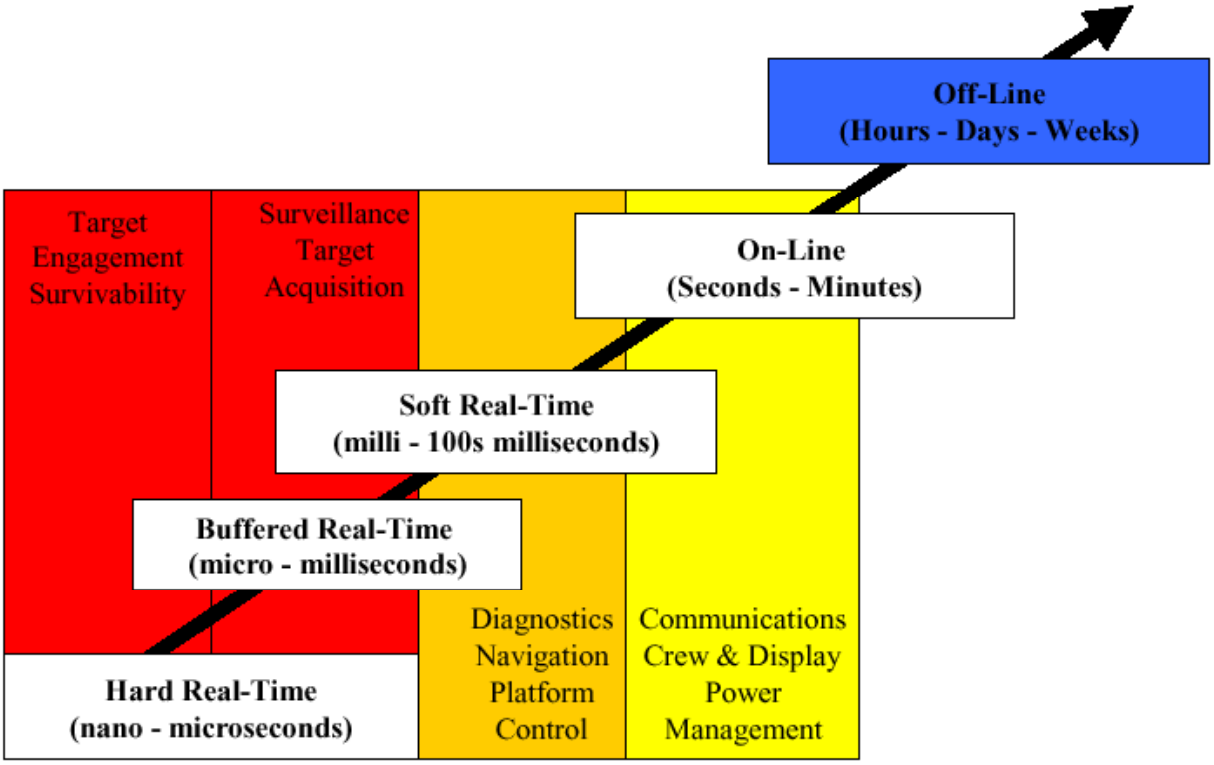


FIGURE F-1. REALM OF WEAPON SYSTEM FUNCTIONAL TIME REGIMES

F.1.1 Purpose

This appendix builds on the JTA-Army core mandates by identifying weapon systems domain specific standards to include information standards and analogous standards applicable to Weapon Systems (see Section 1.2.2 for relationships between core and domain standards).

F.1.2 Scope

The Weapon Systems Domain Appendix is applicable to all weapon systems as defined in Joint Pub 1-02. This appendix, in conjunction with the applicable portions of the JTA-Army core document, establishes the minimum set of rules governing the application of information technology for weapon systems. The JTA-A Weapon Systems Domain is organized into subdomains identified in Figure F-2. This will facilitate the identification of interoperability standards while maintaining the systems' primary design function of supporting attack and/or defense against an adversary. The inclusion or exclusion of subdomains in the Weapon Systems Domain is based on the domain participants' agreement to include or exclude a candidate.

It is important to note that some weapon systems incorporate features/functions associated with more than one subdomain or are integrated, based on operational requirements, into a "system of systems" on the battlefield and therefore developers must also consider applicable standards from the other pertinent subdomains. However, the determination of which standard(s) is (are) applicable, in terms of interoperability and affordability, must be the result of analyzing system requirements (operational architecture) and applying the best solutions (system architectures). ”

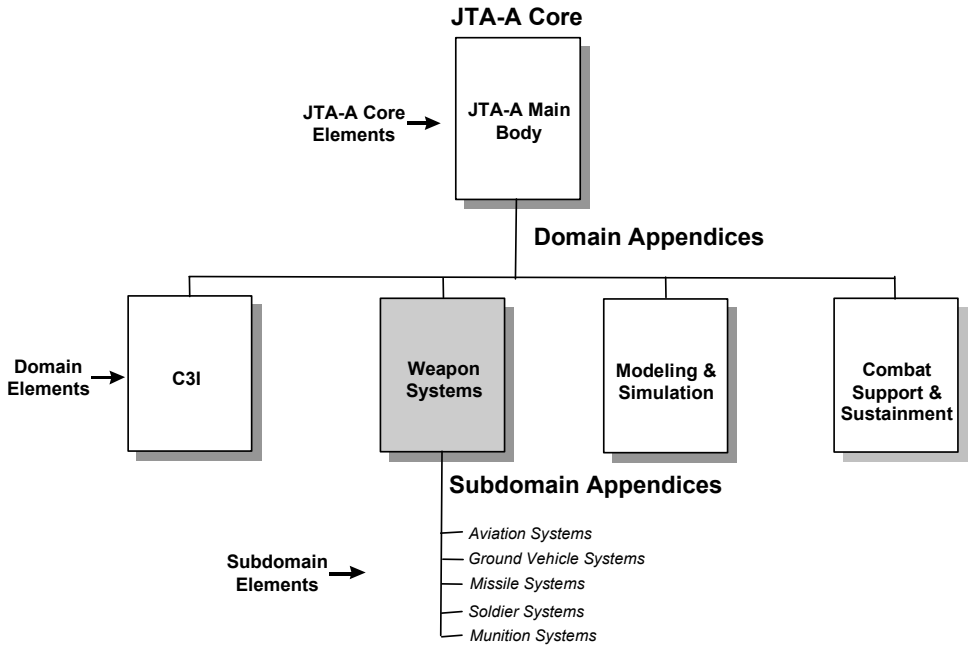


FIGURE F-2. NOTIONAL JTA-ARMY HIERARCHY

As depicted in Figure F-2, the current Weapon Systems subdomains are as follows:

Aviation Systems (AVS) Subdomain

Applies to Army weapon systems integral to aeronautical platforms. Fixed-wing, rotorcraft, manned, and unmanned aeronautical platforms are subject to the standards specified in this subdomain appendix. Excludes missile and munition systems.

Ground Vehicle Systems (GVS) Subdomain

Applies to Army weapon systems integral to mobile ground platforms. Wheeled, tracked, manned, and unmanned vehicles are subject to the standards specified in this subdomain appendix. Excludes missile and munition systems.

Missile Systems (MS) Subdomain

Includes all Army missile and missile defense systems (including associated battle management/command, control, communications, and intelligence (BM/C3I) systems), both strategic and tactical.

Soldier Systems (SS) Subdomain

The Soldier Systems Subdomain includes any system or subsystem integrating target location, identification, acquisition, enhanced survivability, navigation, position location, enhanced mobility or command and control into a system worn or carried by a soldier in performance of their duties.

Munition Systems (MUS) Subdomain

These non-mobile, transportable, weapon systems include, but are not limited to, munitions and munitions integrated with combat sensors, control stations, and the supporting combat communication systems with their repeaters and gateways.

F.1.3 Background

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. The WSTAWG was formed to support the identification, development, and maintenance of unique information standards and related interface specifications for Weapon Systems. The WSTAWG identifies standards based on the DoD TRM to accommodate the requirements of the Weapon Systems Domain. The Weapon Systems Domain Appendix is the vehicle for mandating the standards and APIs identified or developed by the WSTAWG that are considered to be unique to Weapon Systems, and are in addition to those standards identified in the JTA-A core.

F.1.4 Technical Reference Model (TRM)

The Weapon Systems Domain and Subdomains use both the Services and Interfaces Views of the DoD TRM, as shown in Figure F-3, to capture all of the standards required for Weapon Systems to operate within the DoD Enterprise. Section F.2 of the Weapon Systems Domain appendix uses the Services View in identifying domain specific standards relative to the core standards. Section F.3 of the Weapon Systems Domain appendix applies the DoD TRM Interfaces View, and provides a framework to identify classes of interfaces for applying open system interface standards to the design of Weapon Systems' hardware/software components.

F.1.5 Appendix Structure

This appendix is divided into three sections: the Introduction in Appendix F.1, the Domain Specific Standards in Appendix F.2, and the Domain Specific Services and Interfaces in Appendix F.3. Appendix F.2 follows the JTA-Army core structure. The structure of Appendix F.3 follows the structure contained in the DoD TRM Interfaces View.

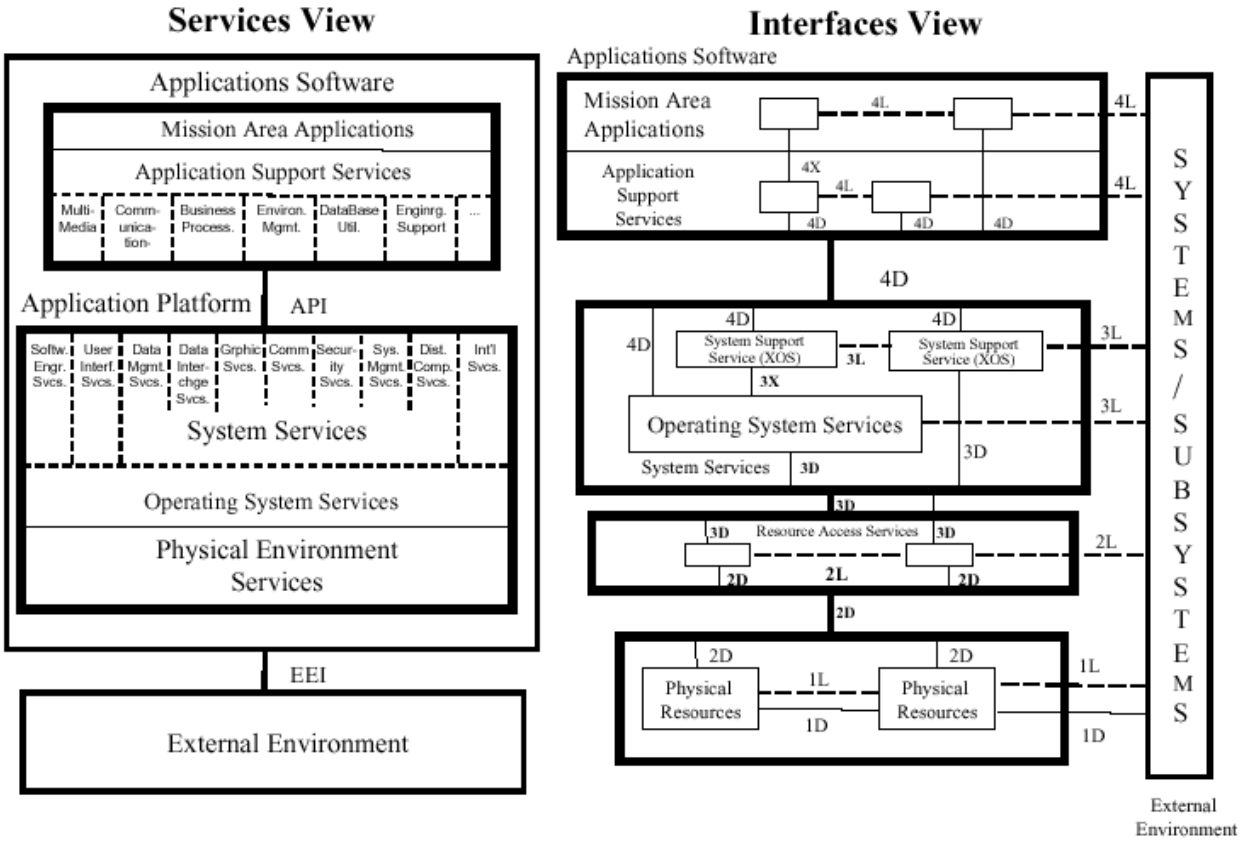


FIGURE F-3. DOD TECHNICAL REFERENCE MODEL SERVICES VIEW AND INTERFACES VIEW

F.2 DOMAIN SPECIFIC STANDARDS

F.2.1 Introduction

The DoD TRM provides for sufficient fidelity to allow identification of critical and common services, functions, interfaces, and technical issues applicable to the Weapon Systems Domain. This section of the Weapon Systems Domain appendix follows the structure of the JTA-Army core. Only those subsections of the JTA-Army core that require domain-specific standards for Weapon Systems are addressed in this section.

F.2.2 Information Processing Standards

F.2.2.1 Mandates

F.2.2.1.1 Operating System Services

The following IEEE standard, which defines Application Environment Profiles for realtime applications utilizing the POSIX® interfaces, is mandated:

- IEEE 1003.13:1998, IEEE Standard for Information Technology, Standardized Application Environment Profile, POSIX® Realtime Application Support.

F.2.2.1.2 Mapping Services

The Weapon System Mapping Services (WSMS) Application Programmer's Interface (API) provides a standardized interface to a set of mapping and mapping related services to be utilized by weapon systems applications in the presentation, interaction, and maintenance of Command, Control, Communications, and Intelligence (C3I) data. This API has been specified in a scaleable, extensible, language independent manner such that it can be tailored to application specific requirements (e.g. level of functionality, programming language, etc.), resulting in an increased potential for application reuse throughout the weapon system subdomains. The WSMS API defines the detailed concepts, functionality, and interfaces required to support the development of both WSMS implementations and applications. In addition, the WSMS API addresses underlying architectural support issues of embedded real time systems such as multitasking, reentrancy, and blocking/non-blocking execution in order to designate the manner in which the WSMS is expected to operate within a weapon system application environment. The following standard is mandated for this section of the Weapon Systems Domain appendix.

- Weapon System Mapping Services (WSMS) Application Programmer's Interface (API), WSTAWG Doc# WSTA-AS-03-01, January 28, 2001.

F.2.2.2 Emerging Standards

F.2.2.2.1 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.

F.2.2.2.2 Mapping Services

The Weapon System Mapping Services (WSMS) Application Programmer's Interface (API) provides a standardized interface to a set of mapping and mapping related services to be utilized by weapon systems applications in the presentation, interaction, and maintenance of Command, Control, Communications, and Intelligence (C3I) data. The following standard is emerging for this section of the Weapon Systems Domain appendix.

- Weapon System Mapping Services (WSMS) Application Programmer's Interface (API), WSTA-AS-03-01, October 2001.

F.2.3 Information Transfer Standards

Information processing nodes and groups of processors within a weapon system are connected by a local network or bus. This network or bus, 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's networks consist of both media access control and point-to-point protocols, and typically have differentially based electrical media or fiber-optic media to provide some inherent electrical noise protection.

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 Appendix F.3.

F.2.3.1 Mandates

F.2.3.1.1 Map Data Loading

The Weapon System Technical Architecture Working Group (WSTAWG) has developed a standard that defines the hardware, software and interface requirements for transferring National Image and Mapping Agency (NIMA) generated map data to weapon system platforms. Use of the standard provides for the timely and effective dissemination of digital mapping data to US Army combat systems. The following standard is mandated:

- Map Data Loading Standard (MDLS), Revision 1.0, February 26, 1998.

F.2.3.2 Emerging Standards

There are no emerging standards identified for the Weapon Systems Domain appendix.

F.2.4 Information-Modeling, Metadata, and Information-Exchange Standards

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-4. Information exchange must occur between each of these phases.

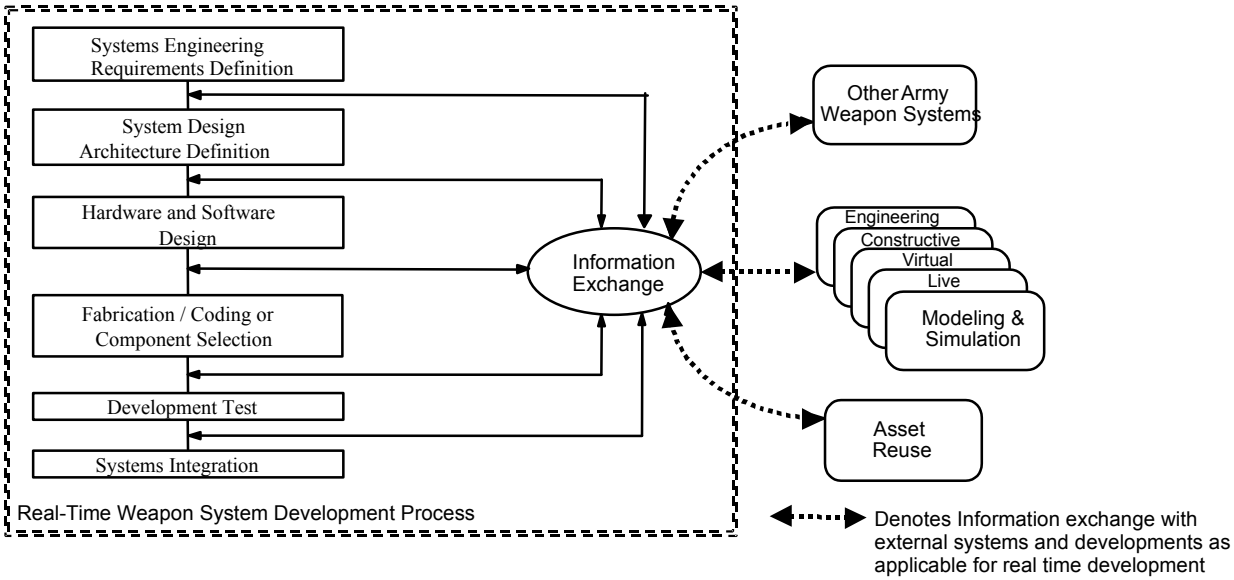


FIGURE F-4. DEVELOPMENT PROCESS RELATIVE TO THE REAL-TIME, EMBEDDED PROCESSING SYSTEM

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.2.4.1 Mandates

The WSTAWG has identified the need for guidance to follow in the creation of APIs for the Weapon Systems Domain. The following standard guidance was approved for release and is mandated for the Weapon Systems Domain:

- U.S. Army Weapon Systems Application Program Interface (API) GuideBook: Volume II - API Specification Style Guide, February 2, 1999.

F.2.4.2 Emerging Standards

There is a need within the Weapon Systems Domain for high order hardware languages that can implicitly relate embedded computing system timing constraints to activity modeling. The following standards are being evaluated as emerging Information-Modeling, Metadata, and Information-Exchange Standards for the Weapon Systems Domain:

- IEEE 1076: 1993, Standard VHSIC Hardware Description Language (VHDL) Reference Manual, 1993 - (VHDL is a high-level hardware language).
- IEEE 1076.2: VHDL Mathematical Package, 1996.

- IEEE 1076.3: Standard VHDL Synthesis Packages, 1997.
- IEEE 1076.4: VITAL Application-Specific Integrated Circuit (ASIC) Modeling Specification, 1995 (Provides VITAL timing and primitives).

F.2.5 Human-Computer Interface Standards

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 (e.g., the design of graphical and character-based displays and controls) across Army 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.

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

> "Systems where no perceptible 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)."

There are some aspects of HCI's that can be common across the Weapon Systems Domain, while others are subdomain specific. Hence, an HCI style guide is required at the weapon systems level, and currently for each of the five subdomains (Aviation Systems, Ground Vehicle Systems, Missile Systems, Soldier Systems, and Munition Systems).

F.2.5.1 Mandates

F.2.5.1.1 Domain-level Style Guide (Refer to Section 5.2.2.3 Domain-level Style Guides)

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, Version 3.0, December 1999.

F.2.5.1.2 Emerging Standards

Currently there are no emerging standards identified for this section of the Weapon Systems Domain appendix.

F.2.5.2 Symbology

Weapons systems require the use of multiple symbology standards to meet platform or system performance requirements. For weapons platforms that require the use of Force Operations, Symbology, MIL-STD-2525B, Common Warfighting Symbology, 30 January 1999 is mandated (see section 5.2.3).

For weapons platforms that require the use of Engagement Operations Symbology to meet safety and performance requirements and approved allied and coalition agreements, the reader should refer to the appropriate subdomain appendix for the applicable standard(s).

F.2.6 Information Systems Security Standards

Currently, there are no domain specific mandated or emerging standards identified for this section of the Weapon Systems Domain appendix.

F.3 DOMAIN SPECIFIC SERVICES AND INTERFACES

F.3.1 Introduction

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 and embedded processing systems must control, sense, and integrate with the hardware environment of the Weapon Systems. A Weapon Systems' hardware environment is generally a custom built electronic or mechanical module. The hardware along with the processing system and applications software must work together to perform unique mission requirements. The level of coupling of the embedded processing system to the hardware environment determines the possibility of modular partitioning. The direct and logical interface semantics, elaborated in the GOA Framework and depicted by the DoD TRM Interfaces View in Figure F-3, provides sufficient fidelity for identifying classes of interfaces to apply open systems interface standards in the design of real-time and embedded hardware/software systems. The Framework also facilitates the identification of critical functions and interfaces within the real-time and embedded computing systems of the Weapon Systems Domain.

This section provides a common framework identifying mandated and emerging embedded computing interface standards associated with the logical and direct interface classes defined for the layers depicted in the DoD TRM.

Only those layers of the DoD TRM Interfaces View, that have domain specific mandated or emerging standards identified, are addressed in this section.

F.3.2 Application Software Layer Interfaces

Currently, there are no mandated or emerging standards identified for this section of the Weapon Systems Domain appendix.

F.3.3 System Services Layer Interfaces

F.3.3.1 Mandates

F.3.3.1.1 Operating Environment Services

The Army WSTAWG Operating Environment (OE) IPT has developed the OE Application Programmer's Interface (API), which provides a standardized interface to a set of distributable objects that can be utilized in the creation of rehostable distributed real time embedded weapon

systems applications. This API has been defined in a scaleable, extensible, language independent manner such that it can be tailored to application specific requirements, resulting in an increased potential for application reuse throughout the Army weapon system domain. The following standard is mandated:

- Weapon Systems Technical Architecture Working Group (WSTAWG) Operating Environment (OE) Application Programmer's Interface (API), Volume I, OE Application Interface, Version 1.4, 13 April 2001.

F.3.3.2 Emerging

F.3.3.2.1 Operating Environment Services

The following standard is emerging:

- Weapon Systems Technical Architecture Working Group (WSTAWG) Operating Environment (OE) Application Programmer's Interface (API), Volume I, OE Application Interface, Version 2.0, 1 October 2001.

F.3.4 Resource Access Services Layer Interfaces

Currently, there are no domain specific mandated or emerging standards identified for this section of the Weapon Systems Domain appendix.

F.3.5 Physical Resources Layer Interfaces

This section identifies the following:

1. The interface standards that provide the requirements for establishing a data interchange interface between Physical Resources and enable bus or communications link boards to address their peers in another node or system, and
2. The interface standards that support the direct connections between Physical Resources, such as those needed to enable busses and communications links to address processors or needed to enable processors to address memory registers.

Included are standards for Serial and Parallel buses. A Serial bus transmits information one bit at a time in a sequential or serial manner. A Parallel bus transfers information (data, interrupts, arbitration, timing, etc.) by sending a number of bits (such as 8 or 16) at the same time using multiconductor cables and connectors. Internal parallel buses include Backplane, Input/Output (I/O), and Single Board Computers (SBC) and Expansion Cards. External parallel buses include peripheral buses.

F.3.5.1 Mandates

F. 3.5.1.1 Parallel Buses

F.3.5.1.1.1 Single Board Computers (SBCs) and Expansion Cards

The PC Card standard will be used by applications requiring hot-swappable peripherals that add memory, mass storage, and I/O capabilities to computers in a rugged, compact form factor. The following standard is mandated:

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

F.3.5.2 Emerging Standards

F.3.5.2.1 Parallel Buses

F.3.5.2.1.1 Single Board Computers (SBCs) and Expansion Cards

PCI (peripheral component interface) is a high-speed local bus being used by several CISC and RISC microprocessors. PCI specification defines a 4.2-inch by 12.3-inch board that plugs into a motherboard in a perpendicular fashion. These perpendicular boards are not usable in many Weapon Systems because they use too much vertical space. The following emerging standard defines the mechanics of a low profile modular horizontal mezzanine card family that uses the logical and electrical layers of the PCI specification for the local bus with I/O accessible via the front panel and/or through the connector to the host computer for rear panel I/O:

- IEEE P1386.1/D2.4, Physical/Environmental layers for Peripheral Component Interface (PCI) Mezzanine Cards (PMC), January 12, 2001.

F.3.6 Combat Identification (CI) Services

Combat Identification (CI) is the process of obtaining an accurate characterization of entities in a combatant's area of responsibility to the extent that high confidence, real-time application of tactical options and weapon resources can occur (Ref: Approved Joint Combat Identification Master Plan, August 1995). CI is the ability to differentiate friend, foe, or neutral, with high confidence, beyond engagement range, and in sufficient time to support successful engagement and weapon release decisions. CI services include Identification Friend or Foe (IFF) and Battlefied Combat Identification (BCI). IFF establishes the identity of friendly systems within the surveillance volume of surface-to-air, air-to-air, and some air-to-ground Weapon System platforms. BCI addresses Air-to-Ground, Ground-to-Air, and Ground-to-Ground scenarios". For Army BCI initiatives, see http://peoiews.monmouth.army.mil/ci/.

F.3.6.1 Mandates

For platforms requiring integrated or appliqué IFF capabilities, the following standards are mandated:

- Aeronautical Telecommunications: Appendix 10 to the Convention on International Civil Aviation, volume IV (Surveillance radar and Collision Avoidance Systems), Edition 1, International Civil Aviation Organization (ICAO): Montreal, 1995, with Supplements (31 May 1996 and 10 November 1997).
- DOT FAA 1010.51A, US National Aviation Standard for the Mark X (SIF) Air Traffic Control Radar Beacon system (ATCRBS) Characteristics, 8 March 1971.
- DoD AIMS 97-1000, Performance/Design and Qualification Requirements Technical Standard For The ATCRBS/IFF/MARK XII Electronic Identification System and Military Mode S, 18 March 1998.
- DoD AIMS 97-900, Performance/Design and Qualification Requirements Mode 4 Input/Output Data, 18 March 1998.

F.3.6.2 Emerging Standards

NATO STANAG 4579 defines criteria for an interoperable NATO Battlefield Target Identification Device (BTID) for identification of forces on the battlefield. For platforms requiring BCID capabilities, the following standard is emerging:

- STANAG 4579, Battlefield Target Identification Devices, 22 March 2000

APPENDIX F.AVS - AVIATION SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN

F.AVS.1 INTRODUCTION

A weapon system is 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. The Aviation Systems Subdomain applies to Army weapon systems that are integral to aeronautical platforms. Fixed-wing, rotorcraft, manned, and unmanned aeronautical platforms are subject to the standards specified in this subdomain appendix. Specifically, this includes the following elements: Air Cavalry/Reconnaissance, Attack, Utility, Medevac, Cargo, Fixed Wing, Command and Control, and Support Programs and Equipment. Within these elements the functions would be grouped as follows: 1) systems Operations and Control, 2) C3I, 3) Lethality and Survivability, and 4) Mission Support and Sustainment. The on-board hardware is categorized in the following manner: 1) Processing Resources, 2) Power Generation and Management Equipment, 3) Controls and Displays, 4) Data Distribution, and 5) Support Electronics. Excluded are missile and munition systems. Aviation systems have explicit real-time processing requirements. The platform-centric Figure F.AVS-1 illustrates the various time regimes for executing basic Rotary-Wing Aviation system functions in an operational environment. The time regimes depicted are weapon-centric, and do not include time associated with external systems. Real-time indicates that processing operations must be executed in a repeatable, predictable and deterministic timeframe.

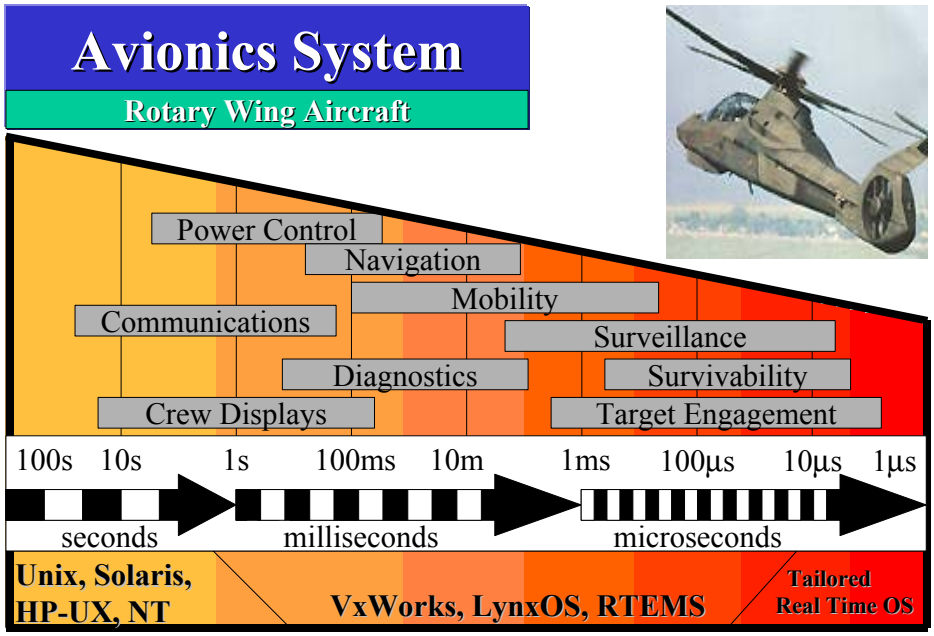


FIGURE F.AVS-1. AVIATION SYSTEMS FUNCTIONAL TIME REGIMES

F.AVS.1.1 Purpose

This subdomain builds on Appendix F by identifying Aviation Systems Subdomain specific standards to include information standards and analogous standards applicable to Aviation Systems (see Section 1.2.2 for relationships between core, domain, and subdomain standards).

F.AVS.1.2 Scope

The scope of this subdomain appendix is the entire Army Aviation Systems Subdomain as defined in Appendix F.AVS.1.

F.AVS.1.3 Background

The standards in this subdomain are based on the work performed by the Army Weapon Systems Technical Architecture Working Group (WSTAWG).

F.AVS.1.4 Technical Reference Model (TRM)

The Technical Reference Model used in this subdomain is the DoD TRM that is described in the Weapon Systems Domain appendix.

F.AVS.1.5 Appendix Structure

This appendix is divided into three sections: the Introduction in Appendix F.AVS.1, the Subdomain Specific Standards in Appendix F.AVS.2, and the Subdomain Specific Services and Interfaces in Appendix F.AVS.3. Appendix F.AVS.2 follows the JTA-Army core structure. The structure of Appendix F.AVS.3 follows the structure contained in the DoD TRM Interfaces View.

F.AVS.2 SUBDOMAIN SPECIFIC STANDARDS

F.AVS.2.1 Introduction

This section identifies the subdomain specific mandated and emerging standards for the Aviation Systems Subdomain appendix, in addition to those standards identified in the WSD Appendix and the JTA-A core.

F.AVS.2.2 Information Processing Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Aviation Systems Subdomain appendix.

However, the Army Science Board Army Avionics Modernization Methodologies study concluded that the core Operating System Services' mandates in section 2.2.2.1.7 are not applicable for many Aviation systems.

F.AVS.2.2.1 Mandates

F.AVS.2.2.1.1 Still Imagery Data Interchange

The following document defines the bandwidth compression standards, conventions and guidelines required for use by the National Imagery Transmission Format Standard (NITFS). It includes specifications on those standards, and implementation related conventions and guidelines to improve interoperability of NITFS compressed files within the United States Imagery and Geospatial System (USIGS). For data compression of still images, the following standard is mandated:

- N-0106-97, Bandwidth Compression Standards and Guidelines Document, 25 August 1998 with Change Notice 1, 01 March 2001.

F.AVS.2.3 Information Transfer Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Aviation Systems Subdomain appendix.

F.AVS.2.4 Information-Modeling, Metadata, and Information-Exchange Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Aviation Systems Subdomain appendix.

F.AVS.2.5 Human-Computer Interface Standards

F.AVS.2.5.1 Mandates

F.AVS.2.5.1.1 Symbology

For primary flight display design and layout the following standard is mandated:

- MIL-STD-1787C, Aircraft Display Symbology, 5 January 01

Note: This standard defines the symbology requirements for a primary flight reference and describes some fundamental relationships between symbol motion and aircraft system states. It describes symbols, symbol formats, and information content for electro-optical displays that provide aircrew members with information for takeoff, navigation, terrain following/terrain avoidance, weapon delivery, and landing. It also provides (in appendixes) non-binding information on symbol geometry, fonts, recommended dimensions, and mechanizations. It does not provide standardized engagement symbology (tactical graphics) at this time.

F.AVS.2.5.1.2 Aviation Systems Subdomain Style Guide

The WSHCI Style Guide has been tailored and extended for the Army Aviation Systems community as the Aviation Human Computer Interface Style Guide (AHCI). This document addresses the design aspects common across most cockpit applications; an issue that is specific to the Aviation Systems Subdomain,. The following standard is mandated for the Aviation Systems Subdomain:

- Aviation Human-Computer Interface Style Guide, Version 2.2, May 1998.

F.AVS.2.5.2 Emerging Standards

F.AVS.2.5.2.1 Aviation Systems Subdomain Style Guide

Currently, there are no subdomain specific emerging standards identified for this section of the Aviation Systems Subdomain appendix.

F.AVS.2.6 Information Systems Security Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Aviation Systems Subdomain appendix.

F.AVS.3 SUBDOMAIN SPECIFIC SERVICES AND INTERFACES

F.AVS.3.1 Introduction

The direct and logical interface semantics, elaborated in the GOA Framework and depicted by the DoD TRM Interfaces View in Figure F-3, provides sufficient fidelity for identifying classes of interfaces to apply open systems interface standards in the design of real-time and embedded hardware/software systems. The Framework also facilitates the identification of critical functions and interfaces within the real-time and embedded computing systems of the Aviation Systems Subdomain.

This section provides a common framework identifying mandated and emerging embedded computing interface standards associated with the logical and direct interface classes defined for the layers depicted in the DoD TRM.

Only those layers of the DoD TRM, that have subdomain specific mandated or emerging standards identified, are addressed in this section.

F.AVS.3.2 Applications Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Aviation Systems Subdomain appendix.

F.AVS.3.3 System Services Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Aviation Systems Subdomain appendix.

F.AVS.3.4 Resource Access Services Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Aviation Systems Subdomain appendix.

F.AVS.3.5 Physical Resources Layer Interfaces

This section identifies the following:

1. The interface standards that provide the requirements for establishing a data interchange interface between Physical Resources and enable bus or communications link boards to address their peers in another node or system, and
2. The interface standards that support the direct connections between Physical Resources, such as those needed to enable busses and communications links to address processors or needed to enable processors to address memory registers.

Included are standards for Serial and Parallel buses. A Serial bus transmits information one bit at a time in a sequential or serial manner. A Parallel bus transfers information (data, interrupts, arbitration, timing,etc.) by sending a number of bits (such as 8 or 16) at the same time using multiconductor cables and connectors. Internal parallel buses include Backplane, Input/Output (I/O), and Single Board Computers (SBC) and Expansion Cards. External parallel buses include peripheral buses.

F.AVS.3.5.1 Mandates

F.AVS.3.5.1.1 Serial Buses

The IEEE 1394 standard is a scalable, flexible, easy to use, low-cost digital interface that defines both a backplane physical layer and a point-to-point cable-connected virtual bus implementation. The backplane version operates at 12.5, 25 or 50 Mbits/sec. The cable version supports data rates of 100, 200 and 400 Mbits/ sec. The Standard defines the media, topology, and the protocol. The following standard is mandated:

- IEEE 1394: 1995, Standard for a High Performance Serial Bus.
- IEEE 1394a: 2000, Amendment 1.

The MIL-STD-1553B data bus standard will be used by applications requiring digital, command/response, time division multiplexing techniques and defines the data bus line and its interface electronics, the concept of operation and information flow on the multiplex data bus, and the electrical and functional formats to be employed. The following standard is mandated:

- MIL-STD-1553B, Standard for Medium Speed System Network Bus, 21 September 1978, with Notice of Change 1, 12 February 1980; Notice of Change 2, 8 September 1986; Notice of Change 3, 31 January 1993; and Notice of Change 4, 15 January 1996.

Some aviation subsystems require a non-multiplexed, high-aggregate bandwidth, Fibre Channel network design. Topologies may be point to point, switched or arbitrated loop. These networks may support multiple communication protocols, such as IP, SCSI, and RDMA with multiple classes of service. The following standards are mandated:

- ANSI/NCITS 288-1999, Information Technology - Fibre Channel - Generic Services - 2 (FC-GS-2), 1999.
- ANSI/NCITS 321, Fibre Channel Switched Fabric and Switched Control Requirements (FC-SW), 1998.
- ANSI/NCITS 332-1999, Fibre Channel Arbitrated Loop (FC-AL-2), 1999.
- ANSI/NCITS X3.230-1994, Fibre Channel Physical and Signaling Interface (FC-PH), 1994.
- ANSI/NCITS X3.230-1994 Amendment 1:1996, Amendment 1 to ANSI/NCITS X3.230-1994 Fibre Channel Physical and Signaling Interface (FC-PH), 1996.

- ANSI/NCITS X3.230-1994 Amendment 2:1999, Amendment 2 to ANSI/NCITS X3.230-1994, Fibre Channel Physical and Signaling Interface (FC-PH), 1999.
- ANSI X3.272, Fibre Channel Arbitrated Loop (FC-AL), 1996.
- ANSI X3.289, Fiber Channel Fabric Generic (FC-FG), 1996.
- ANSI X3.297, Information Technology - Fibre Channel Physical and Signaling Interface 2 (FC-PH-2), 1997.
- ANSI X3.303, Fibre Channel Physical and Signaling Interface 3 (FC-PH-3) 1998.

To integrate commercial aircraft avionics the following avionics interconnect bus standards are mandated:

- ARINC 429, Mark 33 Digital Information Transfer System (DITS), 1999
- ARINC 629, Multi-Transmitter Data Bus, 1999

F.AVS.3.5.1.2 Parallel Buses

F.AVS.3.5.1.2.1 Backplane Buses

The VME64 standard defines a framework for 8-, 16-, 32-, and 64-bit parallel bus computer architectures that can implement single and multiprocessor systems. It is based on the VMEbus specification released by the VMEbus Manufacturers Group (now VITA) in August 1982 and includes the initial four basic subbuses: (1) data transfer bus, (2) priority interrupt bus, (3) arbitration bus, and (4) utility bus. The following standard is mandated:

- ANSI/VITA 1, VME64 Specification, 1994.
- ANSI/VITA 1.1, VME64 Extensions, 1997.

F.AVS.3.5.2 Emerging Standards

For designs that incorporate digital video and define input and output video signals to and from major subsystem components for new and major avionics upgrades the following standard is emerging. This standard is in the balloting process at the NCITS T11 subcommittee and a permanent document number will be applied later:

- T11/Project 1237-D/1.4 (Draft), Information Technology -Fibre Channel - Audio Video (FC-AV)

For real-time embedded avionics subsystems that must interoperate using CORBA technology the following standard is emerging. This standard is in the balloting process at the NCITS T11 subcommittee and a permanent document number will be applied later:

- T11/Project 1332-D/Rev 1.6(Draft) Fibre Channel - Virtual Interface (FC-VI)

Weapon stores interfaces on modern aviation require complex interfaces to allow dependable, timely exchange of sensor data and command messages. Aviation subsystems designers may use the following emerging standard:

- MIL-STD-1760C, Department of Defense Interface Standard for Aircraft/Store Electrical Interconnection System, 20 March 1997

IEEE 1394b-2001 is a full use standard whose scope is to provide a supplement to 1394-1995 and 1394a-2000 that defines features and mechanisms conductive to gigabit speeds in a backward compatible fashion and the ability to signal over single hop distances of up to 100m. The following standard is emerging:

- IEEE 1394b, Standard for a High Performance Serial Bus, 2001

F.AVS.3.6 Global Air Traffic Management Standards

This section addresses civil Air Traffic Management (ATM) interoperability for DoD aircraft in order to operate in the evolving global civil aviation airspace arena. This evolution is the result of the International Civil Aviation Organization (ICAO), and its associated Civil Aviation Authorities' (CAA) desires to take advantage of advancements in the areas of Communications, Navigation, and Surveillance (CNS) technologies. The purpose is to move from a system of ground-based air traffic control to an airborne system of ATM. As a result, DoD aircraft must conform, where required, to appropriate civil requirements and industry standards to meet future civil airspace requirements. If these aircraft are not properly equipped to operate in the airspace/civil aviation regulated environment as it is defined, and accommodate its evolution, they will not be able to operate safely and effectively in airspace where new separation standards and ATM procedures are being implemented by civil aviation authorities. Such aircraft may be excluded from operating in that airspace. The focus of this section is on communications and information transfer standards for civil ATM interoperability.

F.AVS.3.6.1 Mandated Standards

There are no mandated standards for Air Traffic Management Interoperability.

F.AVS.3.6.2 Emerging Standards

The following Air Traffic Management Interoperability Standards covering VHF Digital Link Mode 2, HF Data Link, Aeronautical Mobile Satellite Services, and Mode S capabilities that are needed to interoperate with civil communications infrastructures are considered emerging standards for the Aviation Systems Subdomain:

- Radio Technical Commission for Aeronautics (RTCA) DO-224 – Change 1, Signal-in-Space Minimum Aviation Systems Performance Standards (MASPS) Advanced VHF Digital Data, Communications Including Capability with Digital Voice Technique, 30 April 1998.
- International Civil Aviation Organization (ICAO), Annex 10, Volume III concerning Standards and Recommended Practices (SARPs) for High Frequency Data Link (HFDL), July 1995.
- RTCA DO-210C, Minimum Operational Performance Standards For Aeronautical Mobile Satellite Services (AMSS), 16 January 1996.
- RTCA DO-219, Minimum Operational Performance Standards for ATC Two-Way Data Link Communications, 27 August 1993.
- RTCA DO-212, Minimum Operational Performance Standards for Airborne Automatic Dependent Surveillance (ADS) Equipment, 26 October 1992.
- RTCA DO-181A, Minimum Operational Performance Standards for Air Traffic Control Radar Beacon System/Mode Select (ATCRBS/Mode S), Airborne Equipment, 14 January 1992, Change 1 errata 14 January 1993.

This page was intentionally left blank.

APPENDIX F.GVS - GROUND VEHICLE SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN

F.GVS.1 INTRODUCTION

A weapon system is 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.

The Ground Vehicle Subdomain applies to Army weapon systems that are integral to mobile ground platforms. Wheeled, tracked, manned, and unmanned vehicles are subject to the standards specified in this subdomain appendix. Excluded are missile and munition systems. Specifically, this includes the following elements: tanks, infantry fighting vehicles, engineering vehicles with processor-based mission controls/sensors, howitzers, mortar systems, and chemical/biological systems with processor-based mission controls/sensors. Ground Vehicle Systems have explicit real-time processing requirements. The platform-centric Figure F.GVS-1 below illustrates the time regimes for executing basic Ground Vehicle System functions in an operational environment. The time regimes depicted are weapon-centric, and do not include time associated with external systems. Real-time indicates that processing operations must be executed in a repeatable, predictable and deterministic timeframe."

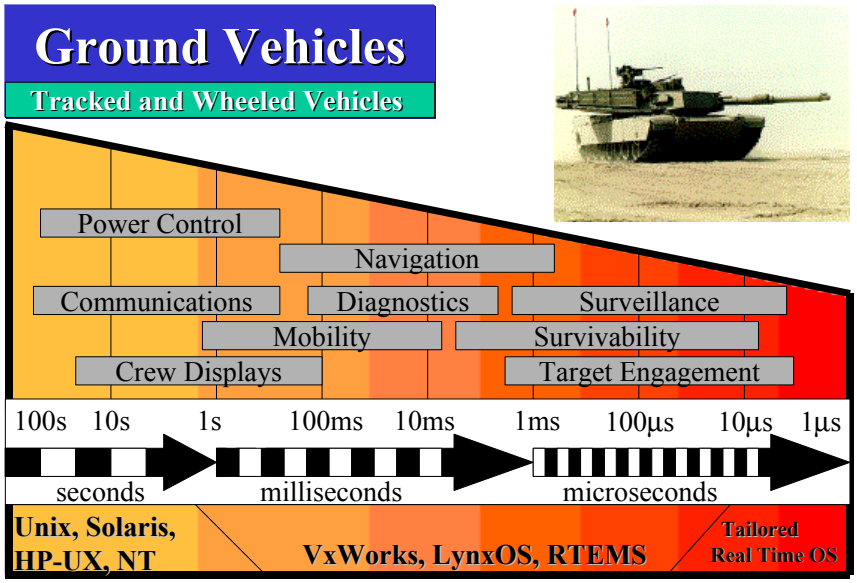


FIGURE F.GVS-1. GROUND VEHICLE SYSTEMS FUNCTIONAL TIME REGIMES

F.GVS.1.1 Purpose

This subdomain builds on Appendix F by identifying Ground Vehicle Systems Subdomain specific standards to include information standards and analogous standards applicable to

Ground Vehicle Systems (see Section 1.2.2 for relationships between core, domain, and subdomain standards).

F.GVS.1.2 Scope

The scope of this appendix is the entire Ground Vehicle Systems Subdomain as defined in Appendix F.GVS.1.

F.GVS.1.3 Background

The standards in this subdomain are based on the work performed by the Army Weapon Systems Technical Architecture Working Group (WSTAWG).

F.GVS.1.4 Technical Reference Model (TRM)

The Technical Reference Model used in this subdomain is the DoD TRM that is described in the Weapon Systems Domain appendix.

F.GVS.1.5 Appendix Structure

This appendix is divided into three sections: the Introduction in Appendix F.GVS.1, the Subdomain Specific Standards in Appendix F.GVS.2, and the Subdomain Specific Services and Interfaces in Appendix F.GVS.3. Appendix F.GVS.2 follows the JTA-Army core structure. The structure of Appendix F.GVS.3 follows the structure contained in the DoD TRM Interfaces View.

F.GVS.2 SUBDOMAIN SPECIFIC STANDARDS

F.GVS.2.1 Introduction

This section identifies the subdomain specific mandated and emerging standards for the Ground Vehicle Systems Subdomain appendix, in addition to those standards identified in the WSD Appendix and the JTA-A core.

F.GVS.2.2 Information Processing Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Ground Vehicle Systems Subdomain appendix.

F.GVS.2.3 Information Transfer Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Ground Vehicle Systems Subdomain appendix.

F.GVS.2.4 Information-Modeling, Metadata, and Information-Exchange Standards

F.GVS.2.4.1 Mandates

Currently there are no subdomain specific mandated standards identified for this section of the Ground Vehicle appendix.

F.GVS.2.4.2 Emerging Standards

F.GVS.2.4.2.1 Tactical Information Exchange Standards (Bit Oriented Formatted Messages)

The Sensor Link Protocol Message Set (SLP) was developed for use as a common interface between electro-optical sensor systems and a diverse set of host computer systems. The SPL message set is decoupled from lower layer protocols to allow implementers the flexibility to select from a number of open standards such as RS-232/485, FireWire or USB. The SLP message set is used in conjunction with the SLP Interface Control Document to develop a common digital data exchange mechanism between sensors and host computing devices that offer full remote operation and control of those sensors by a host-computing device in both a point-to-point and networked environment. The following emerging standard defines the SLP message set:

- SLP-MSG-210, Revision, Sensor Link Protocol Message Set, 26 March 2001.

F.GVS.2.5 Human-Computer Interface Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Ground Vehicle Systems Subdomain appendix.

F.GVS.2.5.1 Mandates

Currently, there are no subdomain specific mandated standards identified for this section of the Ground Vehicle Systems Subdomain appendix.

F.GVS.2.5.2 Emerging Standards

Currently there are no subdomain specific emerging standards identified for this section of the Ground Vehicle Systems Subdomain appendix.

F.GVS.2.6 Information Systems Security Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Ground Vehicle Systems Subdomain appendix.

F.GVS.3 SUBDOMAIN SPECIFIC SERVICES AND INTERFACES

F.GVS.3.1 Introduction

The direct and logical interface semantics, elaborated in the GOA Framework and depicted by the DoD TRM Interfaces View in Figure F-3, provides sufficient fidelity for identifying classes of interfaces to apply open systems interface standards in the design of real-time and embedded hardware/software systems. The Framework also facilitates the identification of critical functions and interfaces within the real-time and embedded computing systems of the Ground Vehicle Systems Subdomain.

This section provides a common framework identifying mandated and emerging embedded computing interface standards associated with the logical and direct interface classes defined for the layers depicted in the DoD TRM.

Only those layers of the DoD TRM, that have subdomain specific mandated or emerging standards identified, are addressed in this section.

F.GVS.3.2 Applications Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Ground Vehicle Systems Subdomain appendix.

F.GVS.3.3 System Services Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Ground Vehicle Systems Subdomain appendix.

F.GVS.3.4 Resource Access Services Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Ground Vehicle Systems Subdomain appendix.

F.GVS.3.5 Physical Resources Layer Interfaces

This section identifies:

1. The interface standards that provide the requirements for establishing a data interchange interface between Physical Resources and enable bus or communications link boards to address their peers in another node or system, and
2. The interface standards that support the direct connections between Physical Resources, such as those needed to enable busses and communications links to address processors or needed to enable processors to address memory registers.

Included are standards for Serial and Parallel buses. A Serial bus transmits information one bit at a time in a sequential or serial manner. A Parallel bus transfers information (data, interrupts, arbitration, timing,etc.) by sending a number of bits (such as 8 or 16) at the same time using multiconductor cables and connectors. Internal parallel buses include Backplane, Input/Output (I/O), and Single Board Computers (SBC) and Expansion Cards. External parallel buses include peripheral buses.

F.GVS.3.5.1 Mandates

F.GVS.3.5.1.1 Serial Buses

The MIL-STD-1553B data bus standard will be used by applications requiring digital, command/response, time division multiplexing techniques and defines the data bus line and its interface electronics, the concept of operation and information flow on the multiplex data bus, and the electrical and functional formats to be employed. The following standard is mandated:

- MIL-STD-1553B, Standard for Medium Speed System Network Bus, 21 September 1978, with Notice of Change 1, 12 February 1980; Notice of Change 2, 8 September 1986; Notice of Change 3, 31 January 1993; and Notice of Change 4, 15 January 1996.

SAE J1850 establishes the requirements for a Class B Data Communication Network Interface applicable to all On- and Off-Road Land-Based Vehicles. It defines a minimum set of data communication requirements such that the resulting network is cost effective for simple

applications and flexible enough to use in complex applications. The following standard is mandated:

- SAE J1850, Class B Data Communication Network Interface, 1 July 1995.

F.GVS.3.5.1.2 Parallel Buses

F.GVS.3.5.1.2.1 Backplane Buses

The VME64 standard defines a framework for 8-, 16-, 32-, and 64-bit parallel bus computer architectures that can implement single and multiprocessor systems. It is based on the VMEbus specification released by the VMEbus Manufacturers Group (now VITA) in August 1982 and includes the initial four basic subbuses: (1) data transfer bus, (2) priority interrupt bus, (3) arbitration bus, and (4) utility bus. The following standard is mandated:

- ANSI/VITA 1, VME64 Specification, 1994
- ANSI/VITA 1.1, VME64 Extensions, 1997

The following industrial bus standard is mandated for applications requiring high-speed data transfer, rugged construction, excellent shock and vibration resistance, Plug'n Fight capability, and the desire for future hot-swappable support:

- PCI Industrial Computer Manufacturer's Group (PICMG): Compact PCI Specification, R2.1, September 1997.

F.GVS.3.5.1.2.2 Single Board Computer (SBC) Expansion Buses

The IEEE 1101.2 Mechanical Core Specification is applicable to, but not limited to, the VMEbus standard, an internal interconnect (backplane) bus intended for connecting processing elements to their immediate fundamental resources, and is cited to facilitate mechanical interchangeability of conduction-cooled circuit card assemblies in a format suitable for military and rugged applications and to ensure their compatibility with the commercial, double-height 16 mm, Eurocard chassis. The following standard is mandated:

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

F.GVS.3.5.1.2.3 Peripheral Bus

The following standard is mandated for applications that require an efficient peer-to-peer I/O bus capable of handling up to 16 devices, including one or more hosts. This standard includes command sets for magnetic and optical disks, tapes, printers, processors, CD-ROMs, scanners, medium changers, and communications devices. The following standard is mandate:

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

F.GVS.3.5.2 Emerging Standards

F.GVS.3.5.2.1 Serial Buses

The Ground Vehicle Systems Subdomain is evaluating the CANBUS protocol and Class C networks documented in SAE J1939 as an emerging standard for use in its heavy trucks and off road vehicles:

- SAE J1939: Truck and Bus Control and Communications Network.

SAE J1587 defines the format of the messages and data being communicated between microprocessors used in heavy-duty vehicle applications. It is meant to serve as a guide toward standard practice software compatibility among microcomputer-based modules. This Standard is to be used with SAE J1708 that defines the requirements for the hardware and basic protocol that is needed to implement the requirements of SAE J1587.

The Ground Vehicle Systems Subdomain is evaluating the following SAE Heavy-Duty Vehicle specification:

- SAE J1587: Joint SAE/TMC Electronic Data Interchange Between Microcomputer Systems in Heavy-Duty Vehicle Applications.

SAE J1708 defines a general-purpose serial data communication link that may be utilized in heavy-duty vehicle applications. It is intended to serve as a guide toward standard practice to promote serial communication compatibility among microcomputer-based modules. This standard requires the definition of the data format, message identification, message priorities, error detection (and correction), maximum message length, percent bus utilization, and methods of physically adding/removing units to/from the line for the particular application.

- SAE J1708: Serial Data Communications Between Microcomputer Systems in Heavy-Duty Vehicle Applications.

APPENDIX F.MS - MISSILE SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN

F.MS.1 INTRODUCTION

A weapon system is 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. Systems covered within the Missile Systems Subdomain include but are not limited to shoulder-fired missiles, line-of-sight direct fire missiles and rockets, non-line-of-sight indirect fire missiles and rockets, and Air and Missile Defense (AMD) systems. Missile Systems may be described in terms of the following subsystems: 1) missile, 2) launcher, 3) C3I (including fire control or battle management), and 4) intra-system sensors, where applicable. These subsystems are designed and developed to deploy and function as a single Missile System where all the subsystems are to a certain degree, interdependent. The subsystems of a Missile System may be collocated, or distributed. Missile Systems include offensive and defensive, tactical (including theater) and strategic missile systems (including air and missile defense), and have explicit real-time processing requirements. The platform-centric Figure F.MS-1 below illustrates the various time regimes for executing basic Missile System functions in an operational environment. The time regimes depicted are weapon-centric, and do not include time associated with external systems. Real-time indicates that processing operations must be executed in a repeatable, predictable and deterministic timeframe.

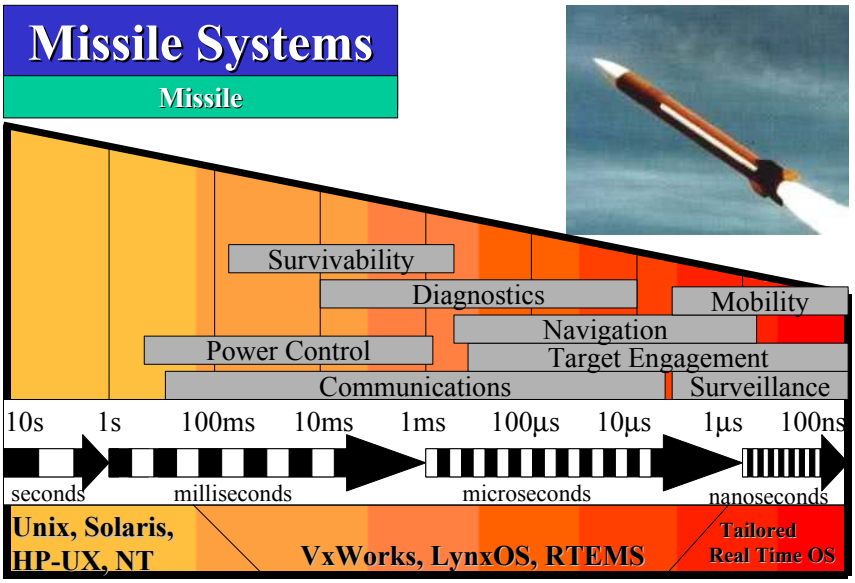


FIGURE F.MS-1. MISSILE SYSTEMS FUNCTIONAL TIME REGIMES

F.MS.1.1 Purpose

This subdomain builds on Appendix F by identifying Missile Systems Subdomain specific standards to include information standards and analogous standards applicable to Missile Systems (see Section 1.2.2 for relationships between core, domain, and subdomain standards).

F.MS.1.2 Scope

The scope of this subdomain appendix is the entire Missile Systems Subdomain (as defined in Appendix F.MS.1 above).

F.MS.1.3 Background

The standards in this subdomain are based on the ongoing work performed by the Army Weapon Systems Technical Architecture Working Group (WSTAWG).

F.MS.1.4 Technical Reference Model (TRM)

The Technical Reference Model used in this subdomain is the DoD TRM that is described in the Weapon Systems Domain appendix.

F.MS.1.5 Appendix Structure

This appendix is divided into three sections: the Introduction in Appendix F.MS.1, the Subdomain Specific Standards in Appendix F.MS.2, and the Subdomain Specific Services and Interfaces in Appendix F.MS.3. Appendix F.MS.2 follows the JTA-Army core structure. The structure of Appendix F.MS.3 follows the structure contained in the DoD TRM Interfaces View.

F.MS.2 SUBDOMAIN SPECIFIC STANDARDS

F.MS.2.1 Introduction

This section identifies the subdomain specific mandated and emerging standards for the Missile Systems Subdomain appendix, in addition to those standards identified in the WSD Appendix and the JTA-Army core.

F.MS.2.2 Information Processing Standards

F.MS.2.2.1 Mandates

Currently, there are no subdomain specific standards mandated in this section.

F.MS.2.2.2 Emerging Standards

F.MS.2.2.2.1 Geospatial Data Interchange

The following standard is being evaluated as an emerging extension to the WGS 84 geospatial data interchange standard for use with Missile Systems:

- ANSI/AIAA R-004-1992, Recommended Practice for Atmospheric and Space Flight Vehicle Coordinate Systems.

F.MS.2.3 Information Transfer Standards

F.MS.2.3.1 Mandates

Currently, there are no mandated standards in this section.

F.MS.2.3.2 Emerging Standards

F.MS.2.3.2.1 Joint Range Extension (JRE) Application Protocol (JREAP)

The Joint Range Extension (JRE) application protocol (JREAP) encapsulates TADIL information (e.g., TADIL-J/Link-16) as an application layer within Joint Technical Architecture (JTA) compliant data protocols (e.g., Internet Protocol (IP), Point-to-Point Protocol (PPP), Ultra High Frequency Demand Assigned Multiple Access (UHF DAMA)). The joint protocol allows a JRE Gateway to process and manage incoming TADIL messages and redirect them to the appropriate destination via the appropriate media. The following standard is emerging for exchange of TADIL-J information over long haul media:

- Joint Range Extension Application Protocol (JREAP) for Encapsulation into Joint Technical Architecture (JTA) Compliant Protocols, Joint Range Extension Application Protocol Working Group, Version 1.0, 19 July 2000.

F.MS.2.4 Information-Modeling, Metadata, and Information-Exchange Standards

Currently there are no subdomain specific mandated or emerging standards in this section.

F.MS.2.5 Human-Computer Interface Standards

F.MS.2.5.1 Mandates

F.MS.2.5.1.1 Symbology

The Missile Systems Subdomain (specifically the AMD systems portion of the subdomain) needs to be able to provide for near-real-time and real-time engagement operations, and MIL-STD-2525B does not support this and other required capabilities. The MIL-STD-1477 series performs this Engagement Operations Symbology function. Developers should be aware that MIL-STD-1477C should NOT be used and is NOT mandated. Developers should use the superceded MIL-STD-1477B as a reference until such time that MIL-STD-1477D receives final approval.

F.MS.2.5.2 Emerging Standards

Currently, there are no subdomain specific emerging standards in this section.

F.MS.2.6 Information Systems Security Standards

Currently, there are no subdomain specific mandated or emerging standards in this section.

F.MS.3 SUBDOMAIN SPECIFIC SERVICES AND INTERFACES

F.MS.3.1 Introduction

The direct and logical interface semantics, elaborated in the GOA Framework and depicted by the DoD TRM Interfaces View in Figure F-3, provides sufficient fidelity for identifying classes of interfaces to apply open systems interface standards in the design of real-time and embedded hardware/software systems. The Framework also facilitates the identification of critical functions and interfaces within the real-time and embedded computing systems of the Missile Systems Subdomain.

This section provides a common framework identifying mandated and emerging embedded computing interface standards associated with the logical and direct interface classes defined for the layers depicted in the DoD TRM.

Only those layers of the DoD TRM, that have subdomain specific mandated or emerging standards identified, are addressed in this section.

F.MS.3.2 Application Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Missile Systems Subdomain appendix.

F.MS.3.3 System Services Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Missile Systems Subdomain appendix.

F.MS.3.4 Resource Access Services Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Missile Systems Subdomain appendix.

F.MS.3.5 Physical Resources Layer Interfaces

This section identifies:

1. The interface standards that provide the requirements for establishing a data interchange interface between Physical Resources and enable bus or communications link boards to address their peers in another node or system, and
2. The interface standards that support the direct connections between Physical Resources, such as those needed to enable busses and communications links to address processors or needed to enable processors to address memory registers.

Included are standards for Serial and Parallel buses. A Serial bus transmits information one bit at a time in a sequential or serial manner. A Parallel bus transfers information (data, interrupts, arbitration, timing,etc.) by sending a number of bits (such as 8 or 16) at the same time using multiconductor cables and connectors. Internal parallel buses include Backplane, Input/Output (I/O), and Single Board Computers (SBC) and Expansion Cards. External parallel buses include peripheral buses.

F.MS.3.5.1 Mandates

F.MS.3.5.1.1 Parallel Buses

F.MS.3.5.1.1.1 Single Board Computer (SBC) Expansion Buses

The IEEE 1101.2 Mechanical Core Specification is applicable to, but not limited to, the VMEbus standard, an internal interconnect (backplane) bus intended for connecting processing elements to their immediate fundamental resources, and is cited to facilitate mechanical interchangeability of conduction-cooled circuit card assemblies in a format suitable for military and rugged applications and to ensure their compatibility with the commercial, double-height 16 mm, Eurocard chassis. The following standard is mandated:

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

F.MS.3.5.2 Emerging Standards

Currently, there are no subdomain specific emerging standards identified for this section of the Missile Systems Subdomain appendix.

This page was intentionally left blank.

APPENDIX F.MUS - MUNITION SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN

F.MUS.1 INTRODUCTION

A weapon system is 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.

Within the U.S Army's inventory of Weapon Systems, many systems do not fit within the parameters of the well-defined Weapon Systems Subdomains of Missile Systems, Soldier Systems, Ground Vehicle Systems, or Aviation Systems. These non-mobile, transportable, Weapon Systems include, but are not limited to, munitions, munitions integrated with combat sensors, and munitions integrated with sensors, control stations, combat communication systems, repeaters, and gateways. The Munition Systems Subdomain includes any system or subsystem containing an explosive warhead (such as dumb, smart, and precision bombs, or mines and artillery shells) or non-lethal deterrent and that detects, classifies, identifies, intercepts, and destroys or negates the effectiveness of the enemy to protect US and coalition forces, civilians, and geopolitical assets. Munition Systems have explicit real-time processing requirements. Figure F.MUS-1 illustrates the various time regimes for executing basic Munition System functions in an operational environment. The time regimes depicted are weapon-centric, and do not include time associated with external systems. Real-time indicates that processing operations must be executed in a repeatable, predictable and deterministic timeframe.

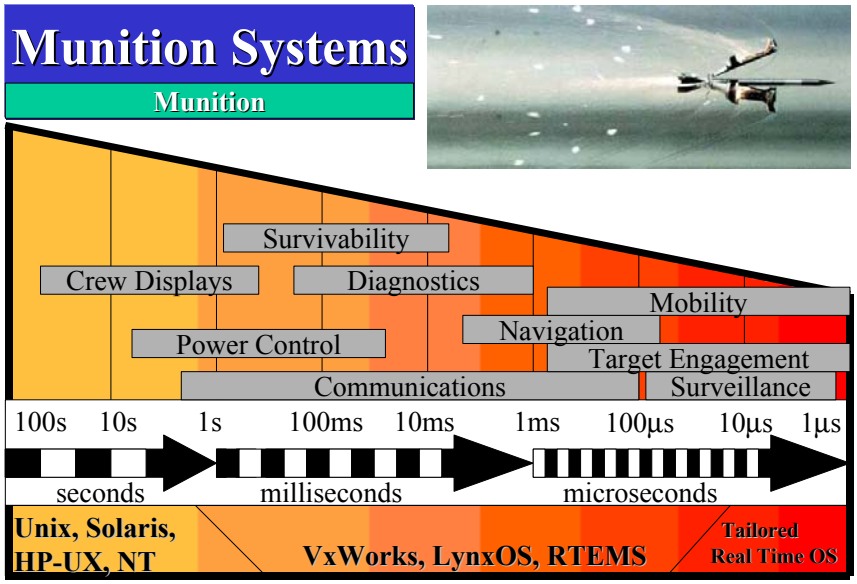


FIGURE F.MUS-1. MUNTION SYSTEMS FUNCTIONAL TIME REGIMES

F.MUS.1.1 Purpose

This subdomain builds on Appendix F by identifying Munition Systems Subdomain specific standards to include information standards and analogous standards applicable to Munition Systems (see Section 1.2.2 for relationships between core, domain, and subdomain standards).

The primary purpose of establishing a subdomain is to ensure interoperability, defined as the ability of two or more systems or components to exchange data and use information (IEEE STD 610.12) within the Family of Systems that constitute the subdomain.

F.MUS.1.2 Scope

The scope of this subdomain appendix is the entire Munition Systems Subdomain (as defined in the overview and subdomain description above).

F.MUS.1.3 Background

The standards in this subdomain are based on the work performed by the Army Weapon Systems Technical Architecture Working Group (WSTAWG).

F.MUS.1.4 Technical Reference Model (TRM)

The Technical Reference Model used in this subdomain is the DoD TRM that is described in the Weapon Systems Domain appendix.

F.MUS.1.5 Appendix Structure

This appendix is divided into three sections: the Introduction in Appendix F.MUS.1, the Subdomain Specific Standards in Appendix F. MUS.2, and the Subdomain Specific Services and Interfaces in Appendix F. MUS.3. Appendix F. MUS.2 follows the JTA-Army core structure. The structure of Appendix F. MUS.3 follows the structure contained in the DoD TRM Interfaces View.

F.MUS.2 SUBDOMAIN SPECIFIC STANDARDS

F.MUS.2.1 Introduction

This section identifies the subdomain specific mandated and emerging standards for the Munition Systems Subdomain appendix, in addition to those standards identified in the WSD Appendix and the JTA-A core.

F.MUS.2.2 Information Processing Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Munition Systems Subdomain appendix.

However, the Munition Systems Subdomain is unable to use X/Open C323, Common Desktop Environment (CDE) Version 1.0, but instead will use Windows NT® (POSIX® configuration) and will be uniquely structured to support the Weapon Systems Human-Computer Interface (WSHCI) Style Guide. (Refer to JTA-A Sections 2.2.2.1.2, User Interface Services and F.2.5.1.1)

F.MUS.2.2.1 Emerging Standards

Currently, there are no subdomain specific emerging standards in this section.

F.MUS.2.3 Information Transfer Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Munition Systems Subdomain appendix.

F.MUS.2.4 Information-Modeling, Metadata, and Information-Exchange Standards

F.MUS.2.4.1 Mandates

Currently, there are no subdomain specific mandated standards identified for this section of the Munition Systems Subdomain appendix.

F.MUS.2.4.2 Emerging Standards

F.MUS.2.4.2.1 Tactical Information Exchange Standards (Bit Oriented Formatted Messages)

The Sensor Link Protocol Message Set (SLP) was developed for use as a common interface between electro-optical sensor systems and a diverse set of host computer systems. The SPL message set is decoupled from lower layer protocols to allow implementers the flexibility to select from a number of open standards such as RS-232/485, FireWire or USB. The SLP message set is used in conjunction with the SLP Interface Control Document to develop a common digital data exchange mechanism between sensors and host computing devices that offer full remote operation and control of those sensors by a host-computing device in both a point-to-point and networked environment. The following emerging standard defines the SLP message set:

- SLP-MSG-210, Revision, Sensor Link Protocol Message Set, 26 March 2001.

F.MUS.2.5 Human-Computer Interface Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Munition Systems Subdomain appendix.

F.MUS.2.6 Information Systems Security Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Munition Systems Subdomain appendix.

However, due to the primarily unattended system nodes involved in this subdomain, Type 1 Information Security systems for some Munition Systems cannot be used. When this occurs, Command and Control of Munition Systems dictates the use of Type II, “Sensitive, But Unclassified” (SBU), Information Security systems with National Security Agency (NSA) endorsement. However, there will be a requirement to protect the SBU information disseminated within the systems included in this subdomain. (Refer to Section 6.2 Information Processing Security Standards, and Section 6.3 Information Transfer Security Standards)

F.MUS.3 SUBDOMAIN SPECIFIC SERVICES AND INTERFACES

F.MUS.3.1 Introduction

The direct and logical interface semantics, elaborated in the GOA Framework and depicted by the DoD TRM Interfaces View in Figure F-3, provides sufficient fidelity for identifying classes of interfaces to apply open systems interface standards in the design of real-time and embedded hardware/software systems. The Framework also facilitates the identification of critical functions and interfaces within the real-time and embedded computing systems of the Munition Systems Subdomain.

This section provides a common framework identifying mandated and emerging embedded computing interface standards associated with the logical and direct interface classes defined for the layers depicted in the DoD TRM.

Only those layers of the DoD TRM, that have subdomain specific mandated or emerging standards identified, are addressed in this section.

F.MUS.3.2 Application Software Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Munition Systems Subdomain appendix.

F.MUS.3.3 System Services Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Munition Systems Subdomain appendix.

F.MUS.3.4 Resource Access Services Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Munition Systems Subdomain appendix.

F.MUS.3.5 Physical Resources Layer Interfaces

This section identifies the following:

1. The interface standards that provide the requirements for establishing a data interchange interface between Physical Resources and enable bus or communications link boards to address their peers in another node or system, and
2. The interface standards that support the direct connections between Physical Resources, such as those needed to enable busses and communications links to address processors or needed to enable processors to address memory registers.

Included are standards for Serial and Parallel buses. A Serial bus transmits information one bit at a time in a sequential or serial manner. A Parallel bus transfers information (data, interrupts, arbitration, timing,etc.) by sending a number of bits (such as 8 or 16) at the same time using multiconductor cables and connectors. Internal parallel buses include Backplane, Input/Output (I/O), and Single Board Computers (SBC) and Expansion Cards. External parallel buses include peripheral buses.

F.MUS.3.5.1 Mandates

F.MUS.3.5.1.1 Parallel Buses

F.MUS.3.5.1.1.1 Backplane Buses

The following industrial bus standard is mandated for applications requiring high-speed data transfer, rugged construction, excellent shock and vibration resistance, Plug'n Fight capability, and the desire for future hot-swappable support:

- PCI Industrial Computer Manufacturer's Group (PICMG): Compact PCI Specification, R2.1, September 1997.

F.MUS.3.5.1.1.2 Peripheral Buses

The following standard is mandated for applications that require an efficient peer-to-peer I/O bus capable of handling up to 16 devices, including one or more hosts. This standard includes command sets for magnetic and optical disks, tapes, printers, processors, CD-ROMs, scanners, medium changers, and communications devices. The following standard is mandated:

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

F.MUS.3.5.2 Emerging Standards

Currently, there are no subdomain specific emerging standards identified for this section of the Munition Systems Subdomain appendix.

F.MUS.3.6 Safety-Critical Software Services

Safety-Critical Software is software that performs the following tasks:

1. Exercises direct command and control over the condition or state of hardware components; and, if not performed, performed out-of-sequence, or performed incorrectly, could result in improper control functions (or lack of control functions) required for proper system operation, which could cause a hazard or allow a hazardous condition to exist.
2. Monitors the state of hardware components; and, if not performed, performed out-of-sequence, or performed incorrectly, could provide data that results in erroneous decisions by human operators or companion systems that could cause a hazard or allow a hazardous condition to exist.
3. Exercises direct command and control over the condition or state of hardware components; and, if performed inadvertently, out-of-sequence, or if not performed, could, in conjunction with other human, hardware, or environmental failure, cause a hazard or allow a hazardous condition to exist.

Once a Munition Systems Subdomain has been determined to have Safety-Critical requirements, MIL-STD-882C is required to assess system safety conditions. Final safety approval will be through the standard Army Type-Classification and Material Release process. In those cases where the Safety-Critical Software is used to direct arming of Army fused systems, Army Fused Safety Review Board (AFSRB) approval will be required prior to Type-Classification and Material Release.

This safety assessment process is applicable only to software that is acquired or developed by the Army that is used as part of a Munition System that possesses the potential to directly or indirectly cause unplanned and undesired harm to humans or damage to property external to the Munition System. This process is intended for application to specific software elements, that have been identified via a system hazard analysis as software that could cause or contribute to

the system achieving a specific hazardous state, or that is intended to detect or take corrective action if the system reaches a specific hazardous state, or that is intended to mitigate damage if an accident occurs.

F.MUS. 3.6.1 Mandates

The following standard is mandated as an interface standard by the Munition Systems Subdomain:

- MIL-STD-882C, System Safety Program Requirements, 19 January 1993.

F.MUS. 3.6.2 Emerging Standards

The following standards are being evaluated as emerging interface standards by the Munition Systems Subdomain:

- Joint Software System Safety Handbook, Draft, 30 September 1997.
- STANAG 4404, Edition 1, Safety Requirements and Guidelines for Munition Systems Related Safety Critical Systems, Draft, 29 August 1997.
- STANAG 4452, Edition 1, Safety Assessment of Munition-Related Computing Systems, Draft, 1 June 1997.

APPENDIX F.SS - SOLDIER SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN

F.SS.1 INTRODUCTION

A weapon system is 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. Systems covered within the Soldier Systems Subdomain include any system or subsystem integrating weapons, target detection, location and warning sensors, ballistic and environmental protective equipment, positioning and location equipment, helmet mounted displays, load carrying, sustainment and special purpose equipment onto the soldier as the platform. The systems are functionally integrated using an embedded computer with multiple pieces of radio communications equipment to enhance command and control and combat effectiveness. These systems are optimized to minimize cognitive overload, to minimize the total weight carried by the individual, and to meet the tactical battlefield environmental characteristics including delivery by parachute while worn by the soldier. All systems are self contained, man-packed and battery powered and do not rely on any fixed infrastructure to meet the operational performance requirements. Soldier Systems have explicit real-time processing requirements. The platform-centric Figure F.SS-1 below illustrates the various time regimes for executing basic Soldier System functions in an operational environment. The time regimes depicted are weapon-centric, and do not include time associated with external systems. Real-time indicates that processing operations must be executed in a repeatable, predictable and deterministic timeframe.

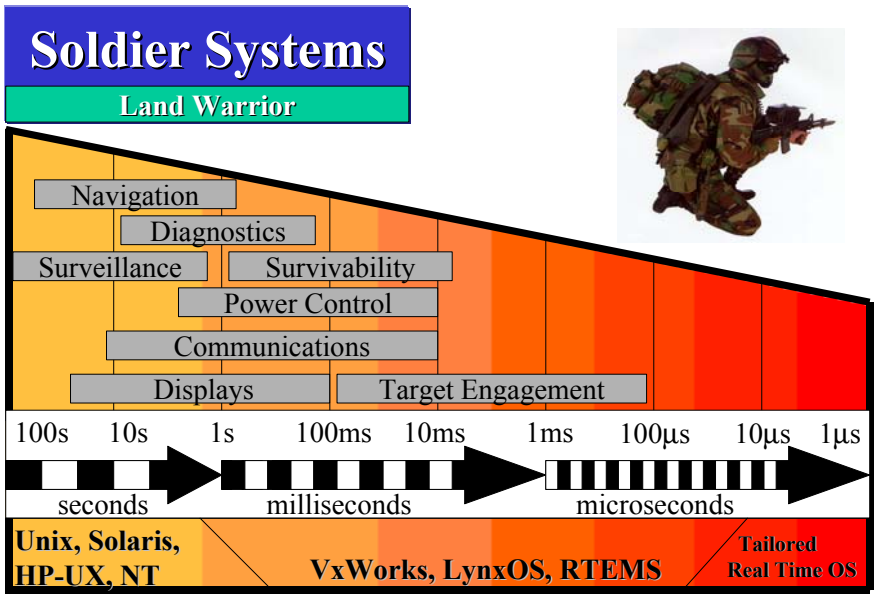


FIGURE F.SS-1. SOLDIER SYSTEMS FUNCTIONAL TIME REGIMES

F.SS.1.1 Purpose

This subdomain builds on Appendix F by identifying Soldier Systems Subdomain specific standards to include information standards and analogous standards applicable to Soldier Systems (see Section 1.2.2 for relationships between core, domain, and subdomain standards).

F.SS.1.2 Scope

The scope of this subdomain appendix is the entire Soldier Systems Subdomain a defined in section F.SS.1 above.

F.SS.1.3 Background

The standards in this subdomain are based on the work performed by the Army Weapon Systems Technical Architecture Working Group (WSTAWG).

The following documents provide useful background information regarding soldier systems with particular emphasis on fighting systems:

1. The Soldier Integrated Protective Ensemble (SIPE), Army Concept Technology Demonstration (ACTD), U.S. Army Natick Research, Development and Engineering Command, Sep 1991.
2. The Enhanced Integrated Soldier System (TEISS), Army Science Board Study, 30 March 1993.
3. The Land Warrior Operational Requirements Document (ORD), HQ US Army Training and Doctrine Command, 17 March 1994.

F.SS.1.4 Technical Reference Model (TRM)

The Technical Reference Model (TRM) used in this subdomain is the DoD TRM that is described in the Weapon Systems Domain appendix.

F.SS.1.5 Appendix Structure

This appendix is divided into three sections: the Introduction in Appendix F.SS.1, the Subdomain Specific Standards in Appendix F.SS.2, and the Subdomain Specific Services and Interfaces in Appendix F.SS.3. Appendix F.SS.2 follows the JTA-Army core structure. The structure of Appendix F.SS.3 follows the structure contained in the DoD TRM Interfaces View.

F.SS.2 SUBDOMAIN SPECIFIC STANDARDS

F.SS.2.1 Introduction

This section identifies the subdomain specific mandated and emerging standards for the Soldier Systems Subdomain appendix, in addition to those standards identified in the WSD Appendix and the JTA-A core.

F.SS.2.2 Information Processing Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Soldier Systems Subdomain appendix.

F.SS.2.3 Information Transfer Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Soldier Systems Subdomain.

F.SS.2.4 Information-Modeling, Metadata, and Information-Exchange Standards

F.SS.2.4.1 Mandates

Currently there are no subdomain specific mandated standards identified for this section of the Soldier Systems Subdomain appendix.

F.SS.2.4.2 Emerging Standards

F.SS.2.4.2.1 Tactical Information Exchange Standards (Bit Oriented Formatted Messages)

F.SS.2.4.2.1.1 Sensor Link Protocol (SLP) Message Set

The Sensor Link Protocol Message Set (SLP) was developed for use as a common interface between electro-optical sensor systems and a diverse set of host computer systems. The SPL message set is decoupled from lower layer protocols to allow implementers the flexibility to select from a number of open standards such as RS-232/485, FireWire or USB. The SLP message set is used in conjunction with the SLP Interface Control Document to develop a common digital data exchange mechanism between sensors and host computing devices that offer full remote operation and control of those sensors by a host-computing device in both a point-to-point and networked environment. The following emerging standard defines the SLP message set:

- SLP-MSG-210, Revision, Sensor Link Protocol Message Set, 26 March 2001.

F.SS.2.5 Human-Computer Interface Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Soldier Systems Subdomain appendix.

F.SS.2.6 Information Systems Security Standards

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Soldier Systems Subdomain appendix.

F.SS.3 SUBDOMAIN SPECIFIC SERVICES AND INTERFACES

F.SS.3.1 Introduction

The direct and logical interface semantics, elaborated in the GOA Framework and depicted by the DoD TRM Interfaces View in Figure F-3, provides sufficient fidelity for identifying classes of interfaces to apply open systems interface standards in the design of real-time and embedded hardware/software systems. The Framework also facilitates the identification of critical functions and interfaces within the real-time and embedded computing systems of the Soldier Systems Subdomain.

This section provides a common framework identifying mandated and emerging embedded computing interface standards associated with the logical and direct interface classes defined for the layers depicted in the DoD TRM.

Only those layers of the DoD TRM, that have subdomain specific mandated or emerging standards identified, are addressed in this section.

F.SS.3.2 Application Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Soldier Systems Subdomain appendix.

F.SS.3.3 System Services Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Soldier Systems Subdomain appendix.

F.SS.3.4 Resource Access Services Layer Interfaces

Currently, there are no subdomain specific mandated or emerging standards identified for this section of the Soldier Systems Subdomain appendix.

F.SS.3.5 Physical Resources Layer Interfaces

This section identifies:

1. The interface standards that provide the requirements for establishing a data interchange interface between Physical Resources and enable bus or communications link boards to address their peers in another node or system, and
2. The interface standards that support the direct connections between Physical Resources, such as those needed to enable busses and communications links to address processors or needed to enable processors to address memory registers.

Included are standards for Serial and Parallel buses. A Serial bus transmits information one bit at a time in a sequential or serial manner. A Parallel bus transfers information (data, interrupts, arbitration, timing,etc.) by sending a number of bits (such as 8 or 16) at the same time using multiconductor cables and connectors. Internal parallel buses include Backplane, Input/Output (I/O), and Single Board Computers (SBC) and Expansion Cards. External parallel buses include peripheral buses.

F.SS.3.5.1 Mandates

F.SS.3.5.1.1 Serial Buses

The IEEE 1394 (aka FireWire) bus supports scalable performance by supporting rates of 100, 200 and 400 Mbps in both the guaranteed delivery asynchronous mode as well as the guaranteed bandwidth isochronous transmission mode. Each topology can support up to a total of 64 nodes with up to 16 contiguous hops, and up to a total of 1024 buses. For serial bus infrastructures requiring transmission of video, voice and data where guaranteed bandwidth for video and voice, and guaranteed delivery of data are required, the following standards are mandated:

- IEEE-1394-1995, IEEE Standard for a High Performance Serial Bus, 1995.

- IEEE-1394a-2000, IEEE Standard for a High Performance Serial Bus, Amendment 1.

F.SS.3.5.2 Emerging Standards

F.SS.3.5.2.1 Serial Buses

The IEEE 1394b-2001 is a full use standard whose scope is to provide a supplement to 1394-1995 and 1394a-2000 that defines features and mechanisms conducive to gigabit speeds in a backward compatible fashion and the ability to signal over single hop distances of up to 100m. The following standard is emerging:

- IEEE-1394b, Standard for a High Performance Serial Bus, 2001.

This page was intentionally left blank.

APPENDIX G - MODELING AND SIMULATION DOMAIN

G.1 DOMAIN OVERVIEW

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

G.1.1 Purpose

This appendix builds on the JTA-Army core mandates by identifying M&S Domain specific standards to include information standards and analogous standards applicable to M&S (see Section 1.2.2 for relationships between core and domain standards).

G.1.2 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,* dated 10 July 1997, and the *Army Model and Simulation Master Plan*, dated October 1997, 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 includes C4I interfaces, weapon systems/platforms with embedded collective training, and instrumented ranges. 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 HLA for Simulations provides the framework for standards for DoD simulations. The HLA builds on and extends the previous architectures and associated standards that have been developed and used successfully for specific classes of simulation.

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 will 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 Distributed Interactive Simulation (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 was a government/industry initiative to define standards for linking various elements of the simulation domain.

G.1.3 Domain Description

This appendix provides a set of standards affecting the definition, design, development, execution and testing of models and simulations. Increasingly the Army and supporting industries are integrating and operating a mix of computer simulations, actual warfighting systems, weapons simulators and instrumented ranges to support a diversity of applications including training, mission rehearsal, operational course of action analysis, investment analysis, and many aspects of acquisition support throughout all phases of the system lifecycle.

G.1.4 Scope and Applicability

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 a model reproduces real-world and conceptual systems.

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 weapon system or C4I system, or an embedded simulation, will fall under the mandates of the JTA-Army main body, this domain annex, and any other applicable domain annexes. Interoperability of embedded simulations will be governed by this domain annex.

G.1.5 Technical Reference Model

There is no separate Technical Reference Model established for the M&S Domain.

G.1.6 Appendix Structure

This appendix is divided into three sections: the Domain Overview in Appendix G.1, the Domain Specific Standards in Appendix G. 2, and the Domain Specific Service Areas in Appendix G. 3.

G.2 DOMAIN SPECIFIC STANDARDS

G.2.1 Introduction

G.2.2 Information Processing Standards

G.2.2.1 Mandates

G.2.2.1.1 HLA Framework and Rules

HLA Rules: The rules comprise a set of underlying technical principles for the HLA. For federations, the rules address the requirement for a federation object model (FOM), object ownership and representation, and data exchange. For federates, the rules require a simulation object model (SOM), time management in accordance with HLA Runtime Infrastructure (RTI) management services, and certain restrictions on attribute ownership and updates.

- IEEE P1516, Modeling and Simulation (M&S) High Level Architecture (HLA) - Framework and Rules, Version 1.3, 23 April 1999.

G.2.2.1.2 HLA Interface Specification

HLA Interface Specification: HLA federates interact with an RTI (analogous to a special-purpose distributed operating system) to establish and maintain a federation and to support efficient information exchange among simulations and other federates. The HLA interface specification defines the nature of these interactions, which are arranged into sets of basic RTI services. On 11 November 1998 the Object Management Group (OMG) Board of Directors adopted the HLA Interface Specification v1.3 (services description and OMG IDL API). The following standards are mandated:

- OMG Facility for Distributed Simulation Systems, Version 1.0, dated 10 November 1998.
- IEEE P1516.1, Modeling and Simulation (M&S) High Level Architecture (HLA) Federate Interface Specification, Version 2, 23 April 1999.

G.2.2.1.3 HLA Object Model Template (OMT)

HLA Object Model Template: The HLA requires simulations (and other federates) and federations to each have an object model describing the entities represented in the simulations and the data to be exchanged across the federation. HLA Object Model Template prescribes the method for recording the information in the object models, including objects, attributes, interactions, and parameters, but it does not define the specific data (e.g., vehicles, unit types) that will appear in the object models

- IEEE P1516.2, Modeling and Simulation (M&S) High Level Architecture (HLA) Object Model Template (OMT) Specification, Version 1.3, 23 April 1999.

G.2.2.1.4 High Level Architecture (HLA) for Simulations

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.

G.2.2.2 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 as 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) <http://fdb.orlando.veda.com> is the Army's portion of CMMS.

Standard representation of the natural environments will offer stability in the M&S Research, Development, and 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.2.3 Information Transport Standards

Currently, there are no domain specific mandated or emerging standards identified for this section of the M&S Domain appendix.

G.2.4 Information-Modeling, Metadata, and Information-Exchange Standards

G.2.4.1 Mandates

G.2.4.1.1 Federation Execution Details Data Interchange Format (FED DIF)

This DIF is the input/output vehicle for sharing HLA initialization data. It contains data from the Federation Object Model as well as additional initialization data needed by the HLA Runtime Infrastructure (RTI) and other HLA initialization tools. The content of the FED DIF is compliant with the HLA Interface Specification referenced above.

- Federation Execution Details Data Interchange Format Version 1.3, February 1998.

G.2.4.1.2 Object Model Template Data Interchange Format

A data interchange format has been adopted as an input/output vehicle for sharing HLA object models presented in the standard Object Model Template (OMT) among object model developers and users.

- Object Model Template Data Interchange Format (OMT DIF), Version 1.3, February 1998.

G.2.4.1.3 Standard Simulator Database Interchange format (SIF)

A DoD data exchange standard (MIL-STD-1821) has been adopted as an input/output vehicle for sharing externally created visual terrain simulator databases among the operational system training and mission rehearsal communities.

- MIL-STD-1821, Standard Simulator Data Base (SSDB) Interchange Format (SIF) Design Standard, 17 June 1993, with Change of Notice 1, 17 April 1994, and Notice of Change 2, 17 February 1996.

G.2.4.2 Emerging Standards

G.2.4.2.1 SEDRIS

Synthetic Environment Data Representation and Interchange Specification (SEDRIS). No standard currently exists for comprehensively describing and interchanging environmental data in all domains (terrain, ocean, atmosphere, and space) among M&S applications supporting the broad range of acquisition, analysis, and training requirements. SIF will be replaced by SEDRIS. SEDRIS establishes a uniform and effective interchange specification for the pre-runtime distribution of source data and integrated databases. The specification encompasses a robust data model, data dictionary, and interchange format supported by read and write application programmer's interfaces (APIs), data viewers, a data model browser, and analytical verification and validation data model compliance tools. While designed to meet M&S community requirements, the interchange specification has the potential for also being used for natural environment data in DoD operational systems.

G.2.4.2.2 Object Model Data Dictionary

The Object Model Data Dictionary is being developed to support the development and reuse of Federation Object Models (FOMs) and Simulation Object Models (SOMs). This will greatly reduce the time needed to develop new HLA applications and transition legacy systems to the HLA. Initially, content standards are being developed based on the requirements of several

programs, which are early adopters of the HLA standards. The early adopter programs cover a broad range of simulation applications from engineering to analysis and multiple levels of aggregation from platform-level (previously addressed by IEEE 1278.1 Protocol Data Unit standards) to aggregate unit simulations (previously addressed by the Aggregate Level Simulation Protocol). The object model requirements of these programs are being consolidated into a common set of data elements, specifying both semantics and syntax. Where existing DoD standards do not exist, they will be developed through the HLA Object Data Dictionary process.

G.2.5 Human-Computer Interfaces

There are no domain specific mandated or emerging standards for this section.

G.2.6 Information Security

There are no domain specific mandated or emerging standards for this section.

G.3 DOMAIN SPECIFIC SERVICE AREAS

There are no domain specific service areas for the Modeling and Simulation Domain.

APPENDIX H - JTA-ARMY VERSION CHANGE MATRIX

A summary of the changes between JTA-Army Version 6.0 and JTA-Army Version 6.5 is contained in the tables below.

TABLE H-1 - SECTION 1, TECHNICAL ARCHITECTURE OVERVIEW CHANGES

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
1.1.3	Scope	Included	Clarified scope.	Clarified that the JTA-Army represents the minimum set of standards and guidelines for the acquisition of all systems…
1.2	Technical Architecture	Included	Updated order of JTA-A standards preference	Added allied standards such as NATO Standardization Agreements (STANAG)

TABLE H-2 - SECTION 2, INFORMATION PROCESSING STANDARDS CHANGES

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
Global	Cross-Area Services	Cross-Area Services	No longer referred to as Cross-Area Services	The application platform is no longer divided into service areas and cross-area services. The application platform entity is now composed of service areas, which include the former cross-area services. This reflects the DoD TRM structure.
2.2	DII COE I&RTS V4.0	Included	Updated Version, I&RTS V4.1	Update
2.2.1	DII COE I&RTS	Included	Deleted	Deleted mandate since it is already mandated in the previous section.
2.2.1.1	Biometric Technology Services	None	Added BioAPI Specification, Version 1.1, March 16, 2001.	New Standard
2.2.2.1.1	Programming Languages – Language Bindings and Object Linking	Included	Deleted	Standard is already mandated in the OS Services section.
2.2.2.1.2	User Interface	Included	T251: CDE 2.1 and	Replaced individual

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
	Services		MOTIF 2.1 Documentation - Full Set	CDE/Motif standards with the single documentation set.
2.2.2.1.2	User Interface Services	C507, C508, C509	C903, C904, C905	Update from X11R5 to X11R6.
2.2.2.1.2	User Interface Services	Win32 APIs	Updated	Changed from Programmers Reference Manual to Microsoft Platform SDK.
2.2.2.1.4.1	Document Interchange	HTML 4.0	HTML 4.01	Update
2.2.2.1.4.1	Document Interchange	XML 1.0	None	XML moved to section 4.2.8
2.2.2.1.4.2	Graphics Data Interchange	PNG, W3C Rec	PNG, IETF RFC	Update
2.2.2.1.4.7.1	Video Imagery	ANSI/SMPTE 293M-1996	None	Deleted
2.2.2.1.4.7.1	Video Imagery	VISP 1.4	MISP 1.7, ITU-R BT. 1358 ANSI/SMPTE 297M-1997 ANSI/SMPTE 291M-1996.	New table format. Add new standards.
2.2.2.1.4	Time-of-Day Interchange	ITU-R TF.460-4	None	Deleted
2.2.2.1.5	Graphic Services	OpenGL V1.1	OpenGL V1.2.1	Update
2.2.2.1.7	Operating System Services	None	Hand-held Devices	Added clarification on the non-applicability of the OS standards in this section to hand-held devices.
2.2.2.1.7	Operating System Services	IEEE 1003.5g, IEEE 1003.13, IEEE 1003.5b	Deleted Deleted Deleted	Draft standard. Poor industry support. Included in ISO/IEC 14519
2.2.2.1.7	Operating System Services	Win32 APIs	Updated	Changed from Programmers Reference Manual to Microsoft Platform SDK.
2.2.2.2.1	Internationalization Services	ISO/IEC 10646-1:1993	ISO/IEC 10646-1:2000	Update
2.2.2.1.11	Remote Procedure Computing	DCE	None	Deleted
2.2.2.1.11	Distributed-Object Computing	CORBA V2.2	CORBA V2.3.1	Updated discussion and standard.
2.2.2.1.11	Distributed-Object Computing	CORBA Services and Interworking Standards	None	Deleted. Interworking standards are included in the core document. Most services provided by the ORB vendor.

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
2.3	Virtual Machines	JVM	None	Deleted
2.3.1.2	Business Processing	OMG document bom/99-03-01	OMG document formal/2000-05-02	Update
2.3.2.2.1	Document Interchange	None	XHTML, XFORMS	Emerging
2.3.2.2.2	Graphics Data Interchange	None	PNG, MNG	Emerging
2.3.2.2.3	Still-Imagery Data Interchange	None	JPEG 2000	Emerging
2.3.2.2.4	Motion-Imagery Data Interchange	None	MISP 1.7; SMPTE RP210.2-2000 SMPTE EG37-2000 SMPTE 335M-2000 SMPTE 336M-2000 MISP 9716 MISP 9717 SMPTE 355M-2000	Emerging

TABLE H-3 - SECTION 3, INFORMATION TRANSFER STANDARDS CHANGES

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
3.2.1.1.1.1	Electronic Mail	Included	Update ACP standard	Update
3.2.1.1.1.9.2	Uniform Resource Identifier (URI)	Not Included	Included	JTA Alignment
3.2.1.1.2.2	Transmission Control Protocol (TCP)	Included	IETF RFC-2581	JTA Alignment
3.2.1.2	Video Teleconferencing (VTC) Standards	Included	Included	Revise text for clarity
Table 3-1:	VTC Standards For Data Rate 56-1920 Kbps	Included	Delete EIA-449	JTA Alignment
3.2.2.2.4	Integrated Services Digital Network (ISDN)	Included	Delete SR-3875, SR-4619, and SR-4620	Delete
3.2.2.2.6	Wireless LAN	Not Included	Mandate Wireless LAN standards	Standardize Combat Support and Sustainment implementations of non-sensitive Wireless Ethernet applications
3.2.3.3	Synchronous Optical Network (SONET) Transmission Facilities	Included	Update SONET standards	Update

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
3.2.1.1.2.1.1	TCP	Included	Included	Revise text for clarity
3.2.2.2.2	Point to Point	Included	EIA/TIA-530-A, Dec 1998	Update of standard
3.3.2	Emerging Network Standards	Included	Revise Third Generation PCS/Cellular paragraph	Revise text for clarity

TABLE H-4 - SECTION 4, INFORMATION-MODELING, METADATA, AND INFORMATION-EXCHANGE STANDARDS

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
4.2.1	Activity Modeling	Included	Revised (Changed Milestone II to Milestone B and Milestone III to Milestone C)	Revised for clarity
4.2.2	Data Modeling	Included	Change DDM to DDA	Update
4.2.3	Object Modeling	Included	Revise text. Revise web link.	Update
4.2.5.1	DoD Date Standards	Included	Deleted	Y2K issue
4.2.6.2.1	Bit-Oriented Formatted Messages	Included	Update standards. Delete STANAG 5516	Update
4.2.6.2.2	Character-based Formatted Messages	Included	Update MIL-STD-6040	Update to the latest release
4.2.8	XML-based Information Exchange	Not Included	Add new section.	New information exchange standards
4.2.8.1	XML Schema	Not Included	Add new section.	New information exchange standards
4.3.3	Object Modeling	Not Included	Add new section.	Clarification that XMI is UML-based metadata exchange standard
4.3.6	Information Exchange Standards	Included	Delete MIDS standards	Inappropriate for inclusion in the JTA-Army
4.3.8	XML-based Information Exchange	Not Included	Move 4.3.8.1 XML Transformation and 4.3.8.2 XML Parsing and Manipulating sections from Section 2	XML is more applicable to information exchange than information processing

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

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
5.2.1	General	Included	Revised	Update
5.2.2	Style Guides	Included	Update standards. Make	Update

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
			DoD HCI Style Guide, Version 4.0 emerging	
5.2.2.3	Domain-level Style Guides	Included	Revised	Clarity
5.3	Emerging Standards	Included	Revised text.	Update

TABLE H-6 - SECTION 6, INFORMATION SECURITY CHANGES

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
6.1.3	Background	DOD 5200.28 STD	Common Criteria (ISO 15408)	Update. Orange Book is now obsolete.
6.1.3	Background	TAFIM	Deleted	Update
6.2.1	Mandated Standards	DOD 5200.28 STD	Common Criteria (ISO 15408)	Update
6.2.1.1	Application Software Entity	DOD 5200.28 STD	Deleted	Update
6.2.1.2	Application Platform Entity	DOD 5200.28 STD	Deleted	Update
6.2.1.2	Application Platform Entity	Open Software Foundation	Open Group	Update
6.2.2.1	Application Software Entity	Included	Deleted Section	Update
6.2.2.5	Security Management Protocols	Included	Address Minimal Standards, SNMP V3	Update
6.2.2	Emerging Standards	Included	Renumber from 6.2.2.1 to 6.2.2.4 because of deleted section	Update
6.3.1	Mandates	Blank	Common Criteria (ISO 15408)	Update
6.3.1.1	Security Protocol	FIPS PUB 196	Moved to Sec. 6.3.2.6.3	Correction
6.3.1.1	Security Protocol	MIL-STD-2045-48501	Deleted	Update
6.3.1.2	DMS Interface	MD4000501-1.52, 30 January 1996	MD4000501-1.52b, 20 October 1997	Update
6.3.1.3	MISSI Cryptographic Algorithms	FIPS PUB 185 as Escrow standard	Deleted	Correction
6.3.1.4	MISSI Digital Signature Infrastructure	Included	Move to PKI Section (6.3.2.6.2)	Correction
6.3.1.5	Transport Mechanisms	Included	Deleted	Minimal Standards
6.3.1.6	Evaluation Criteria Security	Included	Deleted	Minimal Standards
6.3.1.7	Secure WWW Transactions	Included	Renumbered to Section 6.3.1.4	Update
6.3.2.3	Network Security	Draft FIPS 46-3	FIPS PUB 46-3	Update

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
6.3.2.5	Other	EDI	Deleted	Minimal Standards
6.3.2.6.2	Certificate Profiles	Included	Revise entire section	Update
6.3.2.6.6	Cryptography	Draft FIPS 46-3	FIPS PUB 46-3	Update
6.6	Security Related Documents	Included	Deleted, FIPS PUB 46-3 Referenced in Sec. 6.3.1.3	Minimal Standards

TABLE H-7 - APPENDIX D – COMBAT SUPPORT AND SUSTAINMENT DOMAIN CHANGES

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
D.2.2.1.3	Product Data Interchange	Included	Add new 2D symbology standard	Revised text and standards.
D.2.2.1.4	Electronic Data Interchange	Included	Add HL7 as the EDI standard for healthcare environments.	Update
D.2.3.2	Emerging Standards	Included	Delete IEEE 1073	Lack commercial support

TABLE H-8 - APPENDIX E - C3I DOMAIN CHANGES

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
E.2.2.1.1	Still-Imagery Data Interchange	Included	Delete text NITFS standards	Delete
E.2.3.1.3.2.1.3	Data Modems	Included	Update MIL STD-188-110A to MIL STD-188-110B	Update
E.2.3.1.3.2.2	Ultra High Frequency (UHF)	Included	Update standards	Update
E.2.3.1.3.2.4	Link 16 Transmission Standards	Included	Update text and standards to	Clarity
E.2.3.2	Emerging Standards	Included	Delete SLP standard	Delete
E.2.5.1	Mandates	Included	Delete domain-level style guides	Delete section

TABLE H-9 -APPENDIX F - WEAPON SYSTEMS DOMAIN CHANGES

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
F.2.2.1.1	Operating System Services	IEEE 1003.5	Deleted	Standard was moved to core
F.2.2.1.2	Section Deleted: Audio Data Interchange	ITU Recommendation G.726	Deleted	Video standard that does not support narrow bandwidths

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
F.2.2.1.2	Mapping Services	Section was F.2.2.2	WSMS API V2	Moved WSMS V2 to mandates
F.2.2.2.1	Mapping Services	Section was F.2.2.2	WSMS API V3	Cite new version in emerging section
F.2.2.2.3	Operating Environment Services	Section moved Contained OE API V1	F.3.3.1	Section moved and standard updated to V1.4 and mandated
F.3.3.2.1	Operating Environment Services	Emerging cited OE API V1	OE API V2	Updated emerging document version
F.3.5.2.2	Digital Television Standard	ATSC Document A/53	Deleted	Significant concerns have arisen with regards to the technical viability of is standard
F.3.5.2.1.1 Single Board Computers (SBCs) and Expansion Cards	Single Board Computers (SBCs) and Expansion Cards	IEEE P1386.1/D2.0 Physical/Environmental layers for Peripheral Component Interface (PCI) Mezzanine Cards (PMC), April 1995	IEEE P1386.1/D2.4 Physical/Environmental layers for Peripheral Component Interface (PCI) Mezzanine Cards (PMC), January 12, 2001	Changed bus section structure in JTA-A V6.5 and updated IEEE P1386.1 to latest standard
F.3.6.1	Combat Identification Services - Emerging	Aeronautical Telecommunications: Appendix 10, DOT FAA 1010.51A, DoD AIMS 97-1000, DoD AIMS 97-900, STANAG 4193, Part 1, STANAG 4193, Part 2, STANAG 4193, Part 3, STANAG 4193. Part 4	Aeronautical Telecommunications: Appendix 10, DOT FAA 1010.51A, DoD AIMS 97-1000, DoD AIMS 97-900	All STANAGS have been removed from the mandated section.
F.3.6.2	Combat Identification Services - Mandates	STANAG 4193, Part 5	Deleted	STANAG 4193 has been removed from CID Services

TABLE H-10 - APPENDIX F.AVS - AVIATION SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN CHANGES

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
F.AVS.2.5.1.1	Symbology	MIL-STD-1787B	MIL-STD-1787C	Update.
F.AVS.3.5.1	Bus Standards	MIL-STD-1773	Deleted	Aviation does not support this standard
F.AVS.3.5.2	Emerging Standards	HSDB PIB	Deleted	No official standards for these interfaces

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
F.AVS.3.5.1.1	Serial Buses Mandated	Not included	NCITS 288-1999, ANSI/NCITS 321 NCITS 332-1999 ANSI/NCITS X3.230-1994, Fibre Channel Physical and Signaling Interface (FC-PH), 1994 ANSI/NCITS X3.230-1994 Amendment 1:1996, Amendment 1 to ANSI/NCITS X3.230-1994 Fibre Channel Physical and Signaling Interface (FC-PH), 1996 ANSI/NCITS X3.230-1994 Amendment 2:1999, Amendment 2 to ANSI/NCITS X3.230-1994, Fibre Channel Physical and Signaling Interface (FC-PH), 1999 ANSI X3.272, ANSI X3.289 ANSI X3.297 ANSI X3.303, ARINC 429, Mark 33 ARINC 629	Add the citations for the Fibre Channel specs
F.AVS.3.5.2.1	Serial Buses Emerging	Not included	MIL-STD-1760C	
F.AVS.3.5.1.2.1	Backplane Buses Mandated	Not included	ANSI/VITA 1.1, VME64 Extensions, 1997	Extension to ANSI/VITA 1
F.AVS.3.5.2.1	Serial Buses Emerging	Not included	T11/Project 1237-D/1.4 (Draft), Information Technology -Fibre Channel - Audio Video (FC-AV) T11/Project 1332-D/Rev 1.6(Draft) Fibre Channel - Virtual Interface (FC-VI)	Fibre Channel specifications added to JTA-A 6.5

TABLE H-11 - APPENDIX F.GVS - GROUND VEHICLE SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN CHANGES

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
F.GVS.2.4.2.1	Tactical Information Exchange Standards (Bit Oriented	Not included	SLP-MSG-210, Revision, Sensor Link Protocol Message Set, 26 March 2001	The Sensor Link Protocol Message Set (SLP) was developed for use as a common interface between

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
	Formatted Messages)			electro-optical sensor systems and a diverse set of host computer systems
F.GVS.2.5.2	HCI Interface Standards Emerging Standards	HCI Style Guide for the Ground Vehicle Domain	Deleted	Does not have support needed to be mandated
F.GVS.3.5.1 .2.1	Backplane Buses Mandates	Not included	ANSI/VITA 1.1, VME64 Extensions, 1997	Extension to VME64
F.GVS.3.5.1 .6	Other Physical Resource Layer Interfaces	EIA 170 EIA 330 EIA 343 SMPTE 170M	Deleted	By direction of NIMA all analog motion imagery standards are to be phased out.

TABLE H-12 - APPENDIX F.MS - MISSILE SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN CHANGES

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
F.MS.2.2.2.1	Navigation Standard	BMD-P-SD-92-000002A BMD Navigation Standard	Deleted	Not an accepted DoD Standard. Data mandated in MIL-STD-6016
F.MS.2.3.2.1	Joint Range Extension (JRE) Application Protocol (JREAP)	Not Included	Joint Range Extension Application Protocol (JREAP) for Encapsulation into Joint Technical Architecture (JTA) Compliant Protocols, Joint Range Extension Application Protocol Working Group, Version 1.0, 19 July 2000	The joint protocol allows a JRE Gateway to process and manage incoming TADIL messages and redirect them to the appropriate destination via the appropriate media
F.MS.2.4.2	Emerging Standards Information-Modeling, Metadata, and Information-Exchange Standards	MIL-STD-6061A	Deleted	Mandated in the Core of JTA-A V6.5
F.MS.2.5.1.1	Symbology	MIL-STD-2525B	Delete the mandate for MIL-STD-2525B.	25625B is in the core.
F.MS.3.5.1	Mandates Physical Resources Layer Interfaces	IEEE 1496 IEEE 1275.2	Deleted	Mezzanine card standards are replaced with PCI standards

TABLE H-13 - APPENDIX F.MUS - MUNITION SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN CHANGES

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
F.MUS.2.4.2.1	Tactical Information Exchange Standards (Bit Oriented Formatted Messages	Not included	SLP-MSG-210, Revision, Sensor Link Protocol Message Set, 26 March 2001	The Sensor Link Protocol Message Set (SLP) was developed for use as a common interface between electro-optical sensor systems and a diverse set of host computer systems

TABLE H-14 - APPENDIX F.SS - SOLDIER SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN CHANGES

JTA-Army 6.0 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
F.SS.2.3.2	Emerging Standards Information Transfer Standards	ICD SLP 200	Deleted	Replaced by SLP message set see remark below
F.SS.2.4.2.1	Tactical Information Exchange Standards (Bit Oriented Formatted Messages	Not included	SLP-MSG-210, Revision, Sensor Link Protocol Message Set, 26 March 2001	The Sensor Link Protocol Message Set (SLP) was developed for use as a common interface between electro-optical sensor systems and a diverse set of host computer systems
F.SS.3.5.1	Mandates	EIA 170 SMPTE 170M	Deleted	By direction of NIMA all analog motion imagery standards are to be phased out.
F.SS.3.5.1.1	Serial Buses	Not included	IEEE-1394a-2000, IEEE Standard for a High Performance Serial Bus, Amendment 1.	Amendment to IEEE 1394
F.SS.3.5.2.1	Serial Buses	Not included	IEEE-1394b, Standard for a High Performance Serial Bus, 2001	Emerging standard

TABLE H-15 - APPENDIX G, MODELING & SIMULATION DOMAIN CHANGES

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
G.2.2.1.5	Data Management	Included Delete the whole section	Delete references to ODBC 3	ISO/IEC 9075-3 includes ODBC 3

JTA-Army 6.5 Section	Item	JTA-Army 6.0	JTA-Army 6.5	Remarks
	Services	referring to ODBC 3 because ISO/IEC 9075-3 includes ODBC 3		

This page was intentionally left blank.

APPENDIX I - JTA-ARMY COMPARISON TO JTA MATRIX

A summary of the mandate differences between JTA Version 3.1 and JTA-Army Version 6.5 is provided in the tables below.

TABLE I-1 SECTION 1 - TECHNICAL ARCHITECTURE OVERVIEW COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
1	Overview			No mandates

TABLE I-22 SECTION 2 - INFORMATION PROCESSING STANDARDS COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
2.2	DII COE I&RTS	I&RTS Version 3.1	I&RTS Version 4.1	Update
2.2.1.1	Biometric Technology Services	Not included in JTA	BioAPI Specification, Version 1.1, March 16, 2001	New support application service area
2.2.2.1.1.1	Programming languages	No mandates	ISO/IEC 8652 (Ada 95), ISO/IEC 9899 - C ANSI/ISO/IEC 14882-1998 - C++	Mandated 3GL languages: Ada 95, C and C++.
2.2.2.1.2	User Interface Services	X11R5	X11R6	Update
2.2.2.1.4.1	Document Interchange	HTML 4.0	HTML 4.01	Update
Table 2-1	DOCUMENT INTERCHANGE FORMATS	Not included yet	vCard	New Phone Listing
2.2.2.1.4.10	File compression	Not included	RFC-1952, GZIP File Format Specification	Mandate for file compression
2.2.2.1.5	Graphic Services	OpenGL 1.1	OpenGL 1.2.1	Update
2.2.2.1.7	Operating System Services	IEEE 1003.5g, IEEE 1003.13, IEEE 1003.5b	Deleted	Weak industry support
2.2.2.2.1.11	Distributed Computing Services	DCE	Deleted	Not being used in Army
2.2.2.2.1.11.1	Distributed-Object Computing	ORB V2.3	ORB V2.3.1	Update
2.2.2.2.4.2	Distributed-Object Computing	CORBA Services & CORBA Interworking	Deleted	Core standard is sufficient

TABLE I-3 SECTION 3 - INFORMATION TRANSFER STANDARDS COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
3.2.1.1.1.1	Electronic Mail	Included	Update ACP standard	Update
3.2.1.1.1.9.2	Uniform Resource Identifier (URI)	Not Included	Mandate new standards, IETF RFC-1738, IETF RFC 2396	Revise and replace the generic definitions in RFC 1738 and RFC 1808
3.2.1.1.2.2	Transmission Control Protocol (TCP)	Included	IETF RFC-2581	RFC 2581 obsoletes RFC 2001
3.2.1.1.2.4	Internet Protocol (IP)	Not included	Introduce new IGMPv2 standard, IETF RFC-2236	New mandate
3.2.1.2	Video Teleconferencing (VTC) Standards	Included	Included	Revise text for clarity
Table 3-1:	VTC Standards For Data Rate 56-1920 Kbps	Included	Delete EIA-449	EIA-449 is rescinded
3.2.2.1.1	IGMPv2	Not included	Introduce new IGMPv2 standard IETF RFC-2236	New mandate
3.2.2.2.1	Ethernet	Not included	Mandate Ethernet V2 framing, ISO/IEC 10038, Fast Ethernet, Gigabit Ethernet, ISO/IEC 15802-2 standards	New mandate
3.2.2.2.2	Point to Point	Not included	Mandate IETF RFC-1990, EIA 449	Update standards
3.2.2.2.4	ISDN	Deleted: ANSI T1.111 ANSI T1.112 ANSI T1.113 ANSI T1.114 SR-4620 SR-4619 SR-3888 SR-3887	Update the following standards: ANSI T1.601 –1999, ANSI T1.403.01-1999, and ANSI T1.610-1998. Delete proprietary standards: SR-3875, SR-4619, and SR-4620.	Update standards
3.2.2.2.5	Asynchronous Transfer Mode (ATM)	Deleted: ATM Forum, af-lane-0021.000, ATM Forum, af-lane-0038.000	Mandated new standards: ATM Forum, af-lane-0084.000, ATM Forum, af-lane-0093.000 ATM Forum, af-phy-0086.000	Update
3.2.2.2.6	Wireless LAN	Not Included	Mandate Wireless LAN standards	Standardize Combat Support and Sustainment implementations of non-sensitive Wireless Ethernet applications

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
3.2.3.3	Synchronous Optical Network (SONET) Transmission Facilities	Included	Update SONET standards	Update
3.3.2	Emerging Network Standards	Included	Revise Third Generation PCS/Cellular paragraph	Revise text for clarity

TABLE I-4 SECTION 4 - INFORMATION-MODELING, METADATA, AND INFORMATION-EXCHANGE STANDARDS

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
4.2.1	Activity Modeling	Included	Revised (Changed Milestone II to Milestone B and Milestone III to Milestone C)	Revised for clarity
4.2.2	Data Modeling	Included	Mandated C2CDM and DDA	Facilitate sharing data for interoperability. Army requirement to have system traceability to C2CDM and DDA.
4.2.3	Object Modeling	Not Included	Mandate UML.	Facilitate sharing OM data for interoperability
4.2.5.1	DoD Date Standards	Included	Deleted	Y2K issue
4.2.6.2.1	Bit-Oriented Formatted Messages	Included	Delete STANAG 5516, mandate MIL-STD-2045-47001B	Update
4.2.6.2.3	Database to Database Exchange	Not included	Database to Database Exchange will use standard data elements from the DDDS	Forward looking for interoperability
4.2.6.2.2	Character-based Formatted Messages	Included	Update MIL-STD-6040	Update to the latest release
4.2.8	XML-based Information Exchange	Not Included	Add new section.	Mandate new information exchange standards
4.2.8.1	XML Schema	Not Included	Add new section.	Mandate new information exchange standards
4.3.3	Object Modeling	Not Included	Add new section.	Clarification that XMI is UML-based metadata

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
				exchange standard
4.3.6	Information Exchange Standards	Included	Delete MIDS standards	Inappropriate for inclusion in the JTA-Army
4.3.8	XML-based Information Exchange	Not Included	Add 4.3.8.1 XML Transformation and 4.3.8.2 XML Parsing and Manipulating Sections	Mandate new information exchange standards

TABLE I-5 SECTION 5 - HUMAN-COMPUTER INTERFACES COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
5.2.1	General	Included	Revised	Update
5.2.2	Style Guides	Renamed GUI Style guides	Mandate MIL-STD-1472E, DoD HCI Style Guide, selected commercial GUI style guide, appropriate domain-level style guide	Mandate standards
5.2.2.3	Domain-level Style Guides	Included	Revise text. Move User Interface Specification for the DII to section D.2.5	Clarity
5.3	Emerging Standards	Included	Mandate DoD HCI Style Guide, Version 4.0 and delete MIL-PRF 89045.	Update

TABLE I-6 SECTION 6 - INFORMATION SECURITY COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
6.1.3	Background	DOD 5200.28 STD	Common Criteria (ISO 15408)	Update
6.2	Information Processing Security	DOD 5200.28 STD + Rainbow Series	Common Criteria (ISO 15408)	Update
6.2.2.5	Security Management Protocols	Included	Address Minimal Standards, SNMP V3	Update
6.3	Information Transport Security	DOD 5200.28 STD + Rainbow Series	Common Criteria (ISO 15408)	Update
6.3.1.1	Security Protocol	MIL-STD-2045-48501	Deleted	Update
6.3.2.6.6	Cryptography	Draft FIPS 46-3	FIPS PUB 46-3	Update

TABLE I-7 APPENDIX D - COMBAT SUPPORT AND SUSTAINMENT DOMAIN COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
D.2.2.1.3	Product Data Interchange	Included JTA CS.DTS.2.2.2.1 Product Data Interchange. PDF-417 as profiled by ANSI MH10.8.3M-1996, Material Handling – Unit Loads and Transport Packages – Two-Dimensional Symbols.	Mandate ANSI/US Product Data Association (PRO)-100-1996, MIL-PRF-28000A with Amendment 1, ANSI/PC-D-350D, FIPS Pub 172-1, ANSI/IEEE 1076, MIL-STD-1840C, ANSI/AIM BC-8	Mandate new standards, delete PDF-417
D.2.2.1.4	Electronic Data Interchange	Included	Mandate HL7 as the EDI standard for healthcare environments.	The HL7 version in FIPS 161-2 is obsolete.
D.2.2.1.5	Geospatial data interchange	Not included	FIPS PUB 173	Army Corps of Engineers mandates IAW Presidential Executive Order 12906.
D.2.3.2	Emerging Standards	Included	Delete IEEE 1073	Lack commercial support

TABLE I-8 APPENDIX E - C3I DOMAIN COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
E.2.3.1.3.2	Radio Communications, LF	MIL-STD-188-140A, Equipment Technical Design Standards for Common Long Haul/Tactical Radio Communications in the LF Band and Lower Frequency Bands, 1 May 1990	Not included	Not required by Army
E.2.3.1.3.2.6	JTIDS/MIDS Transmission Media, Link 16 Transmission Standards	Not included	SSDCB79S4000 - JTIDS System Segment Specification (Class 2 Terminal)	Army requirement
E.2.2.1.1	Still-Imagery Data Interchange	Included	Delete text NITFS standards	Delete
E.2.3.1.3.2.1.3	Data Modems	Included	Update MIL STD-188-110A to MIL STD-188-110B	Update

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
E.2.3	Common Data Link (CDL)	System Specification for the CDL Segment, Specification 7681990, System Description Document for CDL, Specification 7681996,	Not included	CDL standards do not meet Army criteria for a mandate, such as specification not a standard.
E.2.3.1.3.2.2	Ultra High Frequency (UHF)	Included	Update standards	Update
E.2.3.1.3.2.4	Link 16 Transmission Standards	Included	Update text and standards to	Clarity
E.2.3.1.5	Unattended MASINT Sensor Communication Standards	Interface Specification, Radio Frequency Transmission Interfaces for DoD Physical Security Systems, SEIWG-005	Not included	Documentation for Unattended MASINT Sensors (ICD) does not meet criteria for inclusion in the JTA-Army, such as specification not a standard.
E.2.3.2	Emerging Standards	Included	Delete SLP standard	Delete
E.2.4.1.1	Target/Threat Data Interchange Standards	NTSDS Database Implementation Description & Core Schema Definition, Version 1.2a, NTSDS Supplemental Schema Definition, Version 1.1,	Not included	Documentation for NTSDS (database description and schema definition) does not meet criteria for inclusion in the JTA-Army. Not a standard but a database schema.
E.2.5.1	Mandates	Included	Delete domain-level style guides	Delete section
E.2.5.1.1	Domain-level Style Guides	Not included	User Interface Specifications for the Defense Information Infrastructure.	DII COE pertains to C3I. Army requirement.
E	Nuclear Command and Control (NCC) Subdomain	HDR-SSS-01-S-REC0, Very Low Frequency/Low Frequency (VLF/LF) High Data Rate (HIDAR) Mode	Not included	The Army has no NCC technical or system requirements.

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
		Standard, NAVELEX 28687-0119-404; MEECN Message Processing Mode Standard, Emergency Action Procedures (EAP) Chairman Joint Chiefs of Staff (CJCS), EAP CJCS Volume VII "EAM Dissemination and Force Report Back (U)"		
E	Space Reconnaissance (SR) Subdomain	GR-253, Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria, EIA RS-422, Electrical Characteristics of Balanced Voltage Digital Interface Circuits	Not included	SONET and RS-422 are addressed in the core.
E.3	Payload-Platform Interface	SNU-84-1, Revision D Specification for USAF Standard Form, Fit, and Function (F3) Medium Accuracy Inertial Navigation Unit (INS), Telemetry Group, Range Commanders Council, Telemetry Standards, IRIG 106-96, Compatibility with the published AMPEX Digital Instrumentation Recorder DCRSi 240 User Manual, ANSI X3.175, 19-mm Type ID-1 Recorded Instrumentation – Digital Cassette Tape Form,	Not included	Does not meet criteria for inclusion in the JTA-Army, such as specification and user manual, not a standard.

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
		Instrumentation Group (IRIG) B format as defined in IRIG Serial Time Code Formats, IRIG 200-98		
E.3	Cryptologic systems, Subdomain-Specific Services and Interfaces	Peripheral Component Interconnect (PCI) Standard Version 2.2, PC Card Standard, ANSI/VITA 1-1994, American National Standard for VME64. IEEE 1155-1992, IEEE Standard for VMEbus Extensions for Instrumentation (VXI), IEEE 1101.2-1992, IEEE Standard for Mechanical Core Specifications for Conduction Cooled Eurocards.	Not included in this domain	Addressed in Weapon Systems, Appendix F, and subdomains

TABLE I-9 APPENDIX F - WEAPON SYSTEMS DOMAIN COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
F.2.2.1.1	Operating System Services	Not included	IEEE 1003.13: 1998	Update
F.2.2.1.1	Operating System Services	IEEE 1003.5c IEEE 1003.5f	Neither standard is included	1003.5f is not progressing
F.2.2.1.2	Mapping Services Mandates	Not included	Weapon System Mapping Services (WSMS) Application Programmer's Interface (API), Version 1.2, January 28, 2001, WSTAWG Doc# WSTA-AS-02-01	The Weapon System Mapping Services (WSMS) API provides a standardized interface to a set of mapping and mapping related services
F.2.2.2.1	Mapping Services Emerging	Not included	Weapon System Mapping Services (WSMS) Application Programmer's Interface (API),	The Weapon System Mapping Services

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
			Version 2.0, January 31, 2002, WSTAWG Doc# WSTA-AS-03-01.	(WSMS) Application Programmer's Interface (API) provides a standardized interface to a set of mapping and mapping related services
F.2.3.1.1	Map Data Loading	Not included	Map Data Loading Standard (MDLS)	NIMA generated map data to weapon system platforms. Needs further coordination in Joint community.
F.2.4.1	Information Exchange	Not included	U.S. Army Weapon Systems Application Program Interface (API) GuideBook: Volume II - API Specification Style Guide	Guidance to follow in the creation of APIs for the Weapon Systems Domain. Needs further coordination in Joint community.
F.2.4.2	Emerging Standards Information-Modeling, Metadata, and Information-Exchange Standards	Not included	IEEE 1076.4: VITAL Application-Specific Integrated Circuit (ASIC) Modeling Specification, 1995 (Provides VITAL timing and primitives).	Part of the 1076 group of Citations
F.2.5.1.1	Domain-level Style Guide	See section WS.2.5.3	U.S. Army Weapon Systems Human-Computer Interface (WSHCI) Style Guide	Style Guide provides design guidance. Needs further coordination in Joint community.
F.3.3.1.1	Operating Environment Services	Not included	Weapon Systems Technical Architecture Working Group (WSTAWG) Operating Environment (OE) Application Programmer's Interface (API), Volume I, OE Application Interface, Version 1.4, 13 January 12, 2001	Provides a standardized interface to a set of distributable objects that can be utilized in the creation of rehostable distributed real time embedded weapon systems applications.

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
F.3.3.2.1	Operating Environment Services	Not included	Weapon Systems Technical Architecture Working Group (WSTAWG) Operating Environment (OE) Application Programmer's Interface (API), Volume I, OE Application Interface, Version 2.0, 1 October 2001.	See above
F.3.5.1	PC Card standard	Not included	Personal Computer Memory Card International Association (PCMCIA)	Hot-swap peripheral standard
F.3.5.1	Mandates	ATSC Document A/53	Not Included	Standard in question
F.3.5.2.1.1	Single Board Computers (SBCs) and Expansion Cards	IEEE P1386.1/D2.0	IEEE P1386.1/D2.4	Update
F.3.6.1.1	Combat Identification (CI) Services Mandates	STANAG 4193	Not included	DoD AIMS standards are the proper specifications not the STANAGS
F.3.6.2	Combat Identification (CI) Services Emerging	Not included	STANAG 4579, Battlefield Target Identification Devices, 22 March 2000	Defines criteria for an interoperable NATO Battlefield Target Identification Device (BTID) for identification of forces on the battlefield

TABLE I-10 APPENDIX F.AVS - AVIATION SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
F.AVS.2.5.1.1	Symbology Mandates	MIL-STD-1787B Emerging	MIL-STD-1787C, Aircraft Display Symbology, 5 January 01	Update
F.AVS.2.5.1.2	Style Guide	Not included	Aviation Human-Computer Interface Style Guide	Addresses the design aspects common across most cockpit applications
F.AVS.3.5.1.1	Serial Buses Mandated	No bus standards cited in the JTA V3	MIL-STD-1553B with change notices 1,2,3, and 4 NCITS 288-1999 ANSI/NCITS 321	Accommodates the bus needs of the Aviation community

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
			NCITS 332 – 1999 ANSI/NCITS X3.230-1994 ANSI/NCITS X3.230-1994 Am 1 ANSI/NCITS X3.230-1994 Am 2 ANSI X3.272 ANSI X3.289 ANSI X3.297 ANSI X3.303 ARINC 429 ARINC 629 MIL-STD-1553B IEEE 1394 IEEE 1394a	
F.AVS.3.5.1.2.1	Backplane Buses	No bus standards cited in the JTA V3	ANSI/VITA 1, VME 64 ANSI/VITA 1.1, VME 64	Accommodates the bus needs of the Aviation community
F.AVS.3.5.2.1	Serial Buses	No bus standards cited in the JTA V3	T11/Project 1237-D/1.4 (Draft) T11/Project 1332-D/Rev 1.6 (Draft) MIL-STD-1760C IEEE 1394b	Accommodates the bus needs of the Aviation community

TABLE I-11 APPENDIX F.GVS - GROUND VEHICLE SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
F.GVS.2.4.2.1	Tactical Information Exchange Standards (Bit Oriented Formatted Messages)	Not included	SLP-MSG-210, Revision, Sensor Link Protocol Message Set, 26 March 2001	Provides for digital data exchange between sensors and host computing devices
F.GVS.3.5.1.2.1	Backplane Buses	Not included	ANSI/VITA 1.1, VME64	Extension to ANSI/VITA 1
F.GVS.3.5.1	Physical Resources Layer Interfaces	PCMCIA EIA 330 EIA 343-A EIA 170 SMPTE 170M	Not included	Analog TV standards removed
F.GVS.3.5.2.1	Serial Buses	Not included	SAE J1939 SAE J1587 SAE J1708	Serial Buses for heavy duty vehicles

TABLE I-12 APPENDIX F.MS - MISSILE SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
F.MS.2.2.2.1	Geospatial Date Interchange	Not included	- ANSI/AIAA R-004-1992, Recommended Practice for Atmospheric and Space Flight Vehicle Coordinate Systems	Extension to the WGS 84
F.MS.2.3.2.1	Joint Range Extension (JRE) Application Protocol (JREAP)	Not included	Joint Range Extension Application Protocol (JREAP) for Encapsulation into Joint Technical Architecture (JTA) Compliant Protocols, Joint Range Extension Application Protocol Working Group, Version 1.0, 19 July 2000	Allows a JRE Gateway to process and manage incoming TADIL messages and redirect them to the appropriate destination via the appropriate media
F.MS.3.5.1	Physical Resources Layer	Emerging 1553B PICMG ANSI X3.131 PCMCIA IEEE 1101.2 SAE J1850 ANSI/VITAVME64	IEEE 1101.2 Mandated No emerging standards	Bus standards section for MS subdomain has evolved to the necessary citations

TABLE I-13 APPENDIX F.MUS - MUNITION SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
F.MUS.2.4.2.1	Tactical Information Exchange Standards (Bit Oriented Formatted Messages)	Not included	SLP-MSG-210, Revision, Sensor Link Protocol Message Set, 26 March 2001	Common interface between electro-optical sensor systems and a diverse set of host computer systems
F.MUS.3.5.1	Physical Resources Layer	PCMCIA	Not included	In Appendix F Core
F.MUS. 3.6.1	System Safety Mandates	Not included	MIL-STD-882C, System Safety Program Requirements	Safety critical requirements
F.MUS.3.6.2	System Safety Emerging	Not included	Joint Software System Safety Handbook, Draft, 30 September 1997. STANAG 4404, Edition 1, Safety Requirements and Guidelines for	Being evaluated as emerging interface standards

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
			Munition Systems Related Safety Critical Systems, Draft, 29 August 1997. STANAG 4452, Edition 1, Safety Assessment of Munition-Related Computing Systems, Draft, 1 June 1997.	

TABLE I-14 APPENDIX F.SS - SOLDIER SYSTEMS SUBDOMAIN FOR THE WEAPON SYSTEMS DOMAIN COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
F.SS.2.4.2.1	Tactical Information Exchange Standards (Bit Oriented Formatted Messages)	Not included	SLP-MSG-210, Revision, Sensor Link Protocol Message Set, 26 March 2001	Common interface between electro-optical sensor systems and a diverse set of host computer systems
F.SS.3.5.1.1	Serial Buses Mandates	Not Included	IEEE 1394 IEEE 1394a	Firewire standard
F.SS.3.5.1	Serial Buses Mandates	WS.SS.3.5.2 EIA 170 SMPTE 170M	Not included	Analog TV standards deleted
F.SS.3.5.2.1	Serial Buses Emerging	Not included	IEEE 1394b	Firewire standard

TABLE I-15 APPENDIX G - MODELING AND SIMULATION DOMAIN COMPARISON

JTA-Army 6.5 Section	Item	JTA 3.1	JTA-Army 6.5	Remarks
G.2.2.1.5	Data Management Services	Addressed in the core	Delete references to ODBC 3	ISO/IEC 9075-3 includes ODBC 3