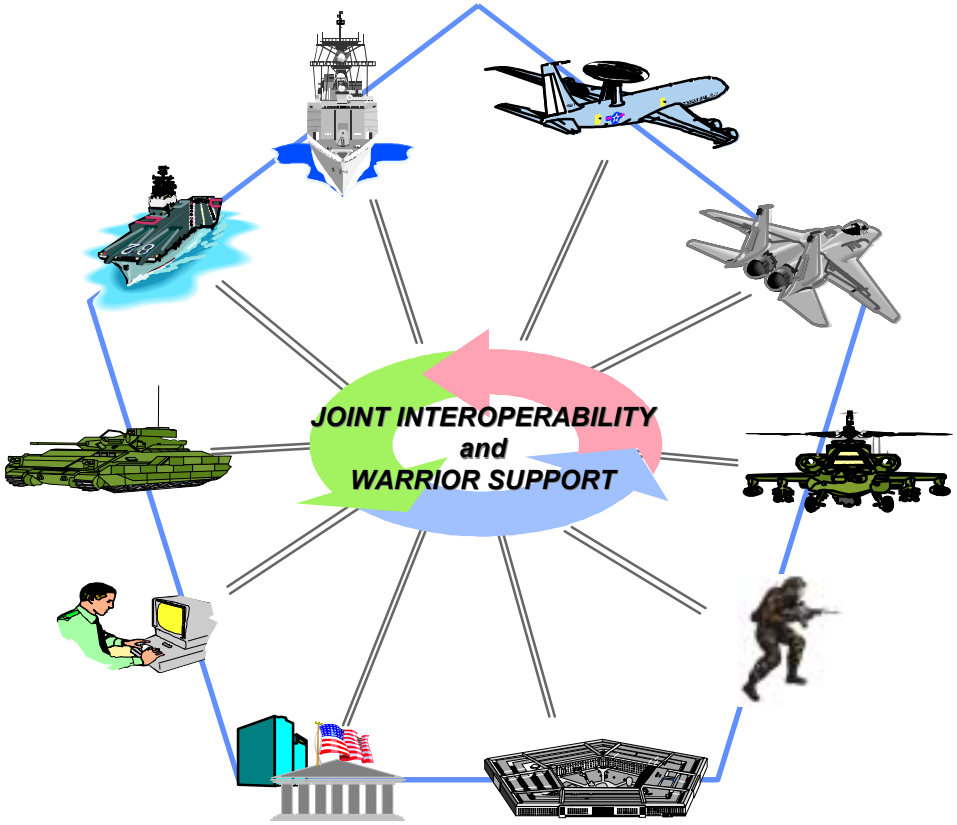
Department of Defense
Joint Technical Architecture



Version 4.0
2 April 2001

Distribution Statement A: Approved for public release; distribution unlimited.

All products mentioned in this document are trademarks of their respective companies.

Send any comments and suggestions via electronic mail to: jta@www.disa.mil

Executive Summary

Effective military operations must respond with a mix of forces, anywhere in the world, at a moment's notice. The ability for the information technology systems supporting these operations to interoperate—work together and exchange information—is critical to their success. The lessons learned from conflicts like Desert Shield/Desert Storm resulted in a new vision for the Department of Defense (DoD). Joint Vision 2010 (JV 2010) is the conceptual template for how America's Armed Forces will channel the vitality and innovation of their people, and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting. The DoD Joint Technical Architecture (JTA) is crucial to achieving JV 2010.

The JTA provides DoD systems with the basis for the needed seamless interoperability. The JTA defines the service areas, interfaces, and standards (JTA elements) applicable to all DoD systems, and its adoption is mandated for the management, development, and acquisition of new or improved systems throughout DoD. The JTA is structured into service areas based on the DoD Technical Reference Model (TRM). The DoD TRM originated from the Technical Architecture Framework for Information Management (TAFIM) and was developed to show which interfaces and content needed to be identified. These are depicted as major service areas in the DoD TRM.

Standards and guidelines in the JTA are stable, technically mature, and publicly available. Standards and guidelines that do not yet meet these criteria, but are expected to mature to meet them in the near-term (within three years), are cited as "emerging standards" in the expectation that they will be mandated in future versions of the JTA.

The JTA consists of two main parts: the JTA Core, and the JTA domains. The JTA Core contains the minimum set of JTA elements applicable to all DoD systems to support interoperability. The JTA annexes contain additional JTA elements applicable to specific functional domains (families of systems). These elements are needed to ensure interoperability of systems within each domain but may be inappropriate for systems in other domains. The current version of the JTA includes domains for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR); Combat Support; Modeling and Simulation; and Weapon Systems. Where subsets of an application domain (subdomain) have special interoperability requirements, the JTA includes subdomains containing JTA elements applicable to systems within that subdomain. The intention is that a system within a specific subdomain adopt the JTA elements contained in the relevant subdomain, the JTA elements contained in the parent domain, and the JTA elements contained in the JTA Core.

The JTA is complementary to, and consistent with, other DoD programs and initiatives aimed at the development and acquisition of effective, interoperable information systems. These include DoD's Specification and Standards Reform; Implementation of the Information Technology Management Reform Act (ITMRA); Defense Modeling and Simulation Initiative; Evolution of the DoD TRM; Defense Information Infrastructure Common Operating Environment (DII COE); and Open Systems Initiative.

Development of the JTA is a collaborative effort, conducted by the JTA Development Group (JTADG), directed by the Technical Architecture Steering Group (TASG), and approved by the Architecture Coordination Council (ACC). Members represent the DoD Components (Office of the Secretary of Defense [OSD], the Military Departments, the Office of the Joint Chiefs of Staff [OJCS], the Unified and Specified Combatant Commands, and the Defense Agencies) and components of the Intelligence Community.

The JTA is a living document and will continue to evolve with the technologies, marketplace, and associated standards upon which it is based.

Table of Contents

Executive Summary iii

Table of Contents v

List of Figures xxi

List of Tables xxiii

Section 1: Overview of the Department of Defense Joint Technical Architecture 1
1.1 Introduction 1
1.1.1 Purpose 2
1.1.2 Scope (Applicability) 2
1.1.3 Background 3
1.2 Architectures Defined 4
1.2.1 Operational Architecture View 4
1.2.2 Technical Architecture View 5
1.2.3 Systems Architecture View 5
1.3 Relationships between the C4ISR Architecture Framework 2.0 and the DoD JTA 5
1.4 Document Organization 5
1.4.1 General Organization 5
1.4.2 Information Technology Standards 6
1.4.3 Domains and Subdomains 7
1.4.4 Appendices (Appendix A, B, C, D, E, F) 8
1.5 DoD Technical Reference Model 9
1.6 Policy 11
1.6.1 Defense Information Infrastructure Common Operating Environment (DII COE) 11
1.6.2 Combined and Coalition Standardization and/or Interoperability 11
1.7 Key Considerations in Using the JTA 12
1.8 Element Normalization Rules 12
1.9 JTA Relationship to DoD Standards Reform 12
1.10 Standards Selection Criteria 13
1.11 Configuration Management 13

Section 2: Information Processing Standards 15
2.1 Introduction 15
2.1.1 Purpose 15
2.1.2 Scope 15
2.1.3 Background 15
2.2 Mandated Standards 15
2.2.1 Application Software Entity 15
2.2.2 Application Platform Entity 15
2.2.2.1 Service Areas 16
2.2.2.1.1 Software Engineering Services 16
2.2.2.1.2 User Interface Services 16
2.2.2.1.2.1 User Interface Service — POSIX 16
2.2.2.1.2.2 User Interface Service — Win32 17
2.2.2.1.3 Data Management Services 17
2.2.2.1.4 Data Interchange Services 18
2.2.2.1.4.1 Document Interchange 18
2.2.2.1.4.2 Graphics Data Interchange 19
2.2.2.1.4.3 Geospatial Data Interchange 20
2.2.2.1.4.4 Still Imagery Data Interchange 21
2.2.2.1.4.5 Motion Imagery Data Interchange 21
2.2.2.1.4.5.1 Video Systems 21
2.2.2.1.4.5.1.1 Video Imagery 22

2.2.2.1.4.5.1.2 Video Teleconference . . . 23
2.2.2.1.4.5.1.3 Video Support . . . 23
2.2.2.1.4.6 Audio Data Interchange . . . 24
2.2.2.1.4.6.1 Audio Associated with Video . . . 24
2.2.2.1.4.6.1.1 Audio for Video Imagery . . . 24
2.2.2.1.4.6.1.2 Audio for Video Teleconference . . . 25
2.2.2.1.4.6.1.3 Audio for Video Support . . . 25
2.2.2.1.4.6.2 Voice Encoder . . . 25
2.2.2.1.4.7 Data Interchange Storage Media . . . 25
2.2.2.1.4.8 Atmospheric and Oceanographic Data Interchange . . . 25
2.2.2.1.4.9 Time-of-Day Data Interchange . . . 26
2.2.2.1.5 Graphic Services . . . 26
2.2.2.1.6 Communications Services . . . 27
2.2.2.1.7 Operating System Services . . . 27
2.2.2.1.8 Internationalization Services . . . 28
2.2.2.1.9 Security Services . . . 28
2.2.2.1.10 System Management Services . . . 28
2.2.2.1.11 Distributed Computing Services . . . 28
2.2.2.1.11.1 Remote-Procedure Computing . . . 28
2.2.2.1.11.2 Distributed-Object Computing . . . 29
2.3 Emerging Standards . . . 30
2.3.1 Data Management . . . 30
2.3.2 Data Interchange . . . 31
2.3.2.1 Document Interchange . . . 31
2.3.2.2 Graphics Data Interchange . . . 32
2.3.2.2.1 Virtual Reality Modeling Language . . . 32
2.3.2.2.2 Multiple-Image Network Graphics . . . 32
2.3.2.2.3 Portable Network Graphics (PNG) . . . 32
2.3.2.3 Still Imagery Data Interchange . . . 32
2.3.2.4 Motion Imagery Data Interchange . . . 33
2.3.2.4.1 Video Systems . . . 33
2.3.2.4.1.1 Video Imagery . . . 33
2.3.2.4.1.2 Video Teleconference . . . 33
2.3.2.5 Multimedia Data Interchange . . . 34
2.3.2.6 Voice Encoder . . . 34
2.3.3 POSIX Operating Systems . . . 34
2.3.4 Distributed Computing Services . . . 35
2.3.4.1 Remote-Procedure Computing . . . 35
2.3.4.2 Distributed-Object Computing . . . 35
2.3.5 Support Application Services . . . 35
2.3.5.1 Environment Management . . . 35
2.3.5.2 Learning Technology . . . 36

Section 3: Information Transfer Standards . . . 37
3.1 Introduction . . . 37
3.1.1 Purpose . . . 37
3.1.2 Scope . . . 37
3.1.3 Background . . . 37
3.2 Mandated Standards . . . 37
3.2.1 Communications . . . 37
3.2.1.1 End-System Standards . . . 37
3.2.1.2 Host Standards . . . 37
3.2.1.2.1 Application Support Services . . . 38
3.2.1.2.1.1 Electronic Mail . . . 38
3.2.1.2.1.2 Directory Services . . . 38
3.2.1.2.1.2.1 X.500 Directory Services . . . 38
3.2.1.2.1.2.2 Lightweight Directory Access Protocol . . . 39
3.2.1.2.1.2.3 Domain Name System . . . 39
3.2.1.2.1.3 File Transfer . . . 39

3.2.1.2.1.4 Remote Terminal . . . 39
3.2.1.2.1.5 Network Time Synchronization . . . 39
3.2.1.2.1.6 Bootstrap Protocol . . . 39
3.2.1.2.1.7 Configuration Information Transfer . . . 40
3.2.1.2.1.8 Web Services . . . 40
3.2.1.2.1.8.1 Hypertext Transfer Protocol . . . 40
3.2.1.2.1.8.2 Uniform Resource Locator . . . 40
3.2.1.2.1.9 Connectionless Data Transfer . . . 40
3.2.1.2.2 Transport Services . . . 40
3.2.1.2.2.1 Transmission Control Protocol/User Datagram Protocol Over Internet Protocol . . . 40
3.2.1.2.2.1.1 Transmission Control Protocol . . . 40
3.2.1.2.2.1.2 User Datagram Protocol . . . 41
3.2.1.2.2.1.3 Internet Protocol . . . 41
3.2.1.2.2.2 Open Systems Interconnection Transport Over IP-Based Networks . . . 41
3.2.1.3 Video Teleconferencing Standards . . . 41
3.2.1.4 Facsimile Standards . . . 43
3.2.1.4.1 Analog Facsimile Standards . . . 43
3.2.1.4.2 Digital Facsimile Standards . . . 43
3.2.1.5 Imagery Dissemination Communications Standards . . . 43
3.2.1.6 Global Positioning System . . . 44
3.2.2 Network Standards . . . 44
3.2.2.1 Internetworking (Router) Standards . . . 44
3.2.2.1.1 Internet Protocol . . . 45
3.2.2.1.2 Internet Protocol Routing . . . 45
3.2.2.1.2.1 Interior Routers . . . 45
3.2.2.1.2.2 Exterior Routers . . . 45
3.2.2.2 Subnetworks . . . 46
3.2.2.2.1 Local Area Network Access . . . 46
3.2.2.2.2 Point-to-Point Standards . . . 46
3.2.2.2.3 Combat Net Radio Networking . . . 46
3.2.2.2.4 Integrated Services Digital Network . . . 47
3.2.2.2.5 Asynchronous Transfer Mode . . . 48
3.2.2.2.6 Gigabit Ethernet . . . 50
3.2.3 Transmission Media . . . 50
3.2.3.1 Military Satellite Communications . . . 50
3.2.3.1.1 Ultra High Frequency Satellite Terminal Standards . . . 50
3.2.3.1.1.1 5-KHz and 25-KHz Service . . . 50
3.2.3.1.1.2 5-KHz Demand-Assigned Multiple Access Service . . . 50
3.2.3.1.1.3 25-KHz Time Division Multiple Access/Demand-Assigned Multiple Access Service . . . 50
3.2.3.1.1.4 Data Control Waveform . . . 51
3.2.3.1.1.5 Demand-Assigned Multiple Access Control System . . . 51
3.2.3.1.2 Super High Frequency Satellite Terminal Standards . . . 51
3.2.3.1.2.1 Earth Terminals . . . 51
3.2.3.1.2.2 Phase-Shift Keying Modems . . . 51
3.2.3.1.3 Extremely High Frequency Satellite Payload and Terminal Standards . . . 51
3.2.3.1.3.1 Low Data Rate . . . 51
3.2.3.1.3.2 Medium Data Rate (MDR) . . . 52
3.2.3.1.4 Satellite State of Health Communication Standards . . . 52
3.2.3.2 Radio Communications . . . 53
3.2.3.2.1 Low Frequency and Very Low Frequency . . . 53
3.2.3.2.2 High Frequency . . . 53
3.2.3.2.2.1 High Frequency and Automatic Link Establishment . . . 53
3.2.3.2.2.2 Anti-Jamming Capability . . . 53
3.2.3.2.2.3 Data Modems . . . 53
3.2.3.2.3 Very High Frequency . . . 53
3.2.3.2.4 Ultra High Frequency . . . 53
3.2.3.2.4.1 Ultra High Frequency Radio . . . 53
3.2.3.2.4.2 Anti-Jamming Capability . . . 53
3.2.3.2.5 Super High Frequency . . . 54

3.2.3.2.6 Link 16 Transmission Standards . . . 54
3.2.3.3 Synchronous Optical Network Transmission Facilities . . . 54
3.2.4 Network and Systems Management . . . 54
3.2.4.1 Data Communications Management . . . 54
3.2.4.2 Telecommunications Management . . . 55
3.3 Emerging Standards . . . 55
3.3.1 End-System Standards . . . 55
3.3.1.1 Internet Standards . . . 55
3.3.1.2 Video Teleconferencing Standards . . . 56
3.3.1.3 Communication Protocols for High-Stress, Resource-Constrained Environments . . . 57
3.3.1.4 Global Positioning System . . . 58
3.3.2 Network Standards . . . 58
3.3.2.1 Wireless LAN . . . 58
3.3.2.2 ATM-Related Standards . . . 59
3.3.2.3 Network Quality of Service (QoS) Standards . . . 59
3.3.2.4 Personal Communications Services and Mobile Cellular . . . 60
3.3.2.5 International Mobile Telecommunications - 2000 . . . 60
3.3.2.6 Point-to-Point Standards . . . 61
3.3.3 Military Satellite Communications . . . 61
3.3.3.1 SHF Satellite Terminal Standards . . . 61
3.3.4 Radio Communications . . . 61
3.3.4.1 Link 22 Transmission Standards . . . 61
3.3.4.2 VHF . . . 61
3.3.5 Network Management . . . 61
3.3.5.1 Simple Network Management Protocol Version 3 (SNMPv3) . . . 61
3.3.5.2 Network Management Systems for Data Communications . . . 61

Section 4: Information Modeling, Metadata, and Information Exchange Standards . . . 63
4.1 Introduction . . . 63
4.1.1 Purpose . . . 63
4.1.2 Scope . . . 63
4.1.3 Background . . . 63
4.2 Mandated Standards . . . 64
4.2.1 Activity Modeling . . . 64
4.2.2 Data Modeling . . . 65
4.2.3 DoD Data Model Implementation . . . 65
4.2.4 DoD Data Definitions . . . 65
4.2.5 Information Exchange Standards . . . 66
4.2.5.1 Information Exchange Standards Applicability . . . 66
4.2.5.2 Tactical Information Exchange Standards . . . 66
4.2.5.2.1 Bit-Oriented Formatted Messages . . . 66
4.2.5.2.2 Character-Based Formatted Messages . . . 67
4.2.5.3 Binary Floating-Point Data Interchange . . . 67
4.2.6 Object Modeling . . . 67
4.3 Emerging Standards . . . 68
4.3.1 Object Modeling . . . 68
4.3.2 DoD Data Definitions . . . 68
4.3.3 Information Exchange Standards . . . 68
4.3.4 Data Modeling . . . 68

Section 5: Human-Computer Interface Standards . . . 71
5.1 Introduction . . . 71
5.1.1 Purpose . . . 71
5.1.2 Scope . . . 71
5.1.3 Background . . . 71
5.2 Mandated Standards . . . 71
5.2.1 General . . . 71
5.2.1.1 Character-Based Interfaces . . . 71
5.2.1.2 Graphical User Interface . . . 72

5.2.2 GUI Style Guides . . . 72
5.2.2.1 Commercial Style Guides . . . 72
5.2.2.1.1 X-Window Style Guides . . . 72
5.2.2.1.2 Windows Style Guide . . . 73
5.2.2.2 DoD Human-Computer Interface Style Guide . . . 73
5.2.2.3 Domain-Level Style Guides . . . 74
5.2.2.4 System-Level Style Guides . . . 74
5.2.3 Symbology . . . 74
5.3 Emerging Standards . . . 74
5.3.1 DoD HCI Style Guide . . . 74
5.3.2 Symbology . . . 75

Section 6: Information Security Standards . . . 77
6.1 Introduction . . . 77
6.1.1 Purpose . . . 77
6.1.2 Scope . . . 77
6.1.3 Background . . . 77
6.2 Mandated Standards . . . 78
6.2.1 Introduction . . . 78
6.2.2 Information Processing Security Standards . . . 78
6.2.2.1 Application Software Entity Security Standards . . . 78
6.2.2.2 Application Platform Entity Security Standards . . . 78
6.2.2.2.1 Authentication Security Standards . . . 79
6.2.3 Information Transfer Security Standards . . . 79
6.2.3.1 End-System Security Standards . . . 79
6.2.3.1.1 Host Security Standards . . . 79
6.2.3.1.1.1 Security Algorithms . . . 79
6.2.3.1.1.2 Security Protocols . . . 80
6.2.3.2 Network Security Standards . . . 80
6.2.3.3 Transmission Media Security Standards . . . 80
6.2.4 Information Modeling, Metadata, and Information Exchange Security Standards . . . 81
6.2.5 Human-Computer Interface Security Standards . . . 81
6.2.6 Web Security Standards . . . 81
6.3 Emerging Standards . . . 81
6.3.1 Introduction . . . 81
6.3.2 Information Processing Security Standards . . . 81
6.3.2.1 Application Software Entity Security Standards . . . 81
6.3.2.1.1 Web Security Standards . . . 81
6.3.2.2 Application Platform Entity Security Standards . . . 82
6.3.2.2.1 Software Engineering Services Security . . . 82
6.3.2.2.1.1 Generic Security Service-Application Program Interface Security . . . 82
6.3.2.2.2 Operating System Services Security . . . 82
6.3.2.2.2.1 Evaluation Criteria Security Standards . . . 82
6.3.2.2.2.2 Authentication Security Standards . . . 83
6.3.2.2.3 Distributed Computing Services Security Standards . . . 83
6.3.3 Information Transfer Security Standards . . . 83
6.3.3.1 End-System Security Standards . . . 83
6.3.3.1.1 Host Security Standards . . . 83
6.3.3.1.1.1 Security Protocols . . . 83
6.3.3.1.1.2 Medium-Assurance Public-Key Infrastructure Security Standards . . . 84
6.3.3.1.1.2.1 Background . . . 84
6.3.3.1.1.2.2 Certificate Profiles . . . 85
6.3.3.1.1.2.3 Operational Protocols and Exchange Formats . . . 85
6.3.3.1.1.2.4 Management Protocols . . . 86
6.3.3.1.1.2.5 Application Program Interfaces (APIs) . . . 86
6.3.3.1.1.2.6 Cryptography . . . 86
6.3.3.2 Network Security Standards . . . 86
6.3.3.2.1 Internetworking Security Standards . . . 87
6.3.3.2.2 Firewall Standards . . . 89

6.3.3.2.3 Virtual Private Network (VPN) . . . 90
6.3.3.2.4 Intrusion Detection Systems . . . 90
6.3.4 Information Modeling, Metadata, and Information Exchange Security Standards . . . 90
6.3.5 Human-Computer Interface Security Standards . . . 90

C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance Domain . . . 91
C4ISR.1 Domain Overview . . . 91
C4ISR.1.1 Purpose . . . 91
C4ISR.1.2 Background . . . 91
C4ISR.1.3 Domain Description . . . 91
C4ISR.1.4 Scope And Applicability . . . 91
C4ISR.1.5 Technical Reference Model . . . 92
C4ISR.1.6 Domain Organization . . . 92
C4ISR.2 Additions to the JTA Core . . . 92
C4ISR.2.1 Introduction . . . 92
C4ISR.2.2 Information Processing Standards . . . 92
C4ISR.2.2.1 Introduction . . . 92
C4ISR.2.2.2 Mandated Standards . . . 93
C4ISR.2.2.2.1 Still Imagery Data Interchange . . . 93
C4ISR.2.2.3 Emerging Standards . . . 94
C4ISR.2.2.3.1 Common Ground Moving Target Indicator Data Format . . . 94
C4ISR.2.3 Information Transfer Standards . . . 94
C4ISR.2.3.1 Introduction . . . 94
C4ISR.2.3.2 Mandated Standards . . . 94
C4ISR.2.3.2.1 Transmission Media . . . 94
C4ISR.2.3.2.1.1 Radio Communications . . . 94
C4ISR.2.3.2.1.1.1 Common Data Link Standards . . . 95
C4ISR.2.3.2.1.1.2 Unattended MASINT Sensor Communication Standards . . . 95
C4ISR.2.3.3 Emerging Standards . . . 95
C4ISR.2.4 Information Modeling, Metadata and Information Exchange Standards . . . 96
C4ISR.2.4.1 Introduction . . . 96
C4ISR.2.4.2 Mandated Standards . . . 96
C4ISR.2.4.2.1 Information Exchange Standards . . . 96
C4ISR.2.4.2.1.1 Target/Threat Data Interchange Standards . . . 96
C4ISR.2.4.3 Emerging Standards . . . 96
C4ISR.2.5 Human-Computer Interface Standards . . . 96
C4ISR.2.5.1 Introduction . . . 96
C4ISR.2.5.2 Mandated Standards . . . 96
C4ISR.2.5.3 Emerging Standards . . . 96
C4ISR.2.6 Information Security Standards . . . 97
C4ISR.2.6.1 Introduction . . . 97
C4ISR.2.6.2 Mandated Standards . . . 97
C4ISR.2.6.3 Emerging Standards . . . 97
C4ISR.3 Domain-Specific Service Areas . . . 97
C4ISR.3.1 Introduction . . . 97
C4ISR.3.2 Payload-Platform Interface . . . 97
C4ISR.3.2.1 Introduction . . . 97
C4ISR.3.2.2 Mandated Standards . . . 97
C4ISR.3.2.2.1 Internal Communications . . . 97
C4ISR.3.2.2.1.1 Fibre Channel . . . 97
C4ISR.3.2.2.1.2 FireWire . . . 98
C4ISR.3.2.2.2 Vehicle/Sensor Telemetry . . . 98
C4ISR.3.2.2.3 Mission Recorder . . . 98
C4ISR.3.2.3 Emerging Standards . . . 98

C4ISR.CRY: Cryptologic Subdomain . . . 99
C4ISR.CRY.1 Subdomain Overview . . . 99
C4ISR.CRY.1.1 Purpose . . . 99

C4ISR.CRY.1.2 Background . . . 99
C4ISR.CRY.1.3 Subdomain Description . . . 99
C4ISR.CRY.1.4 Scope . . . 99
C4ISR.CRY.1.5 Applicability . . . 100
C4ISR.CRY.1.6 Subdomain Organization. . . . 100
C4ISR.CRY.2 Standards in Addition to the JTA Core and C4ISR Domain . . . 100
C4ISR.CRY.2.1 Introduction . . . 100
C4ISR.CRY.2.2 Information Processing Standards . . . 100
C4ISR.CRY.2.2.1 Introduction . . . 100
C4ISR.CRY.2.2.2 Mandated Standards . . . 100
C4ISR.CRY.2.2.3 Emerging Standards . . . 100
C4ISR.CRY.2.3 Information Transfer Standards . . . 100
C4ISR.CRY.2.3.1 Introduction . . . 100
C4ISR.CRY.2.3.2 Mandated Standards . . . 100
C4ISR.CRY.2.3.3 Emerging Standards . . . 100
C4ISR.CRY.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 100
C4ISR.CRY.2.4.1 Introduction . . . 100
C4ISR.CRY.2.4.2 Mandated Standards . . . 101
C4ISR.CRY.2.4.3 Emerging Standards . . . 101
C4ISR.CRY.2.5 Human-Computer Interface Standards . . . 101
C4ISR.CRY.2.5.1 Introduction . . . 101
C4ISR.CRY.2.5.2 Mandated Standards . . . 101
C4ISR.CRY.2.5.3 Emerging Standards . . . 101
C4ISR.CRY.2.6 Information Security Standards. . . . 101
C4ISR.CRY.2.6.1 Introduction . . . 101
C4ISR.CRY.2.6.2 Mandated Standards . . . 101
C4ISR.CRY.2.6.3 Emerging Standards . . . 101
C4ISR.CRY.3 Subdomain-Specific Services and Interfaces. . . . 101
C4ISR.CRY.3.1 Introduction . . . 101
C4ISR.CRY.3.2 Mandated Standards. . . . 101
C4ISR.CRY.3.2.1 Small-Scale Special-Purpose Devices . . . 101
C4ISR.CRY.3.2.2 Backplanes and Circuit Cards . . . 102
C4ISR.CRY.3.2.3 Conduction Cooling . . . 102
C4ISR.CRY.3.3 Emerging Standards . . . 102
C4ISR.CRY.3.3.1 Backplanes and Circuit Cards . . . 102

C4ISR.NCC: Nuclear Command and Control Subdomain . . . 103
C4ISR.NCC.1 Subdomain Overview. . . . 103
C4ISR.NCC.1.1 Purpose . . . 103
C4ISR.NCC.1.2 Background . . . 103
C4ISR.NCC.1.3 Subdomain Description . . . 103
C4ISR.NCC.1.4 Scope and Applicability . . . 103
C4ISR.NCC.1.5 Technical Reference Model . . . 104
C4ISR.NCC.1.6 Subdomain Organization . . . 104
C4ISR.NCC.2 Additions to C4ISR Domain Service Areas . . . 104
C4ISR.NCC.2.1 Introduction. . . . 104
C4ISR.NCC.2.2 Information Processing Standards . . . 104
C4ISR.NCC.2.2.1 Introduction . . . 104
C4ISR.NCC.2.2.2 Mandated Standards. . . . 104
C4ISR.NCC.2.2.3 Emerging Standards . . . 104
C4ISR.NCC.2.3 Information Transfer Standards . . . 104
C4ISR.NCC.2.3.1 Introduction . . . 104
C4ISR.NCC.2.3.2 Mandated Standards . . . 105
C4ISR.NCC.2.3.3 Emerging Standards . . . 105
C4ISR.NCC.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 105
C4ISR.NCC.2.4.1 Introduction . . . 105
C4ISR.NCC.2.4.2 Mandated Standards . . . 105
C4ISR.NCC.2.4.3 Emerging Standards . . . 105
C4ISR.NCC.2.5 human-computer Interface Standards . . . 105

C4ISR.NCC.2.5.1 Introduction. . . . 105
C4ISR.NCC.2.5.2 Mandated Standards . . . 105
C4ISR.NCC.2.5.3 Emerging Standards. . . . 106
C4ISR.NCC.2.6 Information Security Standards . . . 106
C4ISR.NCC.2.6.1 Introduction. . . . 106
C4ISR.NCC.2.6.2 Mandated Standards . . . 106
C4ISR.NCC.2.6.3 Emerging Standards. . . . 106
C4ISR.NCC.3 Subdomain-Specific Service Areas. . . . 106

C4ISR.SR: Space Reconnaissance Subdomain . . . 107
C4ISR.SR.1 Subdomain Overview. . . . 107
C4ISR.SR.1.1 Purpose . . . 107
C4ISR.SR.1.2 Background . . . 107
C4ISR.SR.1.3 Subdomain Description . . . 107
C4ISR.SR.1.4 Scope and Applicability . . . 107
C4ISR.SR.1.5 DoD Technical Reference Model . . . 108
C4ISR.SR.1.5.1 SR TRM Defined. . . . 108
C4ISR.SR.1.6 Subdomain Organization . . . 108
C4ISR.SR.2 Additions to C4ISR Domain Service Areas and JTA Core. . . . 108
C4ISR.SR.2.1 Introduction. . . . 108
C4ISR.SR.2.2 Information Processing Standards . . . 108
C4ISR.SR.2.2.1 Introduction . . . 108
C4ISR.SR.2.2.2 Mandated Standards. . . . 108
C4ISR.SR.2.2.3 Emerging Standards . . . 108
C4ISR.SR.2.3 Information Transfer Standards . . . 109
C4ISR.SR.2.3.1 Introduction . . . 109
C4ISR.SR.2.3.2 Mandated Standards . . . 109
C4ISR.SR.2.3.2.1 Point-to-Point Standards . . . 109
C4ISR.SR.2.3.3 Emerging Standards . . . 109
C4ISR.SR.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 109
C4ISR.SR.2.4.1 Introduction . . . 109
C4ISR.SR.2.4.2 Mandated Standards . . . 109
C4ISR.SR.2.4.3 Emerging Standards . . . 109
C4ISR.SR.2.5 Human-Computer Interface Standards . . . 109
C4ISR.SR.2.5.1 Introduction . . . 109
C4ISR.SR.2.5.2 Mandated Standards . . . 109
C4ISR.SR.2.5.3 Emerging Standards . . . 109
C4ISR.SR.2.6 Information Security Standards . . . 110
C4ISR.SR.2.6.1 Introduction . . . 110
C4ISR.SR.2.6.2 Mandated Standards. . . . 110
C4ISR.SR.2.6.3 Emerging Standards . . . 110
C4ISR.SR.3 Subdomain-Specific Service Areas . . . 110

CS: Combat Support Domain . . . 111
CS.1 Domain Overview . . . 111
CS.1.1 Purpose . . . 111
CS.1.2 Background . . . 111
CS.1.3 Domain Description . . . 111
CS.1.4 Scope and Applicability . . . 112
CS.1.5 Technical Reference Model . . . 112
CS.1.6 Domain Organization . . . 112
CS.2 Additions to JTA Core . . . 112
CS.2.1 Introduction . . . 112
CS.2.2 Information Processing Standards. . . . 112
CS.2.2.1 Introduction. . . . 112
CS.2.2.2 Mandated Standards . . . 112
CS.2.2.2.1 Document Interchange . . . 112
CS.2.2.2.2 Graphics Data Interchange . . . 112
CS.2.2.2.3 Product Data Interchange . . . 113

CS.2.2.2.4 Electronic Data Interchange . . . 113
CS.2.2.3 Emerging Standards . . . 114
CS.2.2.3.1 Product Data Interchange . . . 114
CS.2.3 Information Transfer Standards . . . 116
CS.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 116
CS.2.4.1 Electronic Fingerprint Information Exchange Standards . . . 116
CS.2.5 Human-Computer Interface Standards . . . 116
CS.2.6 Information Security Standards . . . 116
CS.3 Domain-Specific Service Areas and Interfaces . . . 116
CS.3.1 Electronic Business/Electronic Commerce . . . 116
CS.3.1.1 Introduction . . . 116
CS.3.1.2 Mandated Standards . . . 116
CS.3.1.2.1 Smart Card Technology Standards . . . 116
CS.3.1.3 Emerging Standards . . . 117
CS.3.1.3.1 Smart Card Technology Standards . . . 117

CS.ATS: Automatic Test Systems Subdomain . . . 119
CS.ATS.1 Subdomain Overview . . . 119
CS.ATS.1.1 Purpose . . . 119
CS.ATS.1.2 Background . . . 119
CS.ATS.1.3 Subdomain Description . . . 120
CS.ATS.1.4 Scope and Applicability . . . 121
CS.ATS.1.5 Technical Reference Model . . . 121
CS.ATS.1.5.1 Hardware . . . 121
CS.ATS.1.5.2 Software . . . 122
CS.ATS.1.6 Subdomain Organization . . . 125
CS.ATS.1.7 Configuration Management . . . 125
CS.ATS.2 Additions to the JTA Core . . . 125
CS.ATS.2.1 Introduction . . . 125
CS.ATS.2.2 Information Processing Standards . . . 125
CS.ATS.2.2.1 Introduction . . . 125
CS.ATS.2.2.2 Mandated Standards . . . 125
CS.ATS.2.2.2.1 Data Interchange Services . . . 125
CS.ATS.2.2.2.1.1 Instrument Driver API Standards . . . 125
CS.ATS.2.2.2.1.2 Digital Test Data Formats . . . 126
CS.ATS.2.2.3 Emerging Standards . . . 126
CS.ATS.2.2.3.1 Data Interchange Services . . . 126
CS.ATS.2.2.3.1.1 Resource Adapter Interface . . . 126
CS.ATS.2.2.3.1.2 Diagnostic Processing Standards . . . 126
CS.ATS.2.2.3.1.3 UUT Test Requirements Data Standards . . . 127
CS.ATS.2.3 Information Transfer Standards . . . 127
CS.ATS.2.3.1 Introduction . . . 127
CS.ATS.2.3.2 Mandated Standards . . . 127
CS.ATS.2.3.2.1 Instrument Communication Manager Standards . . . 127
CS.ATS.2.3.3 Emerging Standards . . . 128
CS.ATS.2.3.3.1 Maintenance Test Data and Services . . . 128
CS.ATS.2.3.3.2 Product Design Data . . . 128
CS.ATS.2.3.3.3 Built-In Test Data . . . 128
CS.ATS.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 129
CS.ATS.2.4.1 Introduction . . . 129
CS.ATS.2.4.2 Mandated Standards . . . 129
CS.ATS.2.4.3 Emerging Standards . . . 129
CS.ATS.2.5 Human-Computer Interface Standards . . . 129
CS.ATS.2.5.1 Introduction . . . 129
CS.ATS.2.5.2 Mandated Standards . . . 129
CS.ATS.2.5.3 Emerging Standards . . . 129
CS.ATS.2.6 Information Security Standards . . . 129
CS.ATS.2.6.1 Introduction . . . 129
CS.ATS.2.6.2 Mandated Standards . . . 129

CS.ATS.2.6.3 Emerging Standards . . . 129
CS.ATS.3 Subdomain-Specific Service Areas . . . 129
CS.ATS.3.1 Software Engineering Services . . . 129
CS.ATS.3.2 Data/Information Services . . . 129
CS.ATS.3.2.1 Introduction . . . 129
CS.ATS.3.2.2 Mandated Standards . . . 129
CS.ATS.3.2.3 Emerging Standards . . . 129
CS.ATS.3.3 Platform/Environment Services . . . 130
CS.ATS.3.3.1 Introduction . . . 130
CS.ATS.3.3.2 Mandated Standards . . . 130
CS.ATS.3.3.2.1 System Framework Standards . . . 130
CS.ATS.3.3.3 Emerging Standards . . . 130
CS.ATS.3.3.3.1 Receiver/Fixture Interface . . . 130
CS.ATS.3.3.3.2 Switching Matrix Interface . . . 130
CS.ATS.3.3.4 Other Interfaces . . . 131
CS.ATS.3.3.4.1 Computer Asset Controller Interface . . . 131
CS.ATS.3.3.4.2 Host Computer Interface . . . 131
CS.ATS.3.3.4.3 Instrument Control Bus Interface . . . 131
CS.ATS.3.3.4.4 Instrument Command Language . . . 131
CS.ATS.3.3.4.5 Application Development Environments . . . 131

CS.DTS: Defense Transportation System Subdomain . . . 133
CS.DTS.1 Subdomain Overview . . . 133
CS.DTS.1.1 Purpose . . . 133
CS.DTS.1.2 Background . . . 133
CS.DTS.1.3 Subdomain Description . . . 133
CS.DTS.1.4 Scope and Applicability . . . 133
CS.DTS.1.5 Technical Reference Model . . . 133
CS.DTS.1.6 Subdomain Organization . . . 133
CS.DTS.2 Additions to JTA Core and Combat Support Domain . . . 133
CS.DTS.2.1 Introduction . . . 133
CS.DTS.2.2 Information Processing Standards . . . 134
CS.DTS.2.2.1 Introduction . . . 134
CS.DTS.2.2.2 Mandated Standards . . . 134
CS.DTS.2.2.2.1 Product Data Interchange . . . 134
CS.DTS.2.3 Information Transfer Standards . . . 134
CS.DTS.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 134
CS.DTS.2.5 Human-Computer Interface Standards . . . 134
CS.DTS.2.6 Information Security Standards . . . 134
CS.DTS.2.6.1 Introduction . . . 134
CS.DTS.2.6.2 Mandated Standards . . . 134
CS.DTS.2.6.3 Emerging Standards . . . 134
CS.DTS.2.6.3.1 Internetworking Security Standards . . . 134
CS.DTS.3 Subdomain-Specific Service Areas . . . 135

CS.MED: Medical Subdomain . . . 137
CS.MED.1 Subdomain Overview . . . 137
CS.MED.1.1 Purpose . . . 137
CS.MED.1.2 Background . . . 137
CS.MED.1.3 Subdomain Description . . . 137
CS.MED.1.4 Scope and Applicability . . . 137
CS.MED.1.5 Technical Reference Model . . . 138
CS.MED.1.6 Subdomain Organization . . . 138
CS.MED.2 Additions to JTA Core and Combat Support Domain . . . 138
CS.MED.2.1 Introduction . . . 138
CS.MED.2.2 Information Processing Standards . . . 138
CS.MED.2.2.1 Introduction . . . 138
CS.MED.2.2.2 Mandated Standards . . . 138
CS.MED.2.2.2.1 Medical Electronic Data Interchange . . . 138

CS.MED.2.2.2.2 Retail Pharmacy Claims Electronic Data Interchange . . . 138
CS.MED.2.2.2.3 Medical Still Imagery Data Interchange . . . 139
CS.MED.2.2.2.4 Medical Information Exchange Standards . . . 139
CS.MED.2.2.3 Emerging Standards . . . 139
CS.MED.2.2.3.1 Commercial Electronic Data Interchange . . . 139
CS.MED.2.2.3.2 Retail Pharmacy Claim Electronic Data Interchange . . . 140
CS.MED.2.3 Information Transfer Standards . . . 140
CS.MED.2.3.1 Introduction . . . 140
CS.MED.2.3.2 Mandated Standards . . . 140
CS.MED.2.3.3 Emerging Standards . . . 140
CS.MED.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 140
CS.MED.2.4.1 Introduction . . . 140
CS.MED.2.4.2 Mandated Standards . . . 140
CS.MED.2.4.3 Emerging Standards . . . 141
CS.MED.2.5 Human-Computer Interface Standards . . . 141
CS.MED.2.5.1 Introduction . . . 141
CS.MED.2.5.2 Mandated Standards . . . 141
CS.MED.2.5.3 Emerging Standards . . . 141
CS.MED.2.6 Information Security Standards . . . 141
CS.MED.2.6.1 Introduction . . . 141
CS.MED.2.6.2 Mandated Standards . . . 141
CS.MED.2.6.3 Emerging Standards . . . 141

M&S: Modeling and Simulation Domain . . . 143
M&S.1 Domain Overview . . . 143
M&S.1.1 Purpose . . . 143
M&S.1.2 Background . . . 143
M&S.1.3 Domain Description . . . 144
M&S.1.4 Scope and Applicability . . . 144
M&S.1.5 Technical Reference Model . . . 145
M&S.1.6 Domain Organization . . . 145
M&S.2 Additions to the JTA Core . . . 145
M&S.2.1 Introduction . . . 145
M&S.2.2 Information Processing Standards . . . 145
M&S.2.2.1 Introduction . . . 145
M&S.2.2.2 Mandated Standards . . . 145
M&S.2.2.2.1 HLA Framework and Rules . . . 145
M&S.2.2.2.2 HLA Federate Interface Specification . . . 146
M&S.2.2.2.3 HLA Object Model Template . . . 146
M&S.2.2.3 Emerging Standards . . . 146
M&S.2.3 Information Transfer Standards . . . 146
M&S.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 147
M&S.2.4.1 Introduction . . . 147
M&S.2.4.2 Mandated Standards . . . 147
M&S.2.4.2.1 Federation Execution Details Data Interchange Format . . . 147
M&S.2.4.2.2 Object Model Template Data Interchange Format . . . 147
M&S.2.4.2.3 Standard Simulator Database Interchange Format . . . 147
M&S.2.4.3 Emerging Standards . . . 147
M&S.2.4.3.1 Synthetic Environment Data Representation and Interchange Specification (SEDRIS) 147
M&S.2.4.3.2 Object Model Data Dictionary . . . 148
M&S.2.5 Human-Computer Interface Standards . . . 148
M&S.2.6 Information Security Standards . . . 148
M&S.3 Domain-Specific Service Areas . . . 148

WS: Weapon Systems Domain . . . 149
WS.1 Domain Overview . . . 149
WS.1.1 Purpose . . . 149
WS.1.2 Background . . . 149
WS.1.3 Domain Description . . . 149

WS.1.4 Scope And Applicability . . . 149
WS.1.5 DoD Technical Reference Model . . . 150
WS.1.5.1 DoD TRM Views . . . 150
WS.1.5.1.1 Performance Environment . . . 151
WS.1.5.1.2 Application Hardware Environment . . . 151
WS.1.5.2 Hierarchy of TRM Views . . . 151
WS.1.6 Domain Organization . . . 151
WS.2 Additions to the JTA Core . . . 152
WS.2.1 Introduction . . . 152
WS.2.2 Information Processing Standards . . . 152
WS.2.2.1 Introduction . . . 152
WS.2.2.2 Mandated Standards . . . 152
WS.2.2.3 Emerging Standards . . . 152
WS.2.2.3.1 Operating System Services . . . 152
WS.2.2.3.2 Real-Time Common Object Request Broker Architecture . . . 152
WS.2.3 Information Transfer Standards . . . 152
WS.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 152
WS.2.4.1 Introduction . . . 152
WS.2.4.2 Mandated Standards . . . 152
WS.2.4.3 Emerging Standards . . . 153
WS.2.5 Human-Computer Interface Standards . . . 153
WS.2.5.1 Introduction . . . 153
WS.2.5.2 Mandated Standards . . . 153
WS.2.5.3 Emerging Standards . . . 153
WS.2.6 Information Security Standards . . . 153
WS.3 Domain-Specific Service Areas and Interfaces . . . 154
WS.3.1 Introduction . . . 154
WS.3.2 Application Software Layer Interfaces . . . 154
WS.3.3 System Services Layer Interfaces . . . 154
WS.3.4 Resource Access Services Layer Interfaces . . . 154
WS.3.5 Physical Resources Layer Interfaces . . . 154
WS.3.5.1 Introduction . . . 154
WS.3.5.2 Mandated Standards . . . 154
WS.3.5.3 Emerging Standards . . . 154
WS.3.6 Combat Identification Services . . . 154
WS.3.6.1 Identification Friend or Foe . . . 155
WS.3.6.1.1 Introduction . . . 155
WS.3.6.1.2 Mandated Standards . . . 155
WS.3.6.1.3 Emerging Standards . . . 156

WS.AV: Aviation Subdomain . . . 157
WS.AV.1 Subdomain Overview . . . 157
WS.AV.1.1 Purpose . . . 157
WS.AV.1.2 Background . . . 157
WS.AV.1.3 Subdomain Description . . . 157
WS.AV.1.4 Scope And Applicability . . . 157
WS.AV.1.5 Technical Reference Model . . . 157
WS.AV.1.6 Subdomain Organization . . . 157
WS.AV.2 Additions to the JTA Core . . . 157
WS.AV.2.1 Introduction . . . 157
WS.AV.2.2 Information Processing Standards . . . 157
WS.AV.2.2.1 Introduction . . . 157
WS.AV.2.2.2 Mandated Standards . . . 157
WS.AV.2.2.3 Emerging Standards . . . 158
WS.AV.2.2.3.1 Service-Area Standards . . . 158
WS.AV.2.2.3.1.1 Operating System Services . . . 158
WS.AV.2.3 Information Transfer Standards . . . 158
WS.AV.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 158
WS.AV.2.5 Human-Computer Interface Standards . . . 158

WS.AV.2.5.1 Introduction . . . 158
WS.AV.2.5.2 Mandated Standards . . . 158
WS.AV.2.5.2.1 Symbology . . . 158
WS.AV.2.5.3 Emerging Standards . . . 158
WS.AV.2.6 Information Security Standards . . . 158
WS.AV.3 Subdomain-Specific Service Areas . . . 158
WS.AV.3.1 Global Air Traffic Management Standards . . . 158
WS.AV.3.1.1 Introduction . . . 159
WS.AV.3.1.2 Mandated Standards . . . 159
WS.AV.3.1.3 Emerging Standards . . . 159

WS.GV: Ground Vehicle Subdomain . . . 161
WS.GV.1 Subdomain Overview . . . 161
WS.GV.1.1 Purpose . . . 161
WS.GV.1.2 Background . . . 161
WS.GV.1.3 Subdomain Description . . . 161
WS.GV.1.4 Scope And Applicability . . . 161
WS.GV.1.5 Technical Reference Model . . . 161
WS.GV.1.6 Subdomain Organization . . . 161
WS.GV.2 Additions to the JTA Core . . . 161
WS.GV.2.1 Introduction . . . 161
WS.GV.2.2 Information Processing Standards . . . 161
WS.GV.2.2.1 Introduction . . . 161
WS.GV.2.2.2 Mandated Standards . . . 161
WS.GV.2.2.3 Emerging Standards . . . 162
WS.GV.2.3 Information Transfer Standards . . . 162
WS.GV.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 162
WS.GV.2.5 Human-Computer Interface Standards . . . 162
WS.GV.2.6 Information Security Standards . . . 162
WS.GV.3 Subdomain-Specific Service Areas and Interfaces . . . 162
WS.GV.3.1 Introduction . . . 162
WS.GV.3.2 Application Software Layer Interfaces . . . 162
WS.GV.3.3 System Services Layer Interfaces . . . 162
WS.GV.3.4 Resource Access Services Layer Interfaces . . . 162
WS.GV.3.5 Physical Resources Layer Interfaces . . . 163
WS.GV.3.5.1 Introduction . . . 163
WS.GV.3.5.2 Mandated Standards . . . 163
WS.GV.3.5.3 Emerging Standards . . . 163

WS.MD: Missile Defense Subdomain . . . 165
WS.MD.1 Subdomain Overview . . . 165
WS.MD.1.1 Purpose . . . 165
WS.MD.1.2 Background . . . 165
WS.MD.1.3 Subdomain Description . . . 166
WS.MD.1.4 Scope and Applicability . . . 166
WS.MD.1.5 Technical Reference Model . . . 166
WS.MD.1.6 Subdomain Organization . . . 166
WS.MD.2 Additions to the JTA Core . . . 166
WS.MD.2.1 Introduction . . . 166
WS.MD.2.2 Information Processing Standards . . . 167
WS.MD.2.2.1 Introduction . . . 167
WS.MD.2.2.2 Mandated Standards . . . 167
WS.MD.2.2.3 Emerging Standards . . . 167
WS.MD.2.2.3.1 Navigation Standard . . . 167
WS.MD.2.2.3.2 Real-Time Defense Information Infrastructure Common Operating Environment (DII COE) . . . 167
WS.MD.2.3 Information Transfer Standards . . . 167
WS.MD.2.3.1 Introduction . . . 167
WS.MD.2.3.2 Mandated Standards . . . 167

WS.MD.2.3.2.1 Time Synchronization. . . . 167
WS.MD.2.3.3 Emerging Standards . . . 167
WS.MD.2.3.3.1 Joint Range Extension (JRE) Application Protocol (JREAP). . . . 167
WS.MD.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 167
WS.MD.2.4.1 Introduction . . . 167
WS.MD.2.4.2 Mandated Standards. . . . 167
WS.MD.2.4.2.1 Bit-Oriented Formatted Messages. . . . 167
WS.MD.2.4.3 Emerging Standards . . . 168
WS.MD.2.5 Human-Computer Interface Standards. . . . 168
WS.MD.2.5.1 Introduction . . . 168
WS.MD.2.5.2 Mandated Standards. . . . 168
WS.MD.2.5.2.1 Symbology . . . 168
WS.MD.2.6 Information Security Standards . . . 168
WS.MD.3 Subdomain-Specific Service Areas and Interfaces . . . 168

WS.MS: Missile Systems Subdomain . . . 169
WS.MS.1 Subdomain Overview. . . . 169
WS.MS.1.1 Purpose . . . 169
WS.MS.1.2 Background. . . . 169
WS.MS.1.3 Subdomain Description. . . . 169
WS.MS.1.4 Scope and Applicability. . . . 169
WS.MS.1.5 Technical Reference Model . . . 169
WS.MS.1.6 Subdomain Organization . . . 170
WS.MS.2 Additions to JTA Core . . . 170
WS.MS.2.1 Introduction. . . . 170
WS.MS.2.2 Information Processing Standards . . . 170
WS.MS.2.3 Information Transfer Standards . . . 170
WS.MS.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 170
WS.MS.2.5 Human-Computer Interface Standards. . . . 170
WS.MS.2.6 Information Security Standards . . . 170
WS.MS.3 Subdomain-Specific Services and Interfaces. . . . 170
WS.MS.3.1 Introduction. . . . 170
WS.MS.3.2 Application Software Layer Interfaces . . . 170
WS.MS.3.3 System Services Layer Interfaces . . . 170
WS.MS.3.4 Resource Access Services Layer Interfaces . . . 170
WS.MS.3.5 Physical Resources Layer Interfaces . . . 170
WS.MS.3.5.1 Introduction . . . 171
WS.MS.3.5.2 Mandated Standards. . . . 171
WS.MS.3.5.3 Emerging Standards . . . 171

WS.MUS: Munition Systems Subdomain . . . 173
WS.MUS.1 Subdomain Overview . . . 173
WS.MUS.1.1 Purpose . . . 173
WS.MUS.1.2 Background . . . 173
WS.MUS.1.3 Subdomain Description . . . 173
WS.MUS.1.4 Scope and Applicability . . . 173
WS.MUS.1.5 Technical Reference Model . . . 174
WS.MUS.1.6 Subdomain Organization. . . . 174
WS.MUS.2 Additions to the JTA Core . . . 174
WS.MUS.2.1 Introduction . . . 174
WS.MUS.2.2 Information Processing Standards. . . . 174
WS.MUS.2.2.1 Introduction. . . . 174
WS.MUS.2.2.2 Mandated Standards. . . . 174
WS.MUS.2.2.3 Emerging Standards . . . 174
WS.MUS.2.3 Information Transfer Standards . . . 174
WS.MUS.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 174
WS.MUS.2.5 Human-Computer Interface Standards . . . 174
WS.MUS.2.6 Information Security Standards . . . 174
WS.MUS.3 Subdomain-Specific Services and Interfaces . . . 174

WS.MUS.3.1 Introduction . . . 174
WS.MUS.3.2 Application Software Layer Interfaces . . . 175
WS.MUS.3.3 System Services Layer Interfaces . . . 175
WS.MUS.3.4 Resource Access Services Layer Interfaces . . . 175
WS.MUS.3.5 Physical Resources Layer Interfaces . . . 175
WS.MUS.3.5.1 Introduction . . . 175
WS.MUS.3.5.2 Mandated Standards . . . 175
WS.MUS.3.5.3 Emerging Standards . . . 176

WS.SS: Soldier Systems Subdomain . . . 177
WS.SS.1 Subdomain Overview . . . 177
WS.SS.1.1 Purpose . . . 177
WS.SS.1.2 Background . . . 177
WS.SS.1.3 Subdomain Description . . . 177
WS.SS.1.4 Scope and Applicability . . . 177
WS.SS.1.5 Technical Reference Model . . . 178
WS.SS.1.6 Subdomain Organization . . . 178
WS.SS.2 Subdomain-Specific Standards . . . 178
WS.SS.2.1 Introduction . . . 178
WS.SS.2.2 Information Processing Standards . . . 178
WS.SS.2.3 Information Transfer Standards . . . 178
WS.SS.2.4 Information Modeling, Metadata, and Information Exchange Standards . . . 178
WS.SS.2.5 Human-Computer Interface Standards . . . 178
WS.SS.2.6 Information Security Standards . . . 178
WS.SS.3 Subdomain-Specific Services and Interfaces . . . 178
WS.SS.3.1 Introduction . . . 178
WS.SS.3.2 Application Software Layer Interfaces . . . 179
WS.SS.3.3 System Services Layer Interfaces . . . 179
WS.SS.3.4 Resource Access Services Layer Interfaces . . . 179
WS.SS.3.5 Physical Resources Layer Interfaces . . . 179
WS.SS.3.5.1 Introduction . . . 179
WS.SS.3.5.2 Mandated Standards. . . . 179
WS.SS.3.5.3 Emerging Standards . . . 179

Appendix A: Abbreviations and Acronyms 181

Appendix B: DoD JTA List of Mandated and Emerging Standards 197

Appendix C: Document Sources 199

Appendix D: References 209

Appendix E: JTA Relationship to DoD Standards Reform 211

Appendix F: Glossary 213

List of Figures

Figure 1-1: DoD Warfighter Information Technology Environment 1

Figure 1-2: Architecture Views Relationships 4

Figure 1-3: JTA Hierarchy Model 7

Figure 1-4: DoD Technical Reference Model (DoD TRM) 10

Figure 5-1: HCI Development Guidance 73

Figure C4ISR-1: JTA Hierarchy Model 92

Figure CS-1: JTA Hierarchy Model. 111

Figure CS.ATS-1: Generic ATS Architecture. 120

Figure CS.ATS-2: Hardware Interfaces 122

Figure CS.ATS-3: Test Program Sets Runtime Interfaces 123

Figure CS.ATS-4: Test Product Sets Development Interfaces 124

Figure M&S-1: JTA Hierarchy Model 144

Page intentionally left blank.

List of Tables

Table 1-1: Interface Translation Table 10

Table 1-2: JTA Development Group (JTADG) Voting Membership 14

Table 2-1: Common Document Interchange Formats 19

Table 2-2: Mandated Standards from MISP 1.6, Chapter 2.0 22

Table 2-3: Emerging Standards from MISP 1.6, Chapter 2.0 33

Table 3-1: ITU-T/EIA Standards Profiled by FTR 1080A-1998, Appendix A 42

Page intentionally left blank.

Section 1: Overview of the Department of Defense Joint Technical Architecture

1.1 Introduction

Warfighter battlespace is complex and dynamic, requiring timely and informed decisions by all levels of military command. There is an unprecedented increase in the amount of data and information necessary to conduct operational planning and combat decision-making. Information concerning targets, movement of forces, condition of equipment, levels of supplies, and disposition of assets—both friendly and unfriendly—must be provided to joint commanders and their forces. Therefore, information must flow quickly and seamlessly among all tactical, strategic, and supporting elements.

As shown in Figure 1-1, warfighters must be able to work together within and across Services in ways not totally defined in today's operational concepts and/or architectures. They must be able to obtain and use intelligence from national and theater assets that may be widely dispersed geographically. Today's split-base/reach-back concept requires them to obtain their logistics and administrative support from both home bases and deployed locations. All of this requires that information flow quickly and seamlessly among DoD's sensors, processing and command centers, shooters, and support activities to achieve dominant battlefield awareness and move inside the enemy's decision loop.

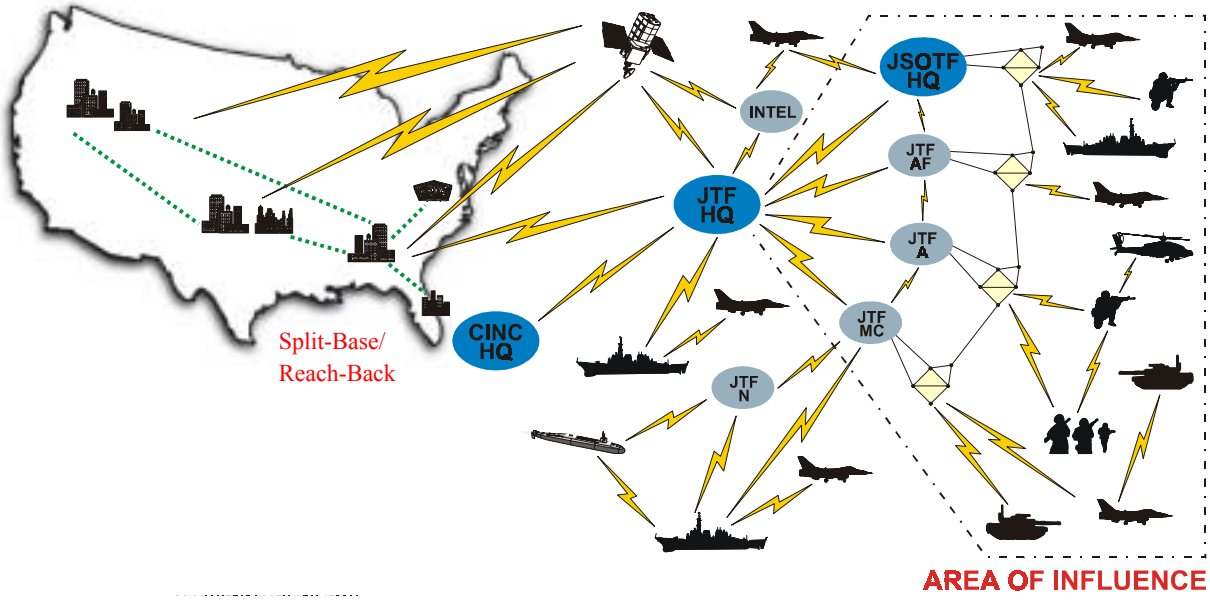


Figure 1-1: DoD Warfighter Information Technology Environment

The DoD Joint Technical Architecture (hereinafter referred to as the JTA) provides the minimum set of standards that, when implemented, facilitates this flow of information in support of the warfighter. The JTA standards promote:

- A distributed information processing environment in which applications are integrated.
- Applications and data independent of hardware to achieve true integration.
- Information transfer capabilities to ensure seamless communications within and across diverse media.
- Information in a common format with a common meaning.

- Common human-computer interfaces for users, and effective means to protect the information.

The current JTA concept is focused on the interoperability and standardization of information technology (IT).

1.1.1 Purpose

Section 1 provides an overview of the JTA. It includes the JTA purpose, scope, background, and applicability; introduces basic architecture concepts; and discusses the selection criteria for standards incorporated in the document.

Also addressed are the roles of the DoD Technical Reference Model and the Combined Communications-Electronics Board (CCEB).

The JTA improves and facilitates the ability of our systems to support joint and combined operations in an overall investment strategy.

The JTA:

- Provides the foundation for interoperability among all tactical, strategic, and combat support systems.
- Mandates IT standards and guidelines for DoD system development and acquisition that will facilitate interoperability in joint and coalition force operations. These standards are to be applied in concert with DoD standards reform.
- Communicates to industry DoD's preference for open system, standards-based products and implementations.
- Acknowledges the direction of industry's standards-based development.

1.1.2 Scope (Applicability)

The JTA is considered a living document and will be updated periodically as a collaborative effort among the DoD Components (Commands, Services, and Agencies) to leverage technology advancements, standards maturity, open systems, commercial product availability, and changing requirements.

The JTA is critical to achieving the envisioned objective of a cost-effective, seamlessly integrated environment. Achieving and maintaining this vision requires interoperability:

- Within a Joint Task Force/Commander in Chief (CINC) Area of Responsibility (AOR).
- Across CINC AOR boundaries.
- Between strategic and tactical systems.
- Within and across Services and Agencies.
- From the battlefield to the sustaining base.
- Among U.S., Allied, and Coalition forces.
- Across current and future systems.

This version of the JTA mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. The applicable mandated standards in the JTA 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.*** The JTA is used by

anyone involved in the management, development, or acquisition of new or improved systems within DoD. Specific guidance for implementing this JTA is provided in the separate DoD Component JTA implementation plans. Operational requirements developers are cognizant of the JTA in developing requirements and functional descriptions. System developers use the JTA to facilitate the achievements of interoperability for new and upgraded systems (and the interfaces to such systems). System integrators use it to foster the integration of existing and new systems.

The JTA is updated periodically with continued DoD Component participation.

1.1.3 Background

The evolution of a national military strategy in the post-Cold War era and the lessons learned from conflicts like Desert Shield/Desert Storm have resulted in a new vision for DoD. Joint Vision 2010 is the conceptual template for how America's Armed Forces will channel the vitality and innovation of their people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting. This template provides a common direction to our Services in developing their unique capabilities within a joint framework of doctrine and programs as they prepare to meet an uncertain and challenging future. The Chairman of the Joint Chiefs of Staff said in Joint Vision 2010, "The nature of modern warfare demands that we fight as a joint team. This was important yesterday, it is essential today, and it will be even more imperative tomorrow."

Joint Vision 2010 (JV 2010) creates a broad framework for understanding joint warfare in the future, and for shaping Service programs and capabilities to fill our role within that framework. JV 2010 defines four operational concepts: Precision Engagement, Dominant Maneuver, Focused Logistics, and Full Dimensional Protection. These concepts combine to ensure that American forces can secure Full Spectrum Dominance, i.e., the capability to dominate an opponent across the range of military operations and domains. Furthermore, Full Spectrum Dominance requires Information Superiority, i.e., the capability to collect, process, analyze, and disseminate information while denying an adversary the ability to do the same. Interoperability is crucial to Information Superiority.

Recognizing the need for joint operations in combat and the reality of a shrinking budget, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD[C3I]) issued a memorandum on 14 November 1995 to Command, Service, and Agency principals involved in the development of Command, Control, Communications, Computers, and Intelligence (C4I) systems. This directive tasked them to "reach a consensus of a working set of standards" and "establish a single, unifying DoD technical architecture that will become binding on all future DoD C4I acquisitions" so that "new systems can be born joint and interoperable, and existing systems will have a baseline to move toward interoperability."

A Joint Technical Architecture Working Group (JTAWG), chaired by ASD(C3I), was formed, and its members agreed to use the U.S. Army Technical Architecture (ATA) as the starting point for the JTA. Version 1.0 of the JTA was released on 22 August 1996 and was immediately mandated by the Under Secretary of Defense, Acquisition and Technology (USD[A&T]) and ASD(C3I) for all new and upgraded C4I systems in DoD.

JTA Version 2.0 development began in March 1997 under the direction of a Technical Architecture Steering Group (TASG), co-chaired by ASD(C3I) and USD(AT&L) Open Systems Joint Task Force (OSJTF). The applicability and scope of Version 2.0 of the JTA was expanded to include the information technology in all DoD systems.

JTA Version 3.0 development began in June 1998. JTA Version 3.0 includes additional subdomains and incorporated the newly developed DoD Technical Reference Model (DoD TRM). JTA Version 3.1 mandated a Gigabit Ethernet standard.

JTA Version 4.0 development began in November 1999. JTA Version 4.0 removes the Orange Book mandate and mandates the Common Criteria.

1.2 Architectures Defined

The C4ISR Architecture Framework (CAF) provides information addressing the development and presentation of architectures. The framework provides the rules, guidance, and product descriptions for developing and presenting architectures to ensure a common denominator for understanding, comparing, and integrating architectures across and within DoD.

An architecture is defined as the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time. DoD has implemented this by defining an interrelated set of views: operational, system, and technical. Figure 1-2 shows the relationship among the three views. The definitions are provided here to ensure a common understanding of the three views.[1]

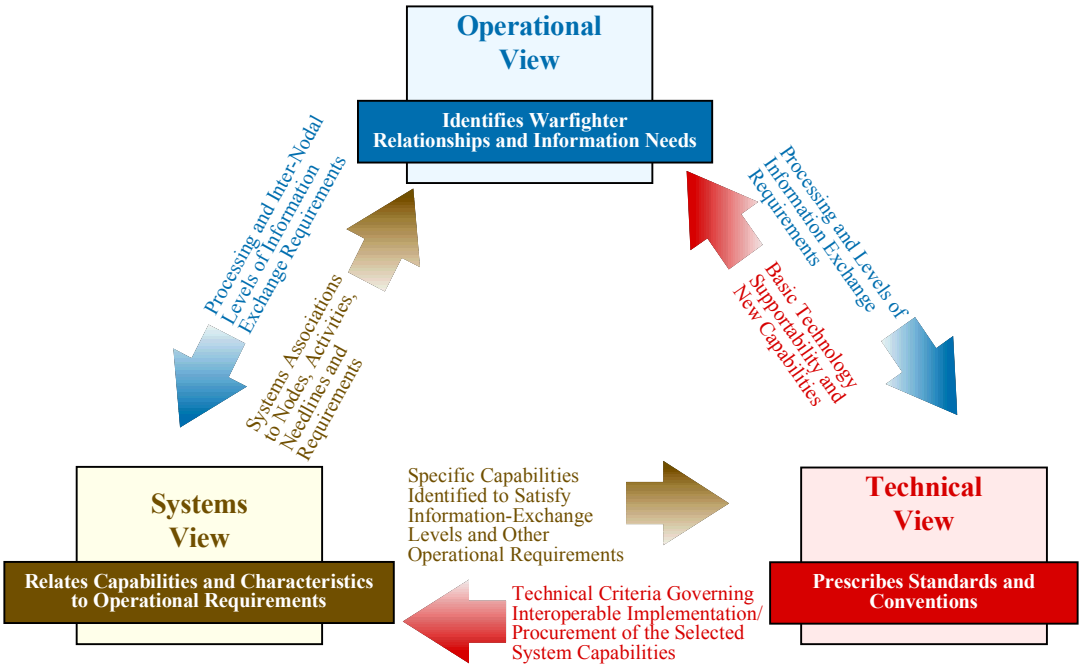


Figure 1-2: Architecture Views Relationships

1.2.1 Operational Architecture View

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.

It 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

[1] These definitions are extracted from the C4ISR Architecture Framework 2.0. The definitions and the products required by the framework focus on information technology. However, the concepts described can be applied to a wide range of technologies.

frequency of 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.

1.2.2 Technical Architecture View

The technical architecture (TA) view is the minimal set of rules governing the arrangement, interaction, and interdependence of system 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 established, and product lines are developed. The technical architecture 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.

1.2.3 Systems Architecture View

The systems architecture (SA) view is a description, including graphics, of 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 it 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.

1.3 Relationships between the C4ISR Architecture Framework 2.0 and the DoD JTA

The C4ISR Architecture Framework defines the technical architecture view and a set of standard technical products for DoD use. The JTA is one of the Universal Reference Resources named in the CAF. The JTA is the primary source document to the essential and supporting Technical Architecture products defined in the C4ISR Architecture Framework. Standards chosen from the JTA and other sources to meet system and operational requirements are incorporated into the technical architecture View.

1.4 Document Organization

The JTA is organized into a main body, followed by domains, subdomains, and a set of appendices. This section describes the structure of the document.

1.4.1 General Organization

The main body identifies the “Core” set of JTA elements consisting of service areas, interfaces, and standards. Each section of the main body, except for the overview, is divided into four subsections as follows:

- **Introduction, Purpose, Scope, and Background:** These subsections are for information purposes only. They define the purpose and scope of the document and the section and provide background descriptions and definitions that are unique to this section.
- **Service Area and Services:** This subsection describes the technical overview of the Services in this section.
- **Mandated Standards:** 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 suitable for inclusion within Requests for Proposals (RFPs), Statements of Work (SOWs), or Statements of Objectives (SOOs).

- **Emerging Standards:** This subsection provides an information-only description of standards that are candidates for possible addition to the JTA mandates. Each emerging standard is clearly identified on a separate dashed (–) line. The purpose of listing these candidates is to help the program manager determine those areas 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. Emerging standards may be implemented, but shall not be used in lieu of a mandated standard.

1.4.2 Information Technology Standards

The JTA Core, or main body, addresses commercial and government standards common to most DoD information technology, grouped into categories each of which addresses a set of functions common to most DoD IT systems. The information technology categories are:

- **Information Processing Standards:** Section 2 describes Government and commercial information processing standards DoD uses to develop integrated, interoperable systems that meet the warfighters' information processing requirements.
- **Information Transfer Standards:** Section 3 describes the information transfer 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 System Network (DISN).
- **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 object 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). This section also mandates information standards, including message formats.
- **Human-Computer Interface Standards**: Section 5 provides a common framework for Human-Computer Interface (HCI) design and implementation in DoD systems. The objective is the standardization of user interface implementation options, enabling DoD applications to appear and behave in a reasonably consistent manner. The section specifies HCI design guidance, mandates, and standards.
- **Information Security Standards**: 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 sections 2 through 5.

The JTA Core establishes the minimum set of rules governing information technology across all DoD systems. Additional domain-specific mandates are found in the corresponding domains and subdomains. They include standards for information processing, information transfer, the structure of information and data, human-computer interface for information entry and display, and information system security. Information technology includes any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

1.4.3 Domains and Subdomains

The JTA Core contains the common service areas, interfaces, and standards (JTA elements) applicable to all DoD systems to support interoperability. Recognizing that there are additional JTA elements common within families of related systems (i.e., domains), the JTA adopted the domain and subdomain notion. A domain represents a grouping of systems sharing common functional, behavioral, and operational requirements. JTA domains and subdomains are intended to exploit the common service areas, interfaces, and standards supporting interoperability across systems within the domain and/or subdomain.

A JTA domain contains domain-specific JTA elements applicable within the specified family of systems to further support interoperability within the systems represented in the domain—in addition to those included in the JTA Core. A domain may be composed of multiple subdomains. Subdomains represent the decomposition of a domain (referred to as the subdomain's parent domain) into a subset of related systems, exploiting additional commonalities and addressing variances within the domain. A subdomain contains domain-specific JTA elements applicable within the specified family of systems to further support interoperability within the systems represented in the subdomain—in addition to those included in the JTA Core and in the parent domain. The relationships between the JTA Core, domains, and subdomains currently in the JTA are illustrated in Figure 1-3.

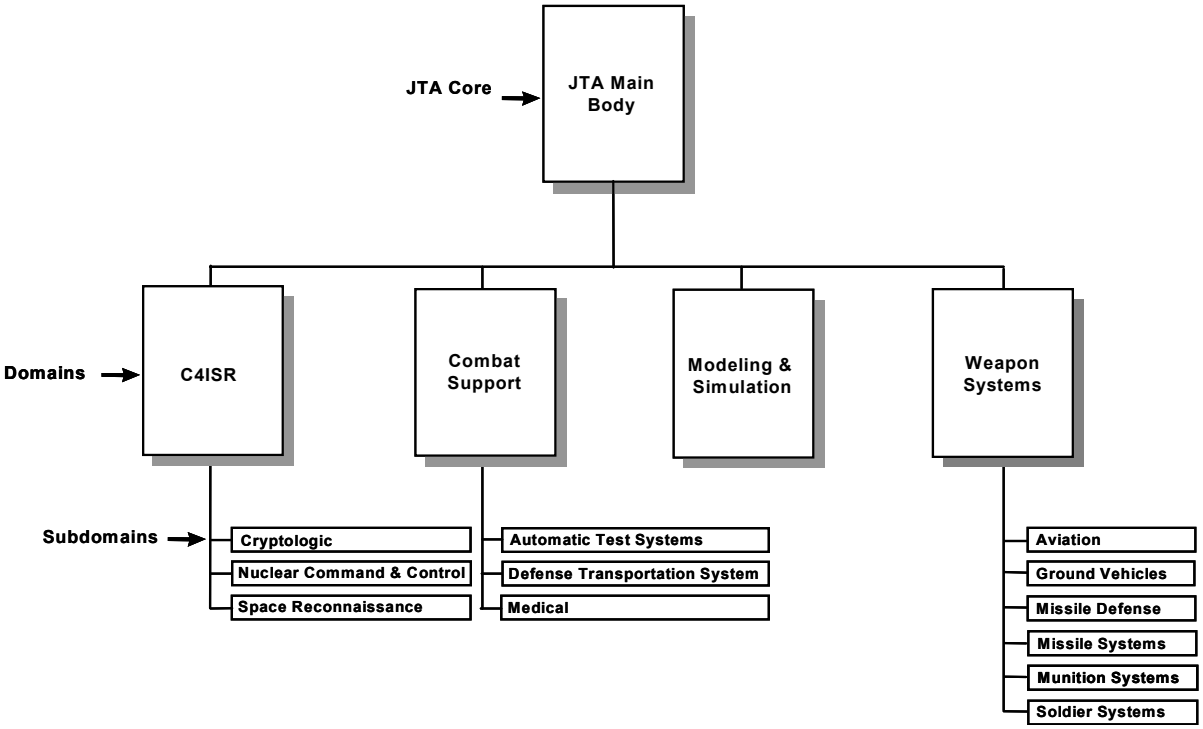


Figure 1-3: JTA Hierarchy Model

The current domains and subdomains are listed as follows:

- Domains
  - Combat Support (CS)
  - Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR)

- Modeling and Simulation (M&S)
- Weapon Systems (WS)

- Subdomains
  - Automatic Test Systems (ATS)
  - Aviation (AV)
  - Cryptologic (CRY)
  - Defense Transportation System (DTS)
  - Ground Vehicles (GV)
  - Medical (MED)
  - Missile Defense (MD)
  - Missile Systems (MS)
  - Munition Systems (MUS)
  - Nuclear Command and Control (NCC)
  - Soldier Systems (SS)
  - Space Reconnaissance (SR)

A program manager or engineer specifying or applying JTA standards for a specific system will first select all appropriate JTA Core elements, and then those included in the relevant domain and subdomain.

The goal is to build on these annexes by incorporating the requirements of additional domains and subdomains. Each domain and subdomain includes an introduction clearly specifying the purpose, scope, description of the domain, and background of the domain and subdomain. As necessary, each domain and subdomain provides a list of domain-specific standards and guidance in a format

consistent with the JTA Core. Domains and subdomains generally use the DoD Technical Reference Model (DoD TRM) defined in 1.5, but may also use a different or expanded model.

1.4.4 Appendices (Appendix A, B, C, D, E, F)

The appendices provide supporting information (e.g., how to get a copy of mandated standards) and available links to standards organizations' web site, which facilitate the use of the document, but are not mainline to its purpose.

Appendix A: Abbreviations and Acronyms contains an abbreviations and acronyms list.

Appendix B: DoD JTA List of Mandated and Emerging Standards now a stand-alone document on the JTA Web site, contains "currently mandated," "previously mandated," and "emerging" standards for each JTA service area.

Appendix C: Document Sources is a list of the organizations from which documents cited in the JTA may be obtained.

Appendix D: References is a list of documents (e.g., a memorandum, a publication) that directs the reader's attention to a source of more information on a subject.

Appendix E: JTA Relationship to DoD Standards Reform describes the relationship of the JTA to the DoD standards reform begun in June 1994 and addresses the relevance of the reform waiver policy to the JTA.

Appendix F: Glossary is a list of terms with their meanings.

1.5 DoD Technical Reference Model

The DoD Technical Reference Model (TRM), Version 1.0, 5 November 1999, 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 TRM is to provide a common conceptual framework and a common vocabulary so that the diverse components within 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 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 JTA has adapted the TRM to serve as the framework for presenting JTA-mandated standards. The JTA's use of the TRM ensures the use of consistent definitions needed to define architectural and design components. The model identifies service areas (i.e., a set of capabilities grouped by functions) and their interfaces. The TRM was chosen as the framework of the JTA because of the model's inherent support of open system concepts. As illustrated in Figure 1-4, the model is partitioned into the following: an Application Software Entity that includes both Mission Area and Support Applications; an Application Platform Entity that contains the system services (e.g., User Interface and Data Management services) and operating system services; Physical Environment Services; and 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).

The following JTA Core services are equivalent to their corresponding TRM system services contained within the Application Platform Entity:

Software Engineering Services	Internationalization Services
User Interface Services	Security Services
Data Management Services	System Management Services
Data Interchange Services	Distributed Computing Services
Graphic Services	Operating System Services
Communication Services	

The relationship between the sections in the JTA and the TRM service areas are as follows:

Section 2 Information Processing Standards specifies standards for the User Interface (2.2.2.1.2), Data Management (2.2.2.1.3), Data Interchange (2.2.2.1.4), Graphics (2.2.2.1.5), Operating System (2.2.2.1.7), Internationalization (2.2.2.1.8), and Distributed Computing (2.2.2.1.11) service areas, and the latter's two subordinate paragraphs become 2.2.2.1.11.1 and 2.2.2.1.11.2 respectively. This section also references, but does not specify, any standards for the Software Engineering (2.2.2.1.1), Communications (2.2.2.1.6), Security (2.2.2.1.9), and System Management (2.2.2.1.10) service areas.

Table 1-1 provides the interface relationships for Figure 1-4.

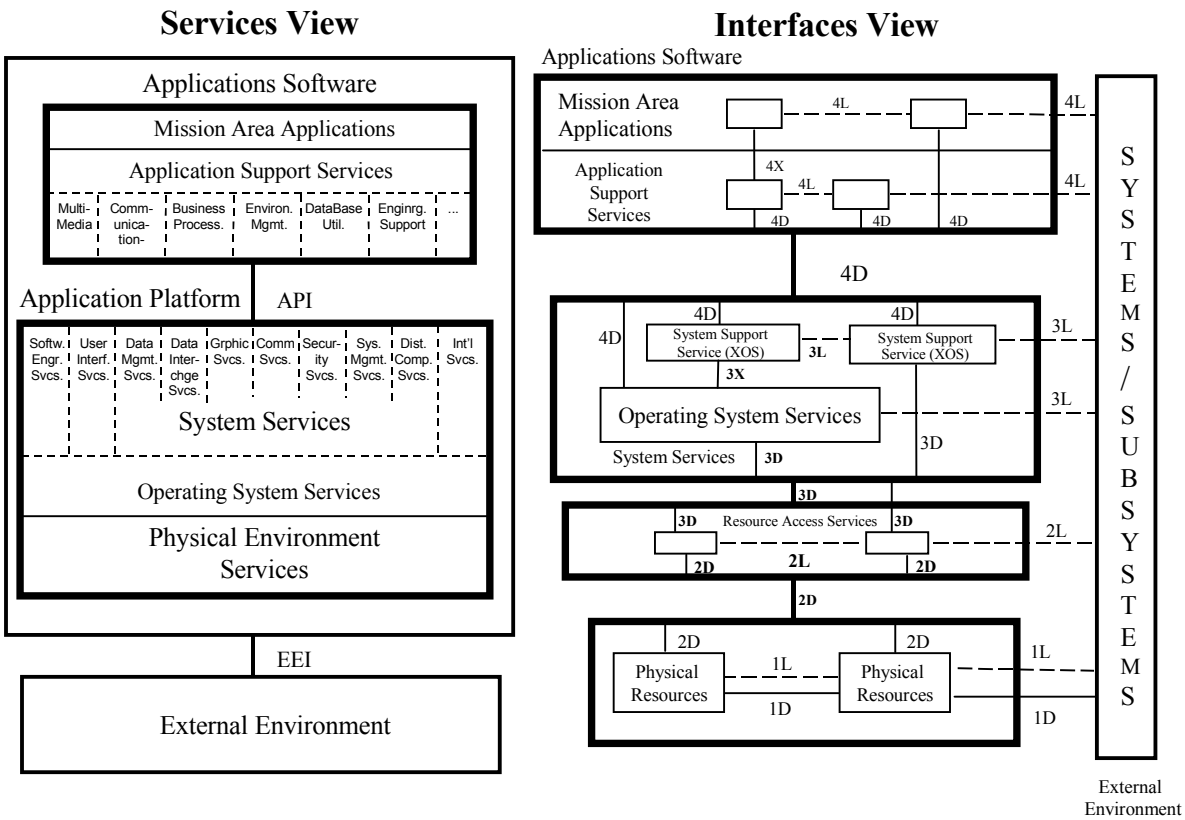


Figure 1-4: DoD Technical Reference Model (DoD TRM)

Section 3 Information Transfer Standards specifies standards for the Communications (3.2.1 through 3.2.3) and Network and System Management (3.2.4) service areas applicable to both system and network management.

Section 4 Information Modeling, Metadata, and Information Exchange Standards addresses standards for an area that is not currently elaborated, but is supported by engineering support, data management, and software engineering services in the TRM.

Table 1-1: Interface Translation Table

Interface Type	Definition
1D	Physical Resources (Direct)
1L	Physical Resources (Logical)
2D	Resources – Physical (Direct)
2L	Resource Access (Logical)
3D	System Service – Resource Access (Direct)
3L	System Service (Logical)
3X	Operating System – Extended OS (Direct)
4D	Applications – System Services (Direct)
4L	Applications – Peer (Logical)
4X	Applications – Support Services (Direct)

Section 5 Human Computer Interface Standards complements those cited for User Interface Services in 2.2.2.1.2 User Interface Services.

Section 6 Information Security Standards, specifies security standards that are relevant to the service areas discussed in Section 2, Section 3, and Section 5.

At this time, the JTA does not include standards for all of the services identified in the TRM.

1.6 Policy

The JTA does not typically include policy. However, two policy issues are addressed below.

1.6.1 Defense Information Infrastructure Common Operating Environment (DII COE)

The Common Operating Environment (COE) concept and levels of compliance are 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 consistent with the service areas identified in the TRM. Application programmers then have access to these software services through standardized APIs. The following standard is mandated:

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

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. All applications of a system that must be integrated into a DII platform shall 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.

Each DII COE version release contains products that meet the operational requirements of the user community. These products are not necessarily fully compliant with JTA standards.

However, the goal of the COE effort is to evolve to be fully compliant with the applicable JTA standards. Additionally, the DII COE does not contain functionality described in a number of JTA service areas. For these service areas, complying with the DII COE does not equate to compliance with the JTA. Additional services not contained in the DII COE must be met by complying with the applicable standards in the JTA. Each DII COE Component Software Requirement Specification (SRS) is being updated to include a profile of applicable JTA mandates.

1.6.2 Combined and Coalition Standardization and/or Interoperability

For combined and coalition standardization and/or interoperability, DoD Directive 2010.6, "Standardization and Interoperability of Weapon Systems and Equipment within the North Atlantic Treaty Organization," March 5, 1980, and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 2700.01, "International Military Rationalization, Standardization, and Interoperability between the United States and Its Allies and Other Friendly Nations," 30 January 1995, govern.

For North Atlantic Treaty Organization (NATO) standardization and/or interoperability issues, see North Atlantic Treaty Organization (NATO) Consultation, Command and Control (C3) Technical Architecture (TA) (NC3TA), 15 December 2000. 🗐

For Combined Communications-Electronics Board (CCEB) standardization and/or interoperability issues, see Allied Communications Publication (ACP) 140, "Combined Interoperability Technical Architecture (CITA)," 3 May 1999. 🗐

1.7 Key Considerations in Using the JTA

The JTA is used to determine the mandated standards within applicable service areas for implementation within new or upgraded systems. However, there are several key considerations in using the JTA.

The mandatory standards in the JTA must be implemented or used by systems that have a need for the corresponding service areas. A standard is mandatory in the sense that if a service/interface is going to be implemented, it shall be implemented in accordance with the associated standard. If a required service can be obtained by implementing more than one standard (e.g., operating system standards), the appropriate standard should be selected based on system requirements.

The JTA is a forward-looking document. It guides the acquisition and development of new and emerging functionality and provides a baseline toward which existing systems will move. It is a compendium of standards (for interfaces/services) that should be used now and in the future. It is *not* a catalog of all information technology standards used within today's DoD systems. If legacy standards are needed to interface with existing systems, they can be implemented on a case-by-case basis in addition to the mandated standard.

1.8 Element Normalization Rules

As the JTA evolves, the JTA elements contained in the JTA Core, domains, and subdomains need to be periodically revisited and updated to ensure correctness. The JTA normalization rules in this section address the movement of elements from subdomain to domain, and from domains into the Core.

All standards are placed in the Core unless they are justified as unacceptable to meet domain-specific requirements. When Core standards cannot meet the requirements of a specific domain,

JTA elements are removed from the JTA Core and placed in the appropriate domain. Likewise, when domain standards cannot meet subdomain-specific requirements, those will be removed from the domain and placed in the appropriate subdomain.

The intent of the above normalization rules is as follows: (1) The Core applies to all DoD systems; (2) the JTA Core contains selected standards for as many JTA services as possible; and (3) the JTA provides the minimum number of standards for a specified service or interface.

1.9 JTA Relationship to DoD Standards Reform

The DoD standards reform was begun in June 1994 when the Secretary of Defense issued a memorandum entitled "Specifications and Standards – A New Way of Doing Business." This memorandum directs that performance-based specifications and standards or nationally recognized private-sector standards be used in future acquisitions. The intent of this initiative is to eliminate non-value-added requirements, and thus reduce the cost of weapon systems and materiel, remove impediments to getting commercial state-of-the-art technology into weapon systems, and integrate the commercial and military industrial bases to the greatest extent possible.

The JTA implements standards reform by selecting the minimum standards necessary to achieve joint interoperability. The JTA mandates commercial standards and practices to the maximum extent possible. Use of JTA-mandated standards or specifications in acquisition solicitations will not require a waiver from standards reform policies. All mandatory standards in the JTA 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. Additional information on this topic can be found in Appendix E.

1.10 Standards Selection Criteria

The standards selection criteria used throughout the JTA focus on mandating only those items critical to interoperability that are based primarily on commercial open system technology, are implementable, and have strong support in the commercial marketplace. Standards will only be mandated if they meet all of the following criteria:

- **Interoperability:** They enhance joint and potentially combined Service/Agency information exchange and support joint activities.
- **Maturity:** They are technically mature (strong support in the commercial marketplace) and stable.
- **Implementability:** They are technically implementable.
- **Public:** They are publicly available.
- **Consistent with Authoritative Source:** They are consistent with law, regulation, policy, and guidance documents.

The following preferences were used to select standards:

- Standards that are commercially supported in the marketplace with validated implementations available in multiple vendors' mainstream commercial products took precedence.
- Publicly held standards were generally preferred.
- International or national industry standards were preferred over military or other government standards.
- Standards that can be implemented without requiring intellectual property (patent) rights were generally preferred.
- Many standards have optional parts or parameters that can affect interoperability. In some cases, an individual standard may be further defined by a separate, authoritative document called a "profile" or a "profile of a standard," which further refines the implementation of the original standard to ensure proper operation and assist interoperability.
- The word "standards" as referred to in the JTA is a generic term for the collection of documents cited herein. An individual "standard" is a document that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. A standard may also establish requirements for selection, application, and design criteria of material. The standards cited in the JTA may include commercial, federal, and military standards and specifications, and various other kinds of authoritative documents and publications.

1.11 Configuration Management

The JTA is configuration-managed by the Joint Technical Architecture Development Group (JTADG), under the direction of the DoD Technical Architecture Steering Group (TASG) and approved by the Architecture Coordination Council (ACC). These groups consist of members representing DoD and

components of the Intelligence Community. Table 1-2 shows the organizations that have voting memberships in the JTADG and TASG.

Table 1-2: JTA Development Group (JTADG) Voting Membership

Ballistic Missile Defense Organization (BMDO)
Defense Advanced Research Projects Agency (DARPA)
Defense Information Systems Agency (DISA)
Defense Intelligence Agency (DIA)
Defense Logistics Agency (DLA)
Defense Modeling and Simulation Office (DMSO)
Defense Threat Reduction Agency (DTRA)
Joint Staff/J6
National Imagery and Mapping Agency (NIMA)
National Reconnaissance Office (NRO)
National Security Agency (NSA)
Office of the Assistant Secretary of Defense (C3I)
Office of the Under Secretary of Defense (AT&L) OSJTF
U.S. Air Force (USAF)
U.S. Army (USA)
U.S. Coast Guard (USCG)
U.S. Marine Corps (USMC)
U.S. Navy (USN)
U.S. Special Operations Command (USSOCOM)
U.S. Transportation Command (USTRANSCOM)

The JTA Management Plan describes the process by which the JTA will be configuration-managed. This document, as well as the charter for the JTADG, may be found on the Defense Information Systems Agency (DISA) Center for Standards (CFS) JTA Web site: http://www-jta.itsi.disa.mil.

Suggested changes to, or comments on, the JTA originating from DoD Components (Office of the Secretary of Defense [OSD], the Military Departments, the Office of the Joint Chiefs of Staff [OJCS], the Unified and Specified Combatant Commands, and the Defense Agencies) should be submitted via the appropriate official JTA Component Representative listed on the JTA Web site. These representatives will integrate and coordinate received comments for submission as official DoD Component-sponsored comments.

Where a standard is highlighted and underscored, it is hyperlinked to the DoD Joint Technical Architecture (JTA) List of Mandated and Emerging Standards (formerly Appendix B). A “link” symbol (🗐) at the end of a citation for a standard indicates the hyperlink to the web site where the standard can be obtained. Clicking on the “link” symbol will access the corresponding web site.

Industry and other non-DoD suggested changes should be submitted through DISA CFS via electronic mail to: jta@www.disa.mil.

Section 2: Information Processing Standards

2.1 Introduction

2.1.1 Purpose

The purpose of this section is to specify the Joint Technical Architecture (JTA) Government and commercial information processing standards DoD will use to develop integrated interoperable systems that directly or indirectly support the warfighter.

2.1.2 Scope

This section applies to mission-area, Figure 5-1 support application, Figure C4ISR-1 and application platform service software. This section does not cover communications standards needed to transfer information between systems (defined in Section 3), nor standards relating to information modeling (process, data, and simulation), data elements, or military-unique message set formats (defined in Section 4).

2.1.3 Background

Information processing standards provide the data formats and instruction-processing specifications required to represent and manipulate data to meet information technology (IT) mission needs. 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.

2.2 Mandated Standards

The following sections provide the applicable mandated standards that shall be used for the selection of commercial off-the-shelf (COTS) or Government off-the-shelf (GOTS) software or in the development of Government software. Appendix B links to the table DoD Joint Technical Architecture List of Mandated and Emerging Standards on the JTA web site.

2.2.1 Application Software Entity

The Application Software Entity is one part of the DoD Technical Reference Model (TRM) that includes both mission-area applications and support applications. Mission-area applications implement specific users' requirements and needs (e.g., personnel, material, management). This application software may be COTS, GOTS, custom-developed software, or a combination of these.

Common support applications (e.g., e-mail and word processing) are those that can be standardized across individual or multiple mission areas. The services they provide can be used to develop mission-area-specific applications or can be made available to the user. The TRM defines six support application categories: Multimedia, Communications, Business Processing, Environment Management, Database Utilities, and Engineering Support. The definitions of these categories are found in the DoD Technical Reference Model, Version 1.0, 5 November 1999.

2.2.2 Application Platform Entity

The Application Platform Entity is the second layer of the DoD TRM, as shown in Figure 1-4, and 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 with the tools that are appropriate to the development and maintenance of applications. There are no mandated standards for this service area.

Language services provide the basic syntax and semantic definition for use by developers to describe the desired software function. "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."[1] Computer languages should be used in such a way as to minimize changes when compilers, operating systems, or hardware change. To maximize portability, the software should be structured where possible so it can be easily ported.

2.2.2.1.2 User Interface Services

User Interface Services control how a user interfaces with an information technology system. The Common Desktop Environment (CDE) provides a common set of desktop applications and management capabilities for environments similar to the Microsoft Windows desktop environment. CDE supports The Open Group Motif-based application execution. Both CDE and Motif applications use the underlying X-Windows system. The Win32 Application Program Interface (API) set provides similar services for Microsoft Windows applications. Refer to Section 5 for Human-Computer Interface (HCI) style guidance and standards.

2.2.2.1.2.1 User Interface Service — POSIX

The Common Desktop Environment (CDE) provides a common set of desktop applications and management capabilities for use with Portable Operating System Interface (POSIX)-based operating systems. CDE supports The Open Group Motif-based application execution. Both CDE and Motif applications use the underlying X-Windows system. The following standards are mandated for use with Portable Operating System Interface (POSIX)-compliant operating systems running (or intended to run) POSIX-compliant applications:

Currently, the CDE and Motif User Interface Service Standards are mandated; but, due to changing market conditions, they are candidates for removal in a future version of the JTA.

- 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.
- C903, X Window System (X11R6): Protocol, The Open Group, July 1999.
- C508, Window Management (X11R5): Xlib - C Language Binding, Open Group Technical Standard, ISBN 1-85912-088-1, May 1995, as updated by X11R6.

[1] Additional guidance may be found in the memorandum "Use of the Ada Programming Language" by ASD (C3I), April 29, 1997, DoD 5000.2-R, and DoDD 3405.1.

- C509, Window Management (X11R5): X Toolkit Intrinsics, Open Group Technical Standard, ISBN 1-85912-089-X, May 1995, as updated by X11R6.
- C510, Window Management (X11R5): File Formats and Application Conventions, Open Group Technical Standard, ISBN 1-85912-090-3, May 1995.
- M021: CDE 2.1/Motif 2.1 User's Guide, ISBN 1-85912-173-X, October 1997.
- M023: CDE 2.1 Programmer's Overview and Guide, Open Group Product Documentation, ISBN 1-85912-183-7, October 1997.
- M024A: CDE 2.1 Programmer's Reference, Volume 1, Open Group Product Documentation, ISBN 1-85912-188-8, October 1997.
- M024B: CDE 2.1 Programmer's Reference, Volume 2, Open Group Product Documentation, ISBN 1-85912-193-4, October 1997.
- M024C: CDE 2.1 Programmer's Reference, Volume 3, Open Group Product Documentation, ISBN 1-85912-174-8, October 1997.
- M026: CDE 2.1 Application Developer's Guide, Open Group Product Documentation, ISBN 1-85912-198-5, October 1997.
- M213: Motif 2.1 - Programmer's Guide, ISBN 1-85912-134-9, October 1997.
- M214A: Motif 2.1 - Programmer's Reference, Volume 1, ISBN 1-85912-119-5, October 1997.
- M214B: Motif 2.1 - Programmer's Reference, Volume 2, ISBN 1-85912-124-1, October 1997.
- M214C: Motif 2.1 - Programmer's Reference, Volume 3, ISBN 1-85912-164-0 October 1997.
- M216: Motif 2.1 — Widget Writer's Guide, Open Group Product Documentation, ISBN 1-85912-129-2, October 1997.

2.2.2.1.2.2 User Interface Service — Win32

User Interface API Services defines the software interfaces needed to control user interfaces with an information technology system. The Win32 API set provides User Interface Services for Microsoft Windows and Windows-compliant applications. Documentation for the Win32 APIs is found within the Microsoft Platform Software Development Kit (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.

2.2.2.1.3 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 support the definition, storage, and retrieval of data elements from Database Management Systems (DBMSs). Application code using Relational Database Management System (RDBMS) resources and COTS RDBMSs are required to conform to Entry-Level SQL. The following standard is mandated for any system using an RDBMS:

- ISO/IEC 9075:1992, Information Technology - Database Language - SQL with amendment 1, 1996, 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. The following API is mandated for both database application clients and database servers:

- 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 Java Database Connectivity (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, motion imagery data, audio data, storage media, atmospheric and oceanographic data, and time-of-day data.

2.2.2.1.4.1 Document Interchange

The Standard Generalized Markup Language (SGML) format supports the production of documents 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) with Amendment 1, 1988, Technical Corrigendum 1:1996 and Technical Corrigendum 2:1999.

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

- HTML 4.01 Specification, W3C Recommendation, revised on 24-Dec-1999, REC-html401-19991224.

The Extensible Markup Language (XML) is a meta-language, based on SGML, for describing languages based on name-attribute tuples. This allows new capabilities to be defined and delivered dynamically. For domain- and application-specific markup languages defined through tagged data items, the following is a mandated standard:

- Extensible Markup Language (XML) 1.0, (Second Edition), W3C Recommendation, 6 October 2000.

Table 2-1 identifies file formats for the interchange of common document types such as text documents, spreadsheets, and presentation graphics. Some of these formats are controlled by individual vendors, but all of these formats are supported by products from multiple companies. In support of the standards mandated in this section, Table 2-1 identifies conventions for file name extensions for documents of various types. If an organization has a requirement for a given document type, the formats in Table 2-1 are mandated, but not the specific products mentioned:

Table 2-1: Common Document Interchange Formats

Document Type	Standard/Vendor Format	Recommended File Name Extension	Reference
Plain Text	ASCII Text Format	.txt	ISO/IEC 646:1991 IRV
Compound Documents	Adobe® PDF 1.3 2nd Edition Format	.pdf	Vendor
	HTML Format 4.01	.htm	W3C
	MS Word® 7.0 Format	.doc	Vendor
	MS Word® 6.0 Format	.doc	Vendor
	Rich Text Format	.rtf	Vendor
	WordPerfect® 5.2 Format	.wp5	Vendor
Briefing - Graphic Presentation	Freelance® Graphics 2.1 Format	.pre	Vendor
	MS PowerPoint® 4.0 Format	.ppt	Vendor
Spreadsheet	Lotus® 1-2-3 Release 3.x Format	.wk3	Vendor
	MS Excel® 5.0 Format	.xls	Vendor
Database	dBASE® 4.0 Format	.dbf	Vendor
Compression	GZIP® file Format	.gz	RFC 1952
	Zip file Format	.zip	Vendor
Computer Automated Design	AutoCAD® 14 Format	.dxf	Vendor

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

Notes: Compound documents contain embedded graphics, tables, and formatted text. Object Linking and Embedding (OLE) linking complicates document interchange. IRV is International Reference Version. Some special fonts, formatting, or features supported in the native file format may not convert accurately.

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 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 truecolour images are supported, plus an optional alpha channel for transparency. The PNG specification was issued as a W3C Recommendation on 1 October 1996.

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

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

For the interchange of other single raster images that have no geospatial context and where lossy compression is not acceptable or is ineffective, 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, CompuServe Incorporated, 31 July 1990.

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 that 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 based on a georelational data model and intended for direct use. Existing geospatial products that implement VPF include: Vector Map (VMap) Levels 0-2, Urban Vector Map (UVMap), Digital Nautical Chart (DNC), VPF Interim Terrain Data (VITD), Digital Topographic Data (DTOP), and World Vector Shoreline Plus (WVS*PLUS*). For vector-based products, the following standard is mandated:

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

WGS84, 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. The National Imagery and Mapping Agency (NIMA) Technical Report (TR) 8350.2, Third Edition DoD World Geodetic System 1984, Its Definition and Relationships with Local Geodetic Systems, 4 July 1997, defines the technical content of WGS 84. WGS 84 will be used for all joint operations and is recommended for use in multinational and unilateral operations after coordination with allied commands. The following standard is mandated:

- MIL-STD-2401, Department of Defense World Geodetic System (WGS), 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 through Change Notice 3, 17 May 1999.

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. Other image formats can be used internally within a single system; however, NITF is the default format for interchange between systems. 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). NITFS 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 with Notice 1, 27 June 1996.
- MIL-STD-188-199, Vector Quantization Decompression for the National Imagery Transmission Format Standard, 27 June 1994 with Notice 1, 27 June 1996.
- 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 with Notice 1, 12 October 1994 and Notice 2, 14 March 1997. Although the NITFS uses the same ISO JPEG algorithm as mandated in 2.2.2.1.4.2, the NITFS file format is not interchangeable with the JFIF file format.
- The Compendium of Controlled Extensions (CE) for the National Imagery Transmission Format (NITF) Version 1.0, 25 August 1998.

Communication protocols for the transmission of imagery over point-to-point tactical data links in high Bit Error Rate (BER), disadvantaged communications environments are specified in 3.2.1.5.

2.2.2.1.4.5 Motion Imagery Data Interchange

Motion Imagery (MI) 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]) within a common field of regard. Motion Imagery defines temporal domains of 1 Hz or higher, and still imagery defines temporal domains of less than 1 Hz.

2.2.2.1.4.5.1 Video Systems

Video systems, defined as electro-optical motion imagery whose formats are governed by national and international standards, are divided into four categories:

- Video Imagery Systems, which create, transmit, edit, store, archive, or disseminate digital video for real-time, near-real-time or for other end-user product distribution, usually in support of Intelligence, Surveillance, and Reconnaissance (ISR) activities.

- Video Teleconference Systems, which provide real-time visual interchange between remote locations typically in support of meetings. When video teleconference systems are used for the display of Video Imagery, the standards in the Video Imagery section apply.
- Video Telemedicine Systems, which provide real-time visual interchange between remote locations in biomedical applications including fiber-optic and video teleconferencing.
- Video Support Systems, which enable end-user applications associated with video-based training news gathering, or other non-critical functions that do not directly support the warfighter. This includes traditional studio and field video productions not associated with DoD warfighter operations.

The standards and use directives for each class of video system are noted in the following sections:

2.2.2.1.4.5.1.1 Video Imagery

The following standards, as they are profiled by the Motion Imagery Standards Profile (MISP) 1.6 Chapter 2.0, Commercial Standards, Interoperability Profiles, and Recommended Practices for DoD/IC/USIGS Implementations, 27 July 2000, are mandated:

Table 2-2: Mandated Standards from MISP 1.6, Chapter 2.0

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.
● ANSI/SMPTE 293M-1996	Television – 720 x 483 Active Line at 59.94-Hz Progressive Scan Production – Digital Representation.	Progressive Video Sampling Structure – Standard-definition.

Table 2-2: Mandated Standards from MISP 1.6, Chapter 2.0 (cont'd)

Standard	Title	Usage
• ANSI/SMPTE 296M-1997	Television – 1270 x 720 Scanning, 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).

2.2.2.1.4.5.1.2 Video Teleconference

Video Teleconferencing (VTC) standards are specified in 3.2.1.3.

2.2.2.1.4.5.1.3 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 Mbits/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).

2.2.2.1.4.6 Audio Data Interchange

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

2.2.2.1.4.6.1 Audio Associated with Video

The classes of audio in support of video have been subdivided into four categories:

- **Audio for Video Imagery Systems**, which create, transmit, edit, store, archive, or disseminate audio for real-time, near-real-time, and other end-user product distribution, usually in support of Intelligence, Surveillance, and Reconnaissance (ISR) activities.
- **Audio for Video Teleconference Systems**, which provide real-time verbal interchange between remote locations, typically in support of meetings. When video teleconference systems are used for the display of Video Imagery, the standards in the Audio for Video Imagery section apply.
- **Audio for Video Telemedicine Systems**, which provide real-time visual interchange between remote locations in support of biomedical applications including fiber-optic and video teleconferencing.
- **Audio for Video Support Systems**, which enable end-user applications associated with video/audio-based training, news gathering, or other non-critical functions that do not directly support the warfighter. This includes traditional studio and field productions not associated with DoD warfighting operations.

The standards and use directives for each category of audio application are given in the following sections.

2.2.2.1.4.6.1.1 Audio for Video Imagery

For audio systems associated with Video Imagery applications, the audio sub-sections of the Video Imagery Standards Profile (VISP), Version 1.5, 8 September 1999, apply.

- 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.

2.2.2.1.4.6.1.2 Audio for Video Teleconference

Video Teleconferencing (VTC) standards are specified in 3.2.1.3.

2.2.2.1.4.6.1.3 Audio for Video Support

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

- ISO/IEC 11172-3:1993, Information technology - Encoding 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.

2.2.2.1.4.6.2 Voice Encoder

The 2.4 Kbps Mixed Excitation Linear Prediction (MELP) algorithm specified in MIL-STD-3005 is intended to provide seamless interoperability, hence enabling end-to-end security, across the domains of strategic, tactical, satellite communications, including that of internetworking protocols. MIL-STD-3005 provides a common high-performance voice encoding algorithm for use across the communications infrastructure. For processing over 2.4 Kbps digital links (voice data), the following standard is mandated:

- MIL-STD-3005, Analog-to-Digital Conversion of Voice by 2400 Bit/Second Mixed Excitation Linear Prediction (MELP), 20 December 1999.

2.2.2.1.4.7 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 3.2.1.3.

2.2.2.1.4.8 Atmospheric and Oceanographic Data Interchange

The following formats are established by the World Meteorological Organization (WMO) Commission 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 telecommunications 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 1.2 (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 online 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 1.2 (Annex II to WMO Technical Regulations) Parts B and C.

2.2.2.1.4.9 Time-of-Day Data Interchange

Coordinated Universal Time (UTC), traceable to UTC (USNO) maintained by the U.S. Naval Observatory (USNO), shall be used for time-of-day information exchanged among DoD systems. Time-of-day information is exchanged for numerous purposes including time-stamping events, determining ordering, and synchronizing clocks. Traceability to UTC (USNO) may be achieved by various means depending on system-specific accuracy requirements. These means may range from a direct reference via a GPS time code receiver to a manual interface involving an operator, wristwatch, and telephone-based time service. The UTC definition contained in the following standard, traceable to UTC (USNO), is mandated:

- ITU-R TF.460-5, Standard-frequency and Time-signal Emissions, 1997.

In those systems where relativistic effects matter, the following standard is mandated:

- ITU-R TF.1010-1, Relativistic Effects in a Coordinate Time System in the Vicinity of the Earth, October 1997.

Note that the Global Positioning System (GPS) provides time-of-day information traceable to UTC (USNO). Also, note that leap seconds are inserted or deleted when necessary in UTC to keep the time-of-day system synchronized with the Earth's rotation. See Paragraph for a GPS discussion, required standards, and guidelines.

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.
- OpenGL Graphics System, A Specification (Version 1.1) 25 June 1996 (for three-dimensional graphics).

2.2.2.1.6 Communications Services

These services support the distributed applications that require data access and applications interoperability in networked environments. The mandated standards 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 shall be accessed by applications through either the standard Portable Operating System Interface (POSIX) or Win32 APIs.

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 shall comply with the standards listed below. The following standards are mandated:

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: Batch Environment.
- ISO/IEC 14519:1999, Information Technology – POSIX Ada Language Interfaces – Binding for System Application Program Interface (API) – Realtime Extensions.
- IEEE 1003.13:1998, IEEE Standard for Information Technology – Standardized Application Environment Profile (AEP) – POSIX Realtime Application Support.

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, which build upon the ASCII character set, 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 10646-1:1993/Cor1:1996, Cor2:1998, 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. They must often be combined with security procedures, which are beyond the scope of the information technology service areas, to fully meet security requirements. Security services include security policy, accountability, and assurance. (Note: Security Service standards have been consolidated in Section 6)

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 JTA facilitates interoperability by identifying network management standards. These standards can be found in sections 3.2.4 and 3.3.5.

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.

2.2.2.1.11.1 Remote-Procedure Computing

The mandated standards for remote-procedure computing are identified in the Open Group Distributed Computing Environment (DCE) Version 1.1. The mandated standards are:

- C310, DCE 1.1: Time Services Specification, X/Open CAE Specification, November 1994.
- C311, DCE 1.1: Authentication and Security Services, Open Group CAE Specification, August 1997.
- C705, DCE 1.1: Directory Services, Open Group CAE Specification, August 1997.
- C706, DCE 1.1: Remote Procedure Call, Open Group CAE Specification, August 1997.

The C311 specification is included here to provide the complete definition of the DCE. Section 6, Information Security Standards, specifies the other security requirements that must be met.

When used in conjunction with the POSIX Threads Extensions, the recommendations of the Open Group's Single UNIX Specification Version 2 – 6 Vol Set for UNIX 98 are expected to integrate the DCE thread model with the POSIX thread model.

2.2.2.1.11.2 Distributed-Object Computing

The mandate for distributed-object computing is interworking with the Object Management Group (OMG) Object Management Architecture (OMA), composed of the Common Object Request Broker Architecture (CORBA), CORBAservices, and CORBAfacilities. The CORBA specification defines the interfaces and services for Object Request Brokers, including an Interface Definition Language (IDL) and the Internet Inter-ORB Protocol (IIOP). CORBAservices define interfaces and semantics for services required to support distributed objects, such as naming, security, transactions, and events. CORBAfacilities defines interfaces and semantics for services required to support functions such as compound document manipulation. Interworking is the exchange of meaningful information between computing elements (semantic integration). Application-Level Interworking, for CORBA, results in CORBA clients interacting with non-CORBA servers and non-CORBA clients interacting with CORBA servers. For OLE/COM, Application-Level Interworking results in COM/OLE clients interacting with non-COM/OLE servers and non-COM/OLE clients interacting with COM/OLE servers.

The CORBA interoperability mandate does not preclude the use of other distributed-object technologies, such as ActiveX/Distributed Component Object Model (DCOM) or Java, as long as the capability for interworking with CORBA applications and objects is maintained by the non-CORBA system. Products are available that allow interworking among distributed-object techniques. 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.

When a CORBA Object Request Broker (ORB) is used, the following specifications are mandated if the corresponding object service is being implemented:

- OMG document formal/2000-06-19, Naming Service Specification, Version 1.0, April 2000.
- OMG document formal/2000-06-15, Event Service Specification, Version 1.0, June 2000.
- OMG document formal/2000-06-28, Transaction Service Specification, Version 1.1, May 2000.
- OMG document formal/2000-06-26, Time Service Specification, Version 1.0, May 2000.
- OMG document formal/2000-06-27, Trading Object Service Specification, Version 1.0,May 2000.
- OMG document formal/2000-06-20, Notification Service Specification, Version 1.0, June 2000.

For DCE users that need to interwork with CORBA, the following standard is mandated:

- OMG document orbos/98-06-01, CORBAservices DCE/CORBA Interworking Service.

For COM users that need to interwork with CORBA, the following standards are mandated:

- OMG document orbos/97-09-06, COM/CORBA Part B, Interworking, November 19, 1997.
- OMG document orbos/97-09-07, COM/CORBA Part A, Revision November 19, 1997.

2.3 Emerging Standards

Emerging standards are expected to be elevated to mandatory status when implementations of the standards mature and the standards meet all criteria in 1.6.

2.3.1 Data Management

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 and have been completed and approved by ANSI, ISO, and IEC:

- 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).

Additionally, ISO/IEC DIS 9075-9 through ISO/IEC DIS 9075-12 are in progress though they have not been completed.

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 hard-cover 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.

2.3.2 Data Interchange

2.3.2.1 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™ 1.0: The Extensible HyperText Markup Language, A Reformulation of HTML 4 in XML 1.0, W3C Recommendation, 26 January 2000.

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.

Resource Description Framework (RDF) describes a foundation for processing WWW metadata; it supports interoperability between different applications that may need to exchange machine-understandable information on the WWW. RDF uses Extensible Markup Language (XML) for encoding its interchange syntax. RDF is a model for representing named properties (attributes of resources), property values, and relationships between properties. An RDF model can resemble an entity-relationship diagram or virtually any other information structure that can be depicted as a directed graph. The following standard is emerging:

– Resource Description Framework (RDF) Model and Syntax Specification, W3C Recommendation, 22 February 1999, REC-rdf-syntax-19990222.

The RDF Schema specification provides a machine-understandable system for defining “schemas” for descriptive vocabularies like the Dublin Core, a set of 15 metadata elements believed to be broadly applicable to describing Web resources to enable their discovery. It allows designers to specify classes of resource types and properties to convey descriptions of those classes, and constraints on the allowed combinations of classes, properties, and values within a data stream. This has the effect of providing a machine-understandable means of exchanging structured and structural information with respect to various persistent entities, such as DBMSs with XML. The following standard is emerging:

– Resource Description Framework (RDF) Schema Specification, W3C Recommendation, 27 March 2000, PR-rdf-schema-19990303.

A Working Draft of the Extensible Stylesheet Language (XSL) Version 1.0 (Ref: WD-xsl-19981216, 16 December 1998) 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 Working Draft, 27 March 2000.

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 1.1: W3C Recommendations, 16 November 1999.

XPath is a language for addressing parts of an XML document, designed to be used by XSLT. The following standard is emerging.

– XML Path Language (XPATH): Version 1.0, W3C Recommendations, 16 November 1999.

2.3.2.2 Graphics Data Interchange

2.3.2.2.1 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.

2.3.2.2.2 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 design was frozen in May 1999. The working document is MNG (Multiple-image Network Graphics) Format, PNG Development Group, 1999.

2.3.2.2.3 Portable Network Graphics (PNG)

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).

2.3.2.3 Still Imagery Data Interchange

The Basic Image Interchange Format (BIIF) is a published international standard. It provides a commercial/international foundation for interoperability in the interchange of imagery and imagery-related data among applications. BIIF provides a data format container for image, symbol, and

text, along with a mechanism for including image-related support data. The following standard is emerging:

– ISO/IEC 12087-5:1998, Part 5; Basic Image Interchange Format (BIIF), 15 October 1998.

Part I of JPEG 2000 Image Coding System has been approved as an International Standard. JPEG 2000 is intended to provide 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 15444-1:2000, FCD JPEG 2000 Image Coding System.

2.3.2.4 Motion Imagery Data Interchange

2.3.2.4.1 Video Systems

2.3.2.4.1.1 Video Imagery

The following standards, as they are profiled by the Motion Imagery Standards Profile (MISP) 1.6, Chapter 2.0, Commercial Standards, Interoperability Profiles, and Recommended Practices for DoD/IC/USIGS Implementations, 27 July 2000, are emerging:

Table 2-3: Emerging Standards from MISP 1.6, Chapter 2.0

Standard	Title	Usage
– MISB 0001-720P	1280x720 Progressive High Definition Television Sample Structure, Analog and Digital Representation and Analog Interface, 27 July 2000.	HDTV Sample Structure, Representation and Interface
– SMPTE RP210.2-2000	SMPTE Metadata Dictionary Contents, 2000	Dictionary Contents
– SMPTE Egxxx-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 RP213-2000	Format for Non-PCM Audio and Data in AES3 — KLV Data Type, 2000.	Standard Method for Packing Video Metadata into AES3

The following standard is emerging for advanced television applications:

– ATSC A/52 (Audio), Dolby Digital AC3 is an emerging standard for advanced television applications.

2.3.2.4.1.2 Video Teleconference

Emerging standards for video teleconferencing are covered in the Information Transfer section of the JTA, 3.3.1.2.

2.3.2.5 Multimedia Data Interchange

The "Draft DoD Guide to Selecting Computer-Based Multimedia Standards, Technologies, Products, and Practices," dated 15 February 1998, defines emerging standards for DoD systems employing multimedia. In this context, interactivity is a key distinguishing characteristic, in which "two or more media types (audio, video, imagery, text, and data) are electronically manipulated, integrated, and reconstructed in synchrony, where interactivity indicates an ability of a user to make decisions or selections that (can) alter the type and sequence of information or communication."

2.3.2.6 Voice Encoder

The 1.2 Kbps enhanced Mixed Excitation Linear Prediction (MELP) algorithm is based upon MIL-STD-3005 and is intended to extend seamless interoperability to bandwidth limited users (HF links, MILSATCOMs, covert ops, etc.), hence enabling end-to-end security to this user community. MIL-STD-3005 provides a common high-performance voice-encoding algorithm for use across the communications infrastructure and will be included in the current MIL-STD-3005 as an annex. For processing voice data at rates under 2.4 Kbps, the following standard is emerging:

- Analog-to-Digital Conversion of Voice, by 1200 Bit/Second Mixed Excitation Linear Prediction (MELP).

2.3.3 POSIX Operating Systems

The following POSIX standards are emerging:

- P1003.1a, Draft Standard for Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) [C Language] - Amendment, Draft 16, December 1998.
- IEEE 1003.1d:1999, Standard for Information Technology - Portable Operating System Interface (POSIX) Part 1: System Application Program Interface (API) - Amendment d: Additional Realtime Extensions [C Language].
- P1003.1h, D5, July 1999: Services for Reliable, Available, Serviceable Systems.
- IEEE 1003.1j:2000, Standard for Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) - Amendment j: Advanced Realtime Extensions [C Language].
- P1003.1m, Draft Standard for Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) - Amendment m: Checkpoint/Restart Interface [C Language], Draft 2, January 1999.
- P1003.1q, Draft Standard for Information Technology - Portable Operating System Interface (POSIX) Part 1: System Application Program Interface (API) - Amendment x: Tracing [C Language], Draft 8, April 2000.
- P1003.5g/D1, Standard for Information Technology - Portable Operating System Interface (POSIX) - Ada Language Interfaces - Part 1: Binding for System Application Program Interface (API) -Amendment g: Realtime Extensions, September 1999.
- P1003.13a/D1, Standard for Information Technology – Standardized Application Environment Profile – POSIX Realtime Application Support (AEP) – Amendment a: Realtime Extension, September 1999.
- P1003.21, Draft Standard for Information Technology - Portable Operating System Interface (POSIX) - Part 1: Realtime Distributed Systems Communication Application Program Interface (API) [Language-Independent], V3.0, October 1999.
- C808, Networking Services (XNS), Issue 5.2, Open Group Technical Standard, ISBN-1-85912-241-8, January 2000.

In addition, the sponsor committee for POSIX standards (Portable Application Standards Committee), the international POSIX standards working group (JTC1/SC22/WG15), and The Open Group (TOG) are seeking to approve a new IEEE and ISO standards project to revise and consolidate those standards that make up ISO/IEC 9945-1:1996 and ISO/IEC 9945-2:1993 plus any additional supplements to those standards that are already IEEE standards or became IEEE standards by 31 December 1999.

Once this revision is approved by all three bodies, the ISO POSIX standard, the IEEE POSIX standards, and the Single UNIX Specification (SUS) will be identical in all respects. For more information, see: <http://www.opengroup.org/austin/docreg.html>.

2.3.4 Distributed Computing Services

2.3.4.1 Remote-Procedure Computing

The following adopted specification from the Open Group is emerging:

- OSF-DCE Version 1.2.2, Issued to developers by the Open Group in November 1997.

2.3.4.2 Distributed-Object Computing

The CORBA 3 suite of specifications are divided into three major categories: Internet Integration; Quality of Service Control; and the CORBAcomponent architecture. The following CORBA 3 suite of specifications are emerging:

- OMG document orbos/98-05-04, Joint Firewall Revised Specification.
- OMG document orbos/98-07-04, Summary of Firewall Errata.
- OMG document orbos/98-10-11, Interoperable Naming Service, October 1998.
- OMG document orbos/98-05-05, Revised Messaging RFP Submission.
- OMG document orbos/98-08-04, MinimumCORBA Joint Revised Submission.
- OMG document orbos/99-02-12, RealtimeCORBA Joint Revised Submission.
- OMG document orbos/99-03-29, Errata for the Realtime CORBA Joint Revised Submission.

The following distributed-object computing specifications from the Object Management Group (OMG) are emerging:

- OMG document orbos/99-07-07, Persistent State Service 2.0 Revised Submission.
- OMG document formal/2000-04-03, Meta Object Facility Specification, Version 1.3, April 2000.
- OMG document ec/99-03-01, Negotiation Facility Final Revision Submission, 1 March 1999.
- OMG document formal/00-05-22, Workflow Management Facility Specification, Version 1.2.
- OMG document formal/00-06-35, Distributed Simulation Systems Specification, Version 1.0, April 2000.
- OMG document orbos/99-12-02, Portable Interceptors, Joint Revised Submission.
- OMG document ptc/99-10-03, CORBA Component Model.

2.3.5 Support Application Services

2.3.5.1 Environment 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).

2.3.5.2 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 URL indicated:

- Educom Instructional Management System.
- Aviation Industry Computer-Based Training (CBT) Committee.
- Alliance of Remote Instructional Authoring and Distribution Networks for Europe (ARIADNE).
- IEEE Learning Technology Standards Committee.

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 P1484.12, Learning Object Metadata (LOM), Working Group Document: “Learning Object Metadata, Draft 4, 2000-02-05”.
– IEEE 1484.11, Computer Managed Instruction (CMI) Working Group Document: “Computer-Managed Instruction (CMI), Draft 3.3, 1999-02”.

Section 3: Information Transfer Standards

3.1 Introduction

3.1.1 Purpose

Information Transfer standards and profiles are described in this section. These standards promote seamless communications and information transfer interoperability for DoD systems.

3.1.2 Scope

This section identifies the information transfer standards required for interoperability between DoD information technology systems. These standards support access for end-systems including host, Video Teleconferencing (VTC), facsimile, Global Positioning System (GPS), and secondary imagery dissemination. Networking and internetworking standards are identified. Transmission media standards for MILSATCOM, Synchronous Optical Network (SONET), and radio links as well as network and systems management standards for data communications and telecommunications are identified. Finally, emerging technologies that should be monitored for future extension of information transfer capabilities are identified. This section includes the Communications Services depicted in Figure 1-4, DoD Technical Reference Model. Security standards are addressed in 6.2.3.

3.1.3 Background

The standards 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. For example, the JTA makes use of the open-systems architecture used by the Internet and the Defense Information System Network (DISN). 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 subnetworks that are homogenous in protocol stacks) or have complex internal structures of diverse subnetworks. Routers interconnect two or more subnetworks and forward packets across subnetwork 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.

3.2 Mandated Standards

This subsection identifies the mandatory standards, profiles, and practices for information transfer. 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).

3.2.1 Communications

3.2.1.1 End-System Standards

This section addresses standards for the following types of end-systems: host, VTC, facsimile, imagery dissemination, and GPS.

3.2.1.2 Host Standards

Hosts are computers that generally execute application programs on behalf of users and share information with other hosts. Internet Engineering Task Force (IETF) Standard 3 is an umbrella standard that references other documents and corrects errors in some of the referenced documents. IETF Standard 3 consists of Request for Comments (RFC) 1122 and RFC 1123. This 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. The following standard is mandated:

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

3.2.1.2.1 Application Support Services

3.2.1.2.1.1 Electronic Mail

The standard for official organizational-messaging traffic between DoD organizations is the Defense Message System's (DMS's) X.400-based suite of military messaging standards defined in Allied Communications 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 3.2.1.2.2.2 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 Edition A, U.S. Supplement No. 1, Common Messaging Strategy and Procedures, 15 August 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/RFC 821/RFC 1869/RFC 1870, Simple Mail Transfer Protocol (SMTP) Service Extensions, November 1995.
- IETF Standard 11/RFC 822, Standard for the Format of ARPA Internet Text Messages, 13 August 1982.
- IETF RFCs 2045-2049, Multipurpose Internet Mail Extensions (MIME) Parts 1-5, November 1996.

3.2.1.2.1.2 Directory Services

3.2.1.2.1.2.1 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. While it is appropriate for all grades of service, it must be used for high-grade service where standards-based access control, signed operations, replication, paged results, and server-to-server communication are required. It provides the security services used by DMS-compliant X.400 implementations and is mandated for use with DMS. See Section 6 for security standards. Since X.500 is not an Internet standard, see 3.2.1.2.2.2 for operation over 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.

3.2.1.2.1.2.2 Lightweight Directory Access Protocol

Lightweight Directory Access Protocol (LDAP) (Version 2) is an Internet protocol for accessing online directory services. It runs directly over Transmission Control Protocol (TCP). LDAP derives from the X.500 Directory Access Protocol (DAP). It is appropriate for systems that need to support a medium grade of service in which security is not an issue, and access is only needed to a centralized server. The following standard is mandated:

- IETF RFC 1777, Lightweight Directory Access Protocol, March 1995.

3.2.1.2.1.2.3 Domain Name System

Domain Name System (DNS) is a hierarchical host management system that has a distributed database. It provides the look-up service of translating between host names and IP addresses. DNS uses TCP/User Datagram Protocol (UDP) as a transport service when used in conjunction with other services. 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 standards are mandated:

- IETF Standard 13/RFC 1034/RFC 1035, Domain Name System, November 1987.
- IETF RFC 2136, Dynamic Updates in the Domain Name System, April 1997.

3.2.1.2.1.3 File Transfer

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

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

3.2.1.2.1.4 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 were directly connected to the remote system. The following standard is mandated:

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

3.2.1.2.1.5 Network Time Synchronization

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 (Version 3) Specification, Implementation, and Analysis, March 1992.

3.2.1.2.1.6 Bootstrap Protocol

Bootstrap Protocol (BOOTP) is used to provide address determination and bootfile selection. It assigns an IP address to workstations with no IP address. The following standards are mandated:

- IETF RFC 951, Bootstrap Protocol, September 1985.
- IETF RFC 2132, DHCP Options and BOOTP Vendor Extensions, March 1997.
- IETF RFC 1542, Clarifications and Extensions for the Bootstrap Protocol, October 1993.

3.2.1.2.1.7 Configuration Information Transfer

The Dynamic Host Configuration Protocol (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.

3.2.1.2.1.8 Web Services

3.2.1.2.1.8.1 Hypertext Transfer Protocol

Hyptertext Transfer Protocol (HTTP) is used for search and retrieval within the Web. The following standard is mandated:

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

3.2.1.2.1.8.2 Uniform Resource Locator

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

3.2.1.2.1.9 Connectionless Data Transfer

The Connectionless Data Transfer Application Layer Standard allows Variable Message Format (VMF) messages to be used in connectionless applications. This standard uses User Datagram Protocol (UDP) as a transport service. The following standard is mandated:

- MIL-STD-2045-47001B, Connectionless Data Transfer Application Layer Standard, 20 January 1998.

3.2.1.2.2 Transport Services

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

3.2.1.2.2.1 Transmission Control Protocol/User Datagram Protocol Over Internet Protocol

3.2.1.2.2.1.1 Transmission Control Protocol

Transmission Control Protocol (TCP) provides a reliable connection-oriented transport service. The following standards are mandated:

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

3.2.1.2.2.1.2 User Datagram Protocol

User Datagram Protocol (UDP) provides an unacknowledged, connectionless datagram transport service. The following standard is mandated:

- IETF Standard 6/RFC 768, User Datagram Protocol, 28 August 1980.

3.2.1.2.2.1.3 Internet Protocol

Internet Protocol (IP) is a basic connectionless datagram service. All protocols within the IP suite use the IP datagram as the basic data transport mechanism. Two other protocols are considered integral parts of IP: the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP). ICMP is used to provide error reporting, flow control, and route redirection. IGMP provides multicast extensions for hosts to report their group membership to multicast routers. RFC 2236, IGMPv2 allows group membership termination to be quickly reported to the routing protocol, which is important for high-bandwidth multicast groups and/or subnets with highly volatile group membership. The following standards are mandated:

- IETF Standard 5/RFC 791/RFC 950/RFC 919/RFC 922/RFC 792/RFC 1112, Internet Protocol, September 1981. In addition, all implementations of IP must pass the 8-bit Type-of-Service (TOS) byte transparently up and down through the transport layer as defined in IETF Standard 3, Host Requirements.
- IETF RFC 2236, Internet Group Management Protocol, Version 2 (IGMPv2), November 1997.

Furthermore, 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 standard is mandated:

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

3.2.1.2.2.2 Open Systems Interconnection Transport Over IP-Based Networks

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

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

3.2.1.3 Video Teleconferencing Standards

The ASD (C3I) mandated Federal Telecommunications Recommendation (FTR) 1080A-1998 Video Teleconferencing Profile (VCP) identifies ITU-T H.320 as the key standard to provide interoperability between Video Teleconferencing (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 audiographic conferencing, facsimile, still image transfer, annotation, pointing, whiteboard, file transfer, audiovisual control, and application sharing.

For Video Teleconferencing Units (VTUs) and Multipoint Control Units (MCUs) operating at rates of 56 Kbps to 1,920 Kbps, except for operation over packet-based TCP/IP networks, the following standards, as they are profiled by FTR 1080A-1998, Appendix A, Video Teleconferencing Profile, October 1998, are mandated:

Table 3-1: ITU-T/EIA Standards Profiled by FTR 1080A-1998, Appendix A

Standard	Description	Usage
● H.221	Frame structure for 64 to 1920 Kbit/s channel in audiovisual services.	VTU/MCU General
● H.230	Frame-synchronous control and indication signals for audiovisual systems.	VTU/MCU General
● H.242	System for establishing communication between audio visual terminals using digital channels up to 2 Mbits/s.	VTU/MCU General
● H.261	Video CODEC for audiovisual services at px64 Kbps.	VTU/MCU Video
● H.320	Narrow-band visual telephone systems and telephone equipment.	VTU/MCU General
● H.224	Real-time control protocol for simplex applications using the H.221 LSD/HSD/MLP channels.	VTU Multimedia
● H.281	Far-end camera control protocol for video conferences using H.224.	VTU Multimedia
● G.711	Pulse code modulation 3.1 KHz to 48, 56, and 64 (narrowband speech mode).	VTU Audio
● G.722	Audio CODEC, 7 KHz at 48, 56, and 64 Kbps (wideband speech).	VTU/MCU Audio
● G.728	Audio CODEC 3.1 KHz at 16 Kbps (narrowband speech mode).	VTU/MCU Audio
● H.231	Multipoint control unit functional description.	MCU General
● H.243	Procedure for establishing communication between three or more audiovisual terminals using digital channels up to 2 Mbit/s.	MCU General

For applications implementing the features of audiographic conferencing, facsimile, still image transfer, annotation, pointing, whiteboard, file transfer, audiovisual control, and application sharing, operating at data rates of 9.6 to 1,920 Kbps, or operating over LANs, the following standards are mandated:

- ITU-T T.4, Standardization of Group 3 Facsimile Terminals for Document Transmission, April 1999.
- ITU-T T.81, Information Technology – Digital Compression and Coding of Continuous-tone Still Images – Requirements and Guidelines, September 1992.
- ITU-T T.82, Information Technology – Coded Representation of Picture and Audio Information – Progressive Bi-level Image Compression, March 1993.
- ITU-T T.120, Transmission Protocols for Multimedia Data, July 1996.
- ITU-T T.122, Multipoint Communications Service for Audiographic and Audio Visual Conferencing Service Definition, March 1993.
- ITU-T T.123, Protocol Stacks for Audiographic and Audiovisual Teleconferencing Applications, November 1994.
- ITU-T T.124, Generic Conference Control for Audiographic and Audiovisual Terminals and Multipoint Control Units, August 1995.
- ITU-T T.125, Multipoint Communications Service Protocol Specification, April 1994.
- ITU-T T.126, Multipoint Still Image and Annotation Conferencing Protocol Specification, August 1995.
- ITU-T T.127, Multipoint Binary File Transfer Protocol, August 1995.
- ITU-T T.128, Multipoint Application Sharing, February 1998.

For VTC terminals operating within IP Packet Networks, the following standard is mandated:

- ITU-T H.323, Packet-based Multimedia Communications Systems, February 1998. For all other implementations of H.323, such as used over wide area networks where bandwidth, quality of service, and scalability may not be sufficient for IP-based video conferencing, see emerging standards paragraph 3.3.1.2.

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, February 1998.

For inverse multiplexers connected to VTC terminals, and for VTC terminals with built-in inverse multiplexers, 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: <http://disa.dtic.mil/disnvtc>.

3.2.1.4 Facsimile Standards

3.2.1.4.1 Analog Facsimile Standards

For facsimile (analog output) standards that comply with the ITU-T Group 3 specifications, the following standards are mandated:

- EIA/TIA-465-A, Group 3 Facsimile Apparatus for Document Transmission, June 1995.
- EIA/TIA-466-A, Procedures for Document Facsimile Transmission, May 1997.

3.2.1.4.2 Digital Facsimile Standards

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.

3.2.1.5 Imagery Dissemination Communications Standards

The Tactical Communications Protocol 2 (TACO2) is the communications component of the National Imagery Transmission Format 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 in which JTA transfer protocols in 3.2.1.2.2 fail (e.g., 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 (TISs) 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.

3.2.1.6 Global Positioning System

The CJCS (CJCSI 6130.01A, 1998 CJCS Master Positioning, Navigation, and Timing Plan) has declared that the GPS will be the primary radionavigation system source of positioning, navigation and timing (PNT) for DoD. GPS is a space-based, worldwide, precise positioning, velocity, and timing system. It provides an unlimited number of suitably equipped passive users with a force-enhancing, common-grid, all-weather, continuous, three-dimensional PNT capability. The NAVSTAR GPS provides two levels of service—a Standard Positioning Service (SPS) and a Precise Positioning Service (PPS). The following standard is mandated:

- ICD-GPS-200C, NAVSTAR GPS Space Segment/Navigation User Interfaces, 12 April 2000.

The PPS was designed primarily for U.S. military use, and DoD will control access to the PPS through cryptography. DoD GPS users with combat, combat support, or combat service support missions must acquire and use PPS-capable GPS receivers. The U.S. will enter into special arrangements with military users of allied and friendly governments to allow them use of the PPS. The following standards are mandated:

- ICD-GPS-222A, NAVSTAR GPS UE Auxiliary Output Chip Interface (U), 26 April 1996.
- 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.

The United States discontinued the use of Selective Availability (SA); or in other words, SA errors were set to zero (e.g., SA=0). ASD(C3I) issued SA=0 policy and affirmed that Navigation Warfare (NAVWAR) is now the preferred method to prevent adversary use of GPS. NAVWAR is used to deny, degrade, and otherwise disrupt GPS Standard Positioning Service (SPS) within a theater of operations. This policy further states that it is imperative that DoD users incorporate properly keyed Precise Positioning Service receivers unless a waiver to use SPS is obtained.

For additional information associated with the acquisition and use of PPS-capable GPS receivers, including end-of-week rollover compliance, consult the GPS JPO.

3.2.2 Network Standards

Networks are made up of subnetworks, and the internetworking (router) elements needed for information transfer. This section identifies the standards needed to access certain subnetworks and for routing and interoperability between the subnetworks.

3.2.2.1 Internetworking (Router) Standards

Routers are used to interconnect various subnetworks and end-systems. Protocols necessary to provide this service are specified below. RFC 1812 is an umbrella standard that references other documents and corrects errors in some of the referenced documents. In addition, some of the standards mandated for hosts in 3.2.1.2 also apply to routers. The following standards are mandated:

- IETF RFC 1812, Requirements for IP Version 4 Routers, 22 June 1995.
- IETF Standard 6/RFC 768, User Datagram Protocol, 28 August 1980.
- IETF Standard 7/RFC 793, Transmission Control Protocol, September 1981.
- IETF Standard 8/RFC 854/RFC 855, TELNET Protocol, May 1983.
- IETF Standard 13/RFC 1034/RFC 1035, Domain Name System, November 1987.
- IETF RFC 951, Bootstrap Protocol, September 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 1993.
- IETF Standard 33/RFC 1350, The TFTP Protocol (Revision 2), July 1992, to be used for initialization only.

Security requirements are addressed in Section 6.

3.2.2.1.1 Internet Protocol

Internet Protocol (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. Two other protocols are considered integral parts of IP: ICMP and IGMP. ICMP is used to provide error reporting, flow control, and route redirection. IGMP provides multicast extensions for hosts to report their group membership to multicast routers. IETF RFC 2236, IGMP Version 2, is used by IP hosts to report their multicast group memberships to routers. It updates IETF Standard RFC 1112. IGMP Version 2 allows group membership termination to be quickly reported to the routing protocol, which is important for subnets with highly volatile group membership and high bandwidth multicast group.The following standards are mandated:

- IETF Standard 5/RFC 791/RFC 950/RFC 919/RFC 922/RFC 792/RFC 1112, Internet Protocol, September 1981.
- IETF RFC 2236, Internet Group Management Protocol, Version 2 (IGMP v2), November 1997.

In addition, in all implementations of IP routers that transmit or receive multi-addressed datagrams over CNR, the multi-addressed IP option field must be used. The following standard is mandated:

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

3.2.2.1.2 Internet Protocol 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 Shortest 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, A Border Gateway Protocol 4 (BGP-4), 21 March 1995.
- IETF RFC 1772, Application of the Border Gateway Protocol in the Internet, March 1995.

3.2.2.2 Subnetworks

This section identifies the standards needed to access subnetworks used in joint environments.

3.2.2.2.1 Local Area Network Access

While no specific Local Area Network (LAN) technology is mandated, the following is required for interoperability in a joint environment. This requires provision for a LAN interconnection. Ethernet, the implementation of Carrier Sense Multiple Access with Collision Detection (CSMA/CD), is the most common LAN technology in use with TCP/IP. The hosts use a CSMA/CD scheme to control access to the transmission medium. An extension to Ethernet, Fast Ethernet provides interoperable service at both 10 Mbps and 100 Mbps. 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/RFC 894, Standard for the Transmission of IP Datagrams Over Ethernet Networks, April 1984.
- IETF Standard 37/RFC 826, An Ethernet Address Resolution Protocol, November 1982.

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/RFC 1661/RFC 1662, Point-to-Point Protocol (PPP), July 1994.
- IETF RFC 1332, PPP Internet Protocol Control Protocol (IPCP), May 1992.
- IETF RFC 1989, PPP Link Quality Monitoring (LQM), 16 August 1996.
- IETF RFC 1994, PPP Challenge Handshake Authentication Protocol (CHAP), August 1996.
- IETF RFC 1570, PPP LCP Extensions, January 1994.

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

- EIA/TIA-232-F, Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, October 1997.
- EIA/TIA-530-A, High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment, Including Alternative 26-Position Connector, December 1998. (This calls out TIA/EIA-422-B and -423-B).

3.2.2.2.3 Combat Net Radio Networking

Combat Net Radios (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 shall 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, 20 January 1998.

3.2.2.2.4 Integrated Services Digital Network

Integrated Services Digital Network (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. It should be noted that deployable systems might additionally be required to support other non-North American ISDN standards when accessing region-specific international infrastructure for ISDN services. The JTA recognizes that this is a critical area affecting interoperability but does not recommend specific solutions in this version. The following standards are mandated:

For 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 (Reaffirmed 1999).

For PRI physical layer:

- ANSI T1.403.01-1999, Network and Customer Installation Interfaces – (ISDN) Primary Rate Layer 1 Electrical Interface Specification, 1999.

For the data-link layer:

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

For signaling at the user-network interface:

- ANSI T1.607-1998, 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 T1.619-1992, Multi-Level Precedence and Preemption (MLPP) Service, ISDN Supplementary Service Description, 1992.
- ANSI T1.619a-1994, Supplement, 1994.

For signaling at node-to-node interface:

- ANSI T1.111-1996, Signaling System No. 7, Message Transfer Part.
- ANSI T1.112-1996, Signaling System No. 7, Signaling Connection Control Part Functional Description.
- ANSI T1.113-1995, Signaling System No. 7, ISDN User Part.
- ANSI T1.114-1996, Signaling System No. 7, Transaction Capability Application Part.

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, 13 May 1994.

3.2.2.2.5 Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is a high-speed switched data transport technology that takes advantage of primarily low BER transmission media to accommodate intelligent multiplexing of voice, data, video, 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 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 standards below are mandated. For information on ATM-Forum-approved specifications, see URL: <http://www.atmforum.com/atmforum/specs/specs.html>.

For Physical Layer:

- ATM Forum, af-phy-0040.000, Physical Interface Specification for 25.6 Mbps over Twisted Pair Cable, November 1995.
- ATM Forum, af-uni-0010.002, ATM UNI Specification V 3.1, Section 2.1, and 2.4, September 1994.
- ATM Forum, af-phy-0015.000, ATM Physical Medium Dependent Interface for 155 Mbps over Twisted Pair Cable, September 1994.
- ATM Forum, af-phy-0016.000, DS1 Physical Layer Specification, September 1994.
- ATM Forum, af-phy-0054.000, DS3 Physical Layer Interface Specification, January 1996.
- ATM Forum, af-phy-0046.000, 622.08 Mbps Physical Layer Specification, January 1996.
- ATM Forum, af-phy-0064.000, E1 Physical 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 UNI Specification V3.1, September 1994.
- ATM Forum, af-sig-0061.000, ATM UNI 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-to-Network Interfaces:

- ATM Forum, af-pnni-0055.000, Private Network to Network Interface (PNNI) Specification, Version 1.0, March 1996.
- ATM Forum,af-pnni-0066.000, PNNI 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, Local Area Network Emulation (LANE) Over ATM Version 2.0 – LUNI Specification, July 1997.
- ATM Forum, af-lane-0093.000, LANE Client Management Specification, Version 2.0, October 1998.
- 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 Gigabit Ethernet

While no specific LAN/CAN technology is mandated, when using Gigabit Ethernet (1,000 Mbps service) over fiber on a campus environment, the following physical layer and framing requirements standard is mandated:

- IEEE 802.3-1998, IEEE Standard for 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, (originally developed as IEEE 802.3z-1998).

When using Gigabit Ethernet over Category 5 copper cabling, the following standard is mandated:

- IEEE 802.3ab-1999, IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications – Physical Layer Parameters and Specifications for 1000Mb/s Operation over 4-Pair of Category 5 Balanced Copper Cabling, Type 1000BASE-T.

3.2.3 Transmission Media

3.2.3.1 Military Satellite Communications

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

3.2.3.1.1 Ultra High Frequency Satellite Terminal Standards

3.2.3.1.1.1 5-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.

3.2.3.1.1.2 5-KHz Demand-Assigned Multiple Access Service

For 5-KHz Demand-Assigned Multiple Access (DAMA) service, supporting the transmission of data at 75 to 2400 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; Notice of Change 2, 22 January 1999; and Notice of Change 3, 4 June 1999.

3.2.3.1.1.3 25-KHz Time Division Multiple Access/Demand-Assigned Multiple Access Service

For 25-KHz Time Division Multiple Access (TDMA)/DAMA service, supporting the transmission of voice at 2,400, 4,800, or 16,000 bps and data at rates of 75 to 16,000 bps, the following standard is mandated:

- MIL-STD-188-183A, Interoperability Standard for 25-Khz TDMA/DAMA Terminal Waveform, 20 March 1998; with Notice of Change 1, 9 September 1998; and Notice of Change 2, 4 June 1999.

3.2.3.1.1.4 Data Control Waveform

For data controllers operating 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.

3.2.3.1.1.5 Demand-Assigned Multiple Access 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.

3.2.3.1.2 Super High Frequency Satellite Terminal Standards

3.2.3.1.2.1 Earth Terminals

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

- MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995; with Notice of Change 1, 9 September 1998.

3.2.3.1.2.2 Phase-Shift Keying Modems

For minimum mandatory requirements to ensure interoperability of Phase-Shift Keying (PSK) modems operating in Frequency Division Multiple Access (FDMA) 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.

3.2.3.1.3 Extremely High Frequency Satellite Payload and Terminal Standards

3.2.3.1.3.1 Low Data Rate

For waveform, signal processing, and protocol requirements for acquisition, access control, and communications for Low Data Rate (LDR) (75 to 2,400 bps) Extremely High Frequency (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.

3.2.3.1.3.2 Medium Data Rate (MDR)

For waveform, signal processing, and protocol requirements for acquisition, access control, and communications for Medium Data Rate (MDR) (4.8 Kbps to 1.544 Mbps) EHF satellite data links, the following standard is mandated:

- MIL-STD-188-136A, EHF MDR Uplinks and Downlinks, 8 June 1998; with Notice of Change 1, 1 July 1999.

3.2.3.1.4 Satellite State of Health Communication Standards

National Space Policy directed DoD to lead U.S. Government efforts to improve satellite operations interoperability among U.S. Government agencies. The National Security Space Architect's Satellite Operations Architecture Team recommended a common set of standards for low data rate satellite telemetry and commanding. These standards will allow DoD to share health and status resources with other U.S. Government agencies and with allies to enhance satellite operations while limiting costs. The standards provide a baseline for low data rate communication of health and status information between a spacecraft and the ground. These standards are mandated for S-band communication, but may be applied more generally.

For establishing the physical layer to support satellite health and status communications in the S-band during launch, early orbit, severe anomaly and disposal operations, the following standard is mandated:

- CCSDS 401.0 – B-6, Radio Frequency and Modulation Systems – Part 1: Earth Stations and Spacecraft, May 2000, Consultative Committee for Space Data Systems.

For processing data being sent into distinct, easily distinguishable messages that allow reconstruction of the data with low error probability, the following standard is mandated:

- ISO 11754:1994, Telemetry Channel Coding.

For the data unit formats and functions implemented within the coding and physical layers of the satellite health and status communications, the following standard is mandated:

- ISO 12171:1998, Telecommand, Channel Service, Architectural Specification.

For procedures and data unit formats implemented within the segmentation and transfer layers of the telecommand data routing service, the following standard is mandated:

- ISO 12172:1998, Telecommand, Data Routing Service.

For detailed specification of the logic required to carry out command operation procedure-1 (COP-1) of the transfer layer, the following standard is mandated:

- ISO 12173:1998, Telecommand, Command Operation Procedures.

For the data unit formats and functions implemented within the application, system management, and packetization layers of the satellite command data management service, the following standard is mandated:

- ISO 12174:1998, Telecommand, Data Management Service, Architectural Specification.

Packet telemetry provides a mechanism for implementing common data transport structures and protocols to enhance the development and operation of space mission systems. For facilitating the

transmission of space-acquired data from source to user in a standardized manner, the following standard is mandated:

- ISO 13419:1997, Packet Telemetry.

3.2.3.2 Radio Communications

3.2.3.2.1 Low Frequency and Very Low Frequency

For radio subsystem requirements operating in the Low Frequency (LF)/Very Low Frequency (VLF) frequency bands, the following standard is mandated:

- 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.

3.2.3.2.2 High Frequency

3.2.3.2.2.1 High Frequency and Automatic Link Establishment

For both Automatic Link Establishment (ALE) and radio subsystem requirements operating in the High Frequency (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.

3.2.3.2.2.2 Anti-Jamming Capability

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

- MIL-STD-188-148A, Interoperability Standard for Anti-Jam Communications in the HF Band (2-30 Mhz), 18 March 1992.

3.2.3.2.2.3 Data Modems

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

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

3.2.3.2.3 Very High Frequency

For radio subsystem requirements operating in the Very High Frequency (VHF) frequency bands, the following standard is mandated:

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

3.2.3.2.4 Ultra High Frequency

3.2.3.2.4.1 Ultra High Frequency Radio

For radio subsystem requirements operating in the Ultra High Frequency (UHF) frequency bands, the following standard is mandated:

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

3.2.3.2.4.2 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.

3.2.3.2.5 Super High Frequency

For radio subsystem requirements operating in the Super High Frequency (SHF) frequency bands, the following standard is mandated:

- MIL-STD-188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment, 7 May 1987; with Notice of Change 1, 28 July 1992.

3.2.3.2.6 Link 16 Transmission Standards

For communicating with the Joint Tactical Information Distribution System (JTIDS)/Multi-Functional Information Distribution System (MIDS) radios, the following standard is mandated:

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

3.2.3.3 Synchronous Optical Network Transmission Facilities

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. The following standards are mandated:

- ANSI T1.105-1995, Telecommunications - Synchronous Optical Network (SONET) Basic Description Including Multiplex Structure, Rates and Formats (Revision and Consolidation of ANSI T1.105-1991 and ANSI T1.105A-1991).
- ANSI T1.107-1995, Digital Hierarchy - Formats Specifications,1995.
- ANSI T1.117-1991, (R1997), Digital Hierarchy - Optical Interface Specifications (Single Mode - Short Reach), (Reaffirmed 1997).

The citation of applicable ANSI standards for SONET does not ensure C4I interoperability in regions outside North America where standards for these services differ. The JTA recognizes that this is a critical area affecting interoperability but does not recommend specific solutions in this version.

3.2.4 Network and Systems Management

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

3.2.4.1 Data Communications Management

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

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

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

- IETF Standard 16/RFC 1155/RFC 1212, Structure of Management Information, May 1990.
- IETF Standard 17/RFC 1213, Management Information Base, March 1991.
- IETF RFC 1514, Host Resources MIB, September 1993.
- IETF Standard 50/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.

3.2.4.2 Telecommunications Management

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

- ANSI T1.204 -1997, OAM&P - Lower Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements, 1997.
- ANSI T1.208 -1997, 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 (CMIP): Protocol Implementation Conformance Statement (PICS) proforma.

3.3 Emerging Standards

Commercial communications standards and products will evolve over time. The JTA must also evolve to benefit from these standards and products. The purpose of this section is to provide notice of those standards expected to be elevated to mandatory status when implementations of the standards mature.

3.3.1 End-System Standards

3.3.1.1 Internet Standards

IP Next Generation/Version 6 (IPv6). IPv6 is being designed to provide better internetworking capabilities than are currently available within IP (Version 4). IPv6 will include support for the following: expanded addressing and routing capabilities, authentication and privacy, auto-configuration, and increased quality of service capabilities. IPv6 is described by proposed and draft IETF standards including:

- IETF RFC 2373, Internet Protocol, Version 6 (IPv6) Addressing Architecture, July 1998.
- IETF RFC 2374, Internet Protocol, Version 6 (IPv6) Aggregatable Global Unicast Address Format, July 1998.
- IETF RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, December 1998.
- IETF RFC 2461, Neighbor Discovery for IP Version 6, (IPv6), December 1998.
- IETF RFC 2462, IPv6 Stateless Address Autoconfiguration, December 1998.
- IETF RFC 2463, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, December 1998.

Lightweight Directory Access Protocol 3 (LDAPv3). 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.

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, RFC 2002, entitled IP Mobility Support.

Quality of Service (QoS). 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. Resource ReSerVation Protocol (RSVP) is used by a host to request specific qualities of service from the network for particular application data streams or flows. See 3.3.2.3 for emerging Network QoS standards. The following receiver-initiated QoS standard is emerging:

- IETF RFC 2205, Resource ReSerVation Protocol RSVP Version 1 Functional Specification, September 1997.

Voice Over IP (VoIP). Voice Over IP technologies unite the telephony and data worlds, and allow voice traffic to be transmitted over corporate enterprise networks, intranets, and the Internet. Two nearly compatible approaches have been taken to bring voice to TCP/IP networks. On the one hand, the ITU has created H.323, a set of standards specifying protocols to encapsulate ISDN call signaling over an IP transport network. On the other hand, the IETF has created a set of standards to perform similar functions, under the names Session Initiation Protocol (SIP) and Media Gateway Control (Megaco). Both approaches use an IETF standard, RTP (Realtime Transport Protocol), for their voice channels. The SIP standard concerns simple call placement, but is designed so that its scope is easily expandable. Megaco neatly separates out the functions required for interoperability with legacy equipment such as Signaling System 7 circuit switches. In contrast, the H.323 standards for call placement, H.225, H.245, and Q.931 (including RAS) are explicit in the signals that may be sent and the expected responses. The following VoIP standards are emerging:

- ITU-T Recommendation H.323, Packet-Based Multimedia Communications Systems (Version 2), January 1998.
- IETF RFC 2543, Session Initiation Protocol (SIP), March 1999.
- IETF draft-ietf-megaco-protocol-08.txt, Megaco Protocol, April 2000.

3.3.1.2 Video Teleconferencing Standards

There are three 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.
- ITU-T H.323, has the most industry support for VTC over ATM. It provides for two modes of operation over ATM: 1) IP over ATM media stream and 2) Real-Time Protocol (RTP) over ATM media stream transport (H.323 Annex C). Implementation of H.323 over non-LAN media (e.g., Metropolitan Area Networks [MANs] and WANs, such as the Internet, SIPRNET, JWICS) is still evolving.

3.3.1.3 Communication Protocols for High-Stress, Resource-Constrained Environments

DoD entered a cooperative effort in September 1997 with the National Aeronautics and Space Administration (NASA) and the National Security Agency (NSA) to develop Internet-based protocols for "stressed" communications links. Such links are characterized by one or more of: high bit error rates, long delays, low bandwidths, and high degrees of asymmetry. This work is also applicable for systems with limited computer processing power. The cognizant DoD office is SMC/XR. The protocol suite, called the Space Communications Protocol Specification (SCPS), increases the reliability and speed of data transfer over such links, increases interoperability with both DoD and non-DoD assets, and decreases the cost of operating our systems. This set of protocols is particularly applicable to radio frequency Internet communications in battlefield jamming environments. The suite has been issued as both Consultative Committee for Space Data Systems (CCSDS) and ISO standards (with the same content). The suite consists of the following four protocols that operate at and above the network layer of the Open Systems Interconnect (OSI) model:

- The File Protocol (FP) is an application layer protocol (layer 7 in the OSI model) and is an extension of the Internet File Transfer Protocol (FTP). FP adds the ability to update individual records in a file, to suspend and resume file transfers at user request, to automatically restart file transmission in mid-transmission after a communications interruption, and to suppress the text of server replies. FP and FTP clients and servers can interoperate (at the reduced functionality of FTP, i.e., without the FP extensions).
- The Transport Protocol (TP) is a transport layer protocol (layer 4 in the OSI model) and is an extension of the Internet Transmission Control Protocol (TCP). TP can provide better end-to-end throughput in a jamming or noisy radio frequency environment because it can respond to corruption and temporary link outage in addition to congestion. TP's selective negative acknowledgements increase performance in noisy and asymmetric environments. Performance in asymmetric environments is also improved by permitting reduced acknowledgement rates. TP also supports a loss-tolerant compressed TCP header and "best effort" data transfer protocol. TP and TCP clients and servers can interoperate (at the reduced functionality of TCP without the TP extensions).
- The Security Protocol (SP) operates between the network and transport layers (layers 3 and 4). SP is an optional protocol that provides security capabilities (confidentiality, source authentication, and integrity) for the network layer. SP is analogous to IPSEC, but SP is a separate protocol with reduced overhead.
- The Network Protocol (NP) is a network layer protocol (layer 3 in the OSI model) developed to be a bit-efficient, scalable protocol for a broad range of environments. Among other things, NP provides for selectable routing method, connectionless and managed-connection operations, corruption and congestion signaling to TP, and handling of packet precedence. NP is particularly useful in systems that have changing network connectivities. The other protocols

can operate on Internet Protocol if Network Protocol is not used. In most cases IP packets and NP packets can be translated between each other using a gateway. The concept is that TCP/IP would be used in less stressed communication environments, and then translated or tunneled to NP where necessary before entering the stressed communications channel.

For stressed communications environments (such as satellite links) where high bit error rates, large delays, low bandwidth, and/or data rate asymmetry make the standard TCP/IP suite's performance unacceptable, the following standards are emerging for internetworking and file exchange:

- CCSDS 713.0-B-1/ISO 15891:2000, Space data and information transfer systems – Protocol specification for space communications – Network protocol, 5 October 2000. (Adopts MIL-STD-2045-4300)
- CCSDS 713.5-B-1/ISO 15892:2000, Space data and information transfer systems – Protocol specification for space communications – Security protocol, 5 October 2000. (Adopts MIL-STD-2045-4301)
- CCSDS 714.0-B-1/ISO 15893:2000, Space data and information transfer systems – Protocol specification for space communications – Transport protocol, 5 October 2000. (Adopts MIL-STD-2045-4400)
- CCSDS 717.0-B-1/ISO 15894:2000, Space data and information transfer systems – Protocol specification for space communications – File protocol, 5 October 2000. (Adopts MIL-STD-2045-4700).

More information is available at <http://www.scps.org> and <http://www.ccsds.org>.

3.3.1.4 Global Positioning System

The GPS Signal-in-Space (SIS) is being enhanced to accommodate next-generation security functions. These functions will significantly enhance the combatant commander's ability to use the GPS PPS capability and other GPS sensor information in all environments. These functions are exclusively supported by the Selective Availability Anti-Spoofing Module (SAASM) architecture. The following standard is being tracked as a GPS SIS emerging standard:

- SS-GPS-001A, Navstar GPS Selective Availability Anti-Spoofing Module System Specification, 27 Sep 99.

3.3.2 Network Standards

3.3.2.1 Wireless LAN

The 802.11 family of standards provide a common set of operational rules for airwave interoperability of wireless Local Area Network (LAN) products from different vendors. The original IEEE 802.11 standard was updated with editorial changes. The original physical layer was updated by IEEE 802.11a and IEEE 802.11b. The Medium Access Control (MAC) layer is currently undergoing revision and will be updated by IEEE 802.11f. The emerging standards include:

- ISO/IEC 8802-11:1999, (ISO/IEC) (IEEE Std 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 802.11a-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.

- IEEE 802.11b-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: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band.

3.3.2.2 ATM-Related Standards

The following ATM-related standards are emerging:

- ATM Forum, af-tm-0121.000, Traffic Management Specification Version 4.1, March 1999.
- ATM Forum, af-sig-0076.000, Addendum to UNI Signalling V4.0 for ABR parameter negotiation, January 1997.
- ATM Forum, af-mpoa-0114.000, Multi-Protocol Over ATM Version 1.1, May 1999.
- ATM Forum, af-vtoa-0113.000, ATM Trunking Using AAL2 for Narrowband Services, February 1999.
- ATM Forum, af-phy-0086.001, Inverse Multiplexing for ATM (IMA) Specification Version 1.1, March 1999.
- ATM Forum, af-saa-0124.000, Gateway for H.323 Media Transport Over ATM, July 1999.
- ATM Forum, af-vtoa-0119.000, Low Speed Circuit Emulation Service (LSCES), May 1999.
- ATM Forum, af-lane-0112.000, LAN Emulation Over ATM Version 2 – LNNI Specification, February 1999.
- ATM Forum, af-ra-0123.000, PNNI Addendum for Mobility Extensions, Version 1.0, May 1999.
- ATM Forum, af-sec-0096.000, ATM Security Framework Specification Version 1.0, February 1998.
- TIA/EIA/IS-787, Common ATM Satellite Interface Interoperability Specification (CASI), July 1999.

For ATM Conformance Testing, the 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.

3.3.2.3 Network Quality of Service (QoS) Standards

Quality of Service is the ability of a network to ensure that the predetermined traffic and service requirements of a network element can be satisfied. Multiple forums 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 following standard protocols currently under development to enable end-to-end QoS, are emerging:

- IETF RFC 2205, Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification, September 1997.
- IETF RFC 2207, RSVP Extensions for IPSEC Data Flows, September 1997.
- IETF RFC 2380, RSVP over ATM Implementation Requirements, August 1998.
- ISO/IEC 15802-3, IEEE 802.1D dtd 25 JUN 1998 Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Common Specifications – Part 3: Media Access Control (MAC) Bridges (Replaces IEEE P802.1P, 802.1J-1996, 802.6K-1992, 802.11C-1998, and P802.12E).
- IEEE 802.1Q:1998, IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridge Local Area Networks.

3.3.2.4 Personal Communications Services and Mobile Cellular

Personal Communications Services (PCS), second-generation mobile systems, will support both terminal mobility and personal mobility. Terminal mobility is based on wireless access to the public switched telephone network (PSTN). Personal mobility allows users of telecommunications services to gain access to these services from any convenient terminal (either wireline or wireless). Mobile cellular radio can be regarded as an early form of "personal communications service" allowing subscribers to place and receive telephone calls over the PSTN wherever cellular service is provided. The three predominant competing worldwide methods for digital PCS and Mobile Cellular access are: Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), and Global System for Mobile Communications (GSM). Of these three, CDMA offers the best technical advantages for military applications based on its utilization of Direct Sequence Spread Spectrum (DSSS) techniques for increased channel capacity, low probability of intercept (LPI), and protection against jamming. CDMA's low transmission power requirements should also reduce portable power consumption. It should be recognized that for Operations-Other-Than-War (OOTW), a user may require support of multiple protocols to access region-specific international digital PCS/Mobile Cellular infrastructures. The following PCS/CDMA standards and PCS/Mobile Cellular Interface standards are emerging:

- ANSI/J-STD-018-96, Recommended Minimum Performance Requirements for 1.8 to 2.0 GHz CDMA Personal Stations.
- ANSI/J-STD-019-96, Recommended Minimum Performance Requirements for Base Stations Supporting 1.8 to 2.0 GHz CDMA Personal Stations.
- TIA/EIA-95-B-99, Mobile Station-Base Station Compatibility for Wideband Spread Spectrum Cellular Systems.
- TIA/EIA-41-D-97, Cellular Radio Telecommunications Intersystem Operations.

3.3.2.5 International Mobile Telecommunications - 2000

*International Mobile Telecommunications - 2000 (*IMT-2000) defines third-generation mobile systems that were scheduled to start service around the year 2000. Also known as Future Public Land Mobile Telecommunications Systems (FPLMTS), these systems will provide access by means of one or more radio links to a wide variety of telecommunication services supported by the fixed and mobile telecommunications networks (e.g., PSTN/ISDN) and to other services that may be unique to IMT-2000. A range of mobile terminal types, designed for mobile and fixed use, is envisaged linking to terrestrial- and/or satellite-based networks. A goal for third-generation mobile systems is to provide global coverage and to enable terminals to be capable of seamless roaming between multiple networks. The ability to coexist and work with pre-IMT-2000 systems is required. The Radio Communications Assembly-2000 gave final approval of Recommendation ITU-R M.(IMT.RSPC), "Detailed Specifications of the Radio Interfaces of IMT-2000" for the radio interfaces for IMT-2000 on 5 May 2000. The IMT-2000 radio interface terrestrial standard consists of a set of radio interfaces, which allow performance optimization in a wide range of radio operating environments. The family of IMT-2000 terrestrial radio transmission technologies (RTT) is as follows: CDMA Direct Spread/CDMA Multi-Carrier/CDMA Time Division Duplex (TDD)/TDMA Single-Carrier/TDMA Multi Carrier. Follow-on work on major enhancements to the RTTs' specifications is ongoing in ITU-R Working Party 8F. In addition, standards work is continuing to ensure that the RTTs will support the capability of operating with the two worldwide telecommunications networks: evolved GSM-MAP and ANSI-41. Limited trials of 3G services are expected to be commenced in various regions of the world, especially Japan, in late 2001. The European Union plans a rollout of 3G services in 2002. U.S. 3G services (e.g., 144Kbps/384 Kbps data capability) are expected to be provided in focused markets in late 2003. A mass market for 3G in the U.S. and Europe is not expected to develop until 2005.

3.3.2.6 Point-to-Point Standards.

IETF draft standard IETF RFC 1990, PPP Multilink Protocol, allows for aggregation of bandwidth via multiple simultaneous dial-up connections. It proposes a method for splitting, recombining, and sequencing datagrams across multiple PPP links connecting two systems.

3.3.3 Military Satellite Communications

3.3.3.1 SHF Satellite Terminal Standards.

The following draft standards are under development: MIL-STD-188-166 (Interface Standard, Interoperability and Performance Standard for SHF SATCOM Link Control), MIL-STD-188-167 (Interface Standard, Message Format for SHF SATCOM Link Control), and MIL-STD-188-168 (Interface Standard, Interoperability and Performance Standards for SHF Satellite Communications Mulitplexers and Demultiplexers).

3.3.4 Radio Communications

3.3.4.1 Link 22 Transmission Standards

Link 22 Transmission media will be used to exchange Link 22 messages. Link 22 messages, composed of F-Series formats, will be used for the exchange of maritime operational data between tactical data systems using line of sight (UHF) and beyond line of sight (HF) bands. The standard for Link 22 waveform is under development.

3.3.4.2 VHF

MIL-STD-188-241, RF Interface Requirements for VHF Frequency Hopping Tactical Radio Systems, is a classified document currently under development. This standard identifies the anti-jamming capabilities for VHF radio systems.

3.3.5 Network Management

3.3.5.1 Simple Network Management Protocol Version 3 (SNMPv3)

The SNMPv3 Management Framework is described in IETF-Proposed Standard RFCs 2271-2275. 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). Implementations of the RFCs are undergoing interoperability tests as part of the process to advance these specifications from Proposed to Draft state.

3.3.5.2 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 1471, Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol, June 1993.
- IETF RFC 1472, Definitions of Managed Objects for the Security Protocol of the Point-to-Point Protocol, June 1993.
- IETF RFC 1473, Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol, June 1993.
- IETF RFC 1474, Definitions of Managed Objects for the Bridge Network Control Protocol of the Point-to-Point Protocol, June 1993.
- IETF RFC 1611, DNS Server MIB Extensions, May 1994.
- IETF RFC 1612, DNS Resolver MIB Extensions, May 1994.

- IETF RFC 1657,Definitions of Management Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2, July 1994.
- IETF RFC 2006, Definitions of Managed objects for IP Mobility Support using SMIv2, October 1996.
- IETF RFC 2011, SNMPv2 Management Information Base for the Internet Protocol, November 1996.
- IETF RFC 2012, SNMPv2 Management Information Base for the Transmission Control Protocol (TCP), November 1996.
- IETF RFC 2013, SNMPv2 Management Information Base for the User Datagram Protocol (UDP), November 1996.
- IETF RFC 2021, Remote Network Monitoring Management Information Base Version 2, using SMIv2, January 1997.
- IETF RFC 2248, Network Services Monitoring MIB, January 1998.
- IETF RFC 2249, Mail Monitoring MIB, January 1998.
- IETF RFC 2515, Definitions of Managed Objects for ATM Management, February 1999.
- IETF RFC 2605, Directory Server Monitoring MIB, June 1999.

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 DoD 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.

Security standards related to this section are in 6.2.4.

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/or 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 applications, composed of one or more related activities. The primary product of each activity model is the definition of a measurable set of products, services, and information required to support the mission-area function.

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, DoD created the Defense Data Dictionary System (DDDS). The DDDS, managed by 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 Model (DDM), now called the DoD Data Architecture (DDA), and to document content and format for data elements. System developers use this repository as a primary source of data element standards.

Information exchange is accomplished for the most part by sending formatted messages. The definition and documentation of these exchange mechanisms are provided by various messaging standards. Each message standard provides a means to define message form and functions (i.e., transfer syntax), which includes the definition of the message elements contained in each message. The message fields, which

are currently defined in the various message standards, are not necessarily mutually consistent, nor are they consistently 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 following a rigid format. A model-based structure will provide definitions that will be data element-based and will be compliant with DoD data element standards established in accordance with 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. The primary component of this infrastructure is the Tactical Data Link (TDL), composed of message elements/messages and physical media. However, due to the diversity of warfighter requirements, no single data link is applicable to every platform and weapon system.

Tactical Digital Information Links (TADILs), structured on bit-oriented message standards, evolved to meet critical real-time and near-real-time message requirements. The United States Message Text Format (USMTF), designed primarily for non-real-time exchange, is based on a character-oriented message format and is the standard for human-readable and machine-processable information exchange. The goal of TDLs, character-oriented/human-readable (USMTF messages), imagery, voice, and video standards is to provide a timely, integrated, and coherent picture for joint commanders and their operational forces.

Disparate data link message formats and communications media have resulted in late delivery of crucial battlefield information. This causes significant interoperability problems among the Commanders-in-Chief (CINCs), Services, Agencies (C/S/A), and allied nations. Currently, it is difficult to establish seamless information flow among diverse data-link units. Future joint operations, such as ballistic missile defense and battlefield digitization, will place greater emphasis on the need for automated C4I functions. Tomorrow's battlefields will vastly increase the burden on networks.

4.2 Mandated Standards

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 or major system update, an activity model is prepared to depict the mission-area function to a level of detail sufficient to identify each entity in the data model that is involved in an activity. The activity model can form 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, IDEF0 Function Modeling, is the standard that describes the IDEF0 modeling language semantics and syntax, as well as associated rules and techniques, for developing structured graphical representations of a system or enterprise.

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 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. FIPS PUB 184 is the standard that 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 standard for Data Modeling is:

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

4.2.3 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 DoD 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 DDM. 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.

4.2.4 DoD Data Definitions

The Defense Data Dictionary System (DDDS) is a central database that includes standard data entities, data elements, and provides access to DDM 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. System developers shall use this repository as a primary source of data element standards.

The mandated standards for DoD Data Definitions are

- DoD Manual 8320.1-M-1, DoD Data Standardization Procedures, April 1998.
- Defense Data Dictionary System (DDDS).

4.2.5 Information Exchange Standards

4.2.5.1 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 follows:

- The exchange of information among applications using shared databases or formatted message structures shall be based on the logical data models developed from identifying information requirements through activity models, where appropriate. The data model identifies the logical information requirements, which shall be developed into physical database schemata and standard data elements.
- The standard data elements shall be exchanged using the data-management, data interchange, and distributed-computing services of application platforms. (Refer to Section 2 for further guidance on these services.) The goal is to exchange information directly between information systems, subject to security classification considerations.
- 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.

Information-Exchange standards help form the Defense Information Infrastructure (DII) Common Operating Environment (COE), ensuring the use of system or application formats that can share data. Key references include 2.2.2.1.3, for SQL standards in Data Management Services and 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.

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

4.2.5.2.1 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, LINK 22, 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 are described in the Joint Tactical Data Link Management Plan (JTDLMP), dated 6 June 1996.

New message requirements shall use these messages and data elements or use the message construction hierarchy described in the JTDLMP. Where not addressed by another standard within the JTA (e.g., TADIL-J and VMF), the following standards are mandated as the format for transferring (though not processing) binary floating-point data:

- MIL-STD-6016A, Tactical Digital Information Link (TADIL) J Message Standard, 30 April 1999.
- STANAG 5516, Edition 1, Tactical Data Exchange – LINK 16, Ratified 15 January 1997.
- Variable Message Format (VMF), Technical Interface Design Plan (Test Edition) Reissue 3, 17 June 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>.

4.2.5.2.2 Character-Based Formatted Messages

United States Message Text Format (USMTF) messages are jointly agreed, fixed-format, character-oriented messages that are human-readable and machine-processable. USMTFs are the mandatory standard for record messages when communicating with the Joint Staff, Combatant Commands, and Service Components. The mandated standard for USMTF Messages is:

- MIL-STD-6040, United States Message Text Format (USMTF), 31 March 2001.

Note: Per Service agreement, the USMTF is updated annually. Implementers have a full year from each release date to update their systems.

4.2.5.3 Binary Floating-Point Data Interchange

ANSI/IEEE 754-1985 defines formats and functional requirements for processing binary floating-point numbers including infinities and Not-a-Number values. A few standards with a larger scope define their own specialized binary floating-point format for use within the scope of that standard. Where not addressed by another standard within JTA (e.g., TADIL J and JVMF), the following standard is mandated as the format for transferring (though not processing) binary floating-point data:

- ANSI/IEEE 754-1985, IEEE standard for Binary Floating-Point Arithmetic, March 21, 1985.

4.2.6 Object Modeling

Object-oriented modeling techniques are used in the specification and development of object-oriented systems and to model and design the interoperability requirements of distributed components.

The Unified Modeling Language (UML) is a language for specifying, constructing, visualizing, and documenting the artifacts of a software-intensive system. In an elaborative approach, developers develop models and increasingly add details until the model becomes the actual system being developed. Information may be obtained from the Web at http://www.omg.org. The following standard is mandated:

- Object Management Group (OMG) Unified Modeling Language (UML) Specification, Version 1.3, June 1999.

4.3 Emerging Standards

The emerging standards listed in this subsection are expected to be elevated to mandatory status when implementations of the standards mature.

4.3.1 Object Modeling

The XML Metadata Interchange (XMI) standard describes an information interchange model. This model allows developers using UML object technology tools to exchange programming data in a common format by defining a set of XML DTDs (Document Type Definitions) for exchanging UML information. The following standards are 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.

4.3.2 DoD Data Definitions

The DISA Joint Information Engineering Organization (JIEO), in coordination with the Standards Coordinating Committee (SCC) and the Change Control Board (CCB), will develop the strategy/policy for migration from many tactical data-link (bit-oriented) and character-oriented joint message standards to a minimal family of DoD 8320.1-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. The Data Model basis for the data elements will ensure that the information is normalized.

4.3.3 Information Exchange Standards

The emerging standards for information exchange are:

- Multi-functional Information Distribution System (MIDS), MIDS is a planned replacement for the Joint Tactical Information Distribution System (JTIDS). MIDS will provide secure jam-resistant communications, utilizing tactical digital data and voice. Message format standards for MIDS will not change from those of the JTIDS.
- STANAG 5522, Edition 1, Tactical Data Exchange – LINK 22 (Undated) is the Multinational Group (MG) agreed Configuration Management (CM) baseline document as of 15 September 1995. It is distributed as ADSIA(DLWG)-RCU-C-74-95.

4.3.4 Data Modeling

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

with emerging dynamic modeling techniques to produce full object-oriented models. The following standard is emerging:

– IEEE 1320.2-1998, IEEE Standard Conceptual Modeling Language-Syntax and Semantics for IDEF1X97 (IDEFobject).

Page intentionally left blank.

Section 5: Human-Computer Interface Standards

5.1 Introduction

5.1.1 Purpose

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

5.1.2 Scope

This section addresses the presentation and dialogue of the Human-Computer Interface. Section 2 addresses the API definitions and protocols. See JTA 6.2.5 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 effectively interact 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 Mandated Standards

This subsection identifies the mandatory standards, profiles, and practices for human-computer interfaces. 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).

5.2.1 General

The predominant types of HCIs include graphical user interfaces (GUIs) and character-based interfaces. Although GUIs are the preferred user interface, some specialized devices may require use of character-based interfaces due to operational, technical, or physical constraints. These specialized interfaces shall be defined by domain-level style guides and further detailed in system-level user interface specifications. In order to present a consistent interface to the user, application software shall not mix command line user interfaces and GUIs.

5.2.1.1 Character-Based Interfaces

The following standard is mandated for systems with an approved requirement for a character-based interface:

- DoD Human-Computer Interface 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 Interface

When developing DoD automated systems, the graphical user interface shall be based on one commercial user interface style guide consistent with 5.2.2.1. Hybrid GUIs that mix user interface styles (e.g., Motif with Microsoft Windows) shall not be created. A hybrid GUI is composed of toolkit components from more than one user interface style. When selecting commercial off-the-shelf (COTS)/Government off-the-shelf (GOTS) applications for integration with developed DoD automated systems, maintaining consistency in the user interface style is highly recommended. An application delivers the user interface style that matches the host platform (i.e., Motif on a UNIX platform and Windows on an NT platform). This style conforms to commercial standards, with consistency in style implementation regardless of the development environment used to render the user interface. Applications that use platform-independent languages such as Java deliver the same style as the native application on the host platform.

See 2.2.2.1.2 for mandated GUI standards.

5.2.2 GUI 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 training requirements by ensuring consistent and usable 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 defining “how” the rules are implemented in the application code.

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

The interface developer shall use the selected commercial GUI style guide and the appropriate domain-level style guide for specific style decisions, along with input of human factors specialists to create the system-specific HCI. The following paragraphs include specific guidance regarding the style guide hierarchy levels.

5.2.2.1 Commercial Style Guides

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

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:

- M027: CDE 2.1/Motif 2.1 – Style Guide and Glossary, The Open Group ISBN 1-85912-104-7, October 1997.

- M028: CDE 2.1/Motif 2.1 – Style Guide Certification Check List, The Open Group ISBN 1-85912-109-8, October 1997.
- M029: CDE 2.1/Motif 2.1 – Style Guide Reference, The Open Group ISBN 1-85912-114-4, October 1997.

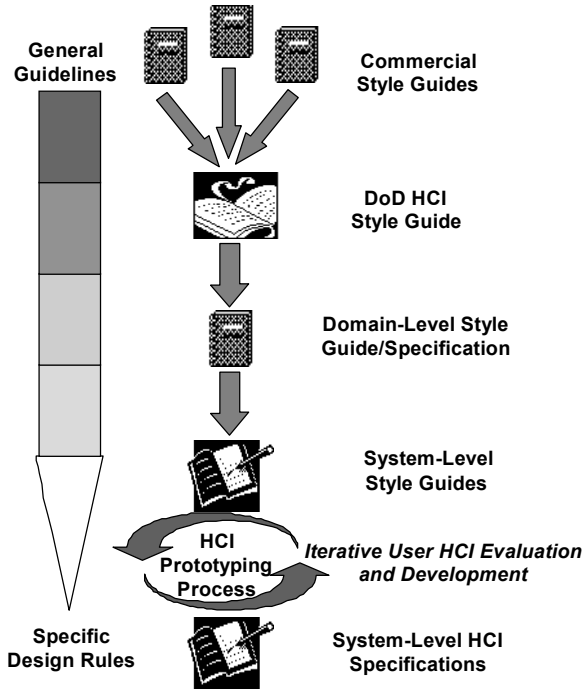


Figure 5-1: HCI Development Guidance

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 Human-Computer Interface Style Guide

The DoD HCI Style Guide is a high-level document providing 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 guidance that can be used for all types of systems including those employing character-based interfaces. Although the DoD HCI Style Guide is not intended to be strictly a compliance document, it does represent DoD policy. The TAFIM has been officially withdrawn, but the DoD HCI Style Guide will be followed until the stand-alone version officially replaces the TAFIM DoD HCI Style Guide. The following guideline is mandated[1]:

[1] On 7 January 2000, TAFIM was cancelled. As a result, the TAFIM Web site may disappear as a resource. A multi-agency, multi-service working group led by the Army was formed to continue support for maintaining/updating the DoD HCI Style Guide due to its criticality to the HCI community and the JTA. Plans are underway for the new DoD HCI Style Guide Working Group to identify and initiate update activities.

- DoD Human-Computer Interface Style Guide, 30 April 1996.

The general principles given in this document apply to all interfaces; some specialized areas, however, require separate consideration. Specialized interfaces, such as those used in hand-held devices, have interface requirements that are beyond the scope of the DoD HCI Style Guide. These systems should 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

The JTA allows for the development of domain-level HCI style guides. These styles, when developed, will reflect the consensus on HCI appearance and behavior for a particular domain within DoD. The domain-level style guide will be the compliance document and may be supplemented by a system-level style guide. Domain-level style guides that make use of commercial standards, COTS products, graphical user interfaces, windows, and/or conventional displays should be developed as extensions to the User Interface Specification for the DII. Domain-level style guides should be complementary and nonconflicting with DoD HCI Interface and applicable commercial standards. The following domain-level style guide is mandated for HTML, Motif, and Windows-based systems:

- User Interface Specifications for the Defense Information Infrastructure (DII), Version 4.0, October 1999.

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 Motif-based system-level style guide will be created in accordance with the User Interface Specification for the DII.

The process of developing effective system-level style guidance and specifications is dependent upon a proper process for human systems integration engineering, as shown in Figure 5-1. ISO 13407, "Human-centred design processes for interactive systems," provides a flexible model for inclusion of critical human systems integration issues into the design process. Use of this process leads to interactive systems that are easier to use, requires lower training and support costs, as well as improve user satisfaction and productivity. The process includes active involvement of users to achieve clear understanding of user/task requirements, appropriate allocations of function between users and technologies, and allows for iterative/multi-disciplinary design solutions to achieve the systems' interoperability and cost goals.

The following standard is mandated:

- ISO 13407:1999(E), Human-centred design processes for interactive systems, June 1999.

5.2.3 Symbology

The following standard is mandated for the display of common warfighting symbology:

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

5.3 Emerging Standards

5.3.1 DoD HCI Style Guide

The DoD Human-Computer Interface Style Guide, dated 30 April 1996, is part of the TAFIM. The TAFIM has been officially withdrawn. The draft DoD HCI Style Guide, Version 4.0, dated 21

December 2000, is a stand-alone updated version, which will officially replace the TAFIM DoD HCI Style Guide when it is finally approved. The following standard is emerging:

– Draft DoD Human-Computer Interface Style Guide, Version 4.0, 21 December 2000.

5.3.2 Symbology

The Geospatial Symbols for Digital Displays (GeoSym) specification defines the format and content of symbol graphics and symbol assignment tables. GeoSym symbols were created for use with VPF products and are designed to complement Common Warfighting Symbology (MIL-STD-2525B). For nonwarfighting, geospatial symbology, the following standard is emerging:

– MIL-PRF-89045, DoD Performance Specification Geospatial Symbols for Digital Displays (GeoSym™), 20 February 1998.

Currently, research is underway to investigate nontraditional 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 includes 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. DoD will integrate standards for nontraditional user interfaces as research matures and commercial standards are developed.

Work to standardize data labeling for classified electronic and hardcopy documents is in progress. The results of this effort will replace the labeling standards currently appearing in Appendix A of the DoD HCI Style Guide, 30 April 1996.

Page intentionally left blank.

Section 6: Information Security Standards

6.1 Introduction

6.1.1 Purpose

This section provides the information security standards necessary to implement security at the required level of protection.

6.1.2 Scope

The standards mandated in this section apply to all DoD information technology systems. This section provides the security standards applicable to information processing, transfer, modeling, metadata, exchange, and Human-Computer Interfaces (HCI). This section also addresses standards for security audit and key management mechanisms. 6.2 addresses mandated security standards, and 6.3 addresses emerging security standards.

6.1.3 Background

Interoperability requires seamless information flow at all levels of information classification without compromising security. The goal is to protect information at multiple levels of security, recognizing that today's DoD systems are "islands" of system-high solutions.

The concept of security assurance provides confidence that the security features do what they are supposed to do, and that they do not do what they are not supposed to do. While assurance has been largely associated with product security, it is an equally important concept applied to system security since it is unlikely that integrated products will retain their individual assurance characteristics.

Systems that process sensitive data must be certified and accredited before use. Certification is the technical evaluation of security features and other safeguards, made in support of the accreditation. Accreditation is the authorization by the Designated Approving Authority (DAA) that an information system may be placed into operation. By authorizing a system to be placed into operation, the DAA is declaring that the system is operating under an "acceptable level of risk." Therefore, system developers should open dialog with the Certifier and DAA concurrently with their use of the Joint Technical Architecture (JTA), as DAA decisions can affect the applicability of standards within specific environments. The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) is defined in DODI 5200.40.

DoD systems should have adequate safeguards to enforce DoD security policies and system security procedures. System safeguards should provide adequate protection from user attempts to circumvent system access control, accountability, or procedures for the purpose of performing unauthorized system operations.

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 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.

The proper selection of standards can also provide a basis for improved information protection. Although few specific standards for the general topic of "information protection" exist within Defensive Information Warfare, selecting standards with security-relevant content contributes to the overall improvement of the security posture of information systems.

For more information on implementing information systems and networks to provide defense-in-depth, see the Information Assurance Technical Framework (IATF), available at <http://www.iatf.net>.

6.2 Mandated Standards

This subsection identifies the mandatory standards, profiles, and practices for information 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 IT 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 Introduction

This section contains the mandatory information security standards and protocols that shall be implemented in systems that have a need for the corresponding interoperability-related services. If a service is to be implemented, then it shall be implemented at the required level of protection using the associated security standards in this section. If a service is specified by more than one standard, the appropriate standard should be selected based on system requirements. 6.2 is structured to mirror the overall organization of the JTA so that readers can easily link security topics with the related subject area in the sections of the JTA (information processing; information transfer; information modeling, metadata, and information exchange; and human-computer interface) and their sub-sections.

6.2.2 Information Processing Security Standards

6.2.2.1 Application Software Entity Security Standards

If FORTEZZA services are used, the following standards are mandated:

- FORTEZZA Application Implementers' Guide, MD4002101-1.52, 5 March 1996.
- FORTEZZA Cryptologic Interface Programmers' Guide (CIPG), Revision 1.52, 30 January 1996.

6.2.2.2 Application Platform Entity Security Standards

For the application platform entity, security standards are mandated for authentication services. Security is an important part of other application platform service areas, but there are no standards for the other service areas.

6.2.2.2.1 Authentication Security Standards

Authentication supports tracing security-relevant events to individual users. If Open Software Foundation DCE Version 1.1 is used, the following authentication standard is mandated:

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

If DCE Version 1.1 is not used, the following authentication standard is mandated:

- FIPS PUB 112, Password Usage, 30 May 1985.

Additional guidance documents: NCSC-TG-017 – A Guide to Understanding Identification and Authentication in Trusted Systems: NCSC-STD-002 DoD Password Management Guidance.

6.2.3 Information Transfer Security Standards

This section discusses the security standards that shall be used when implementing information transfer security services. Security standards are mandated for the following information transfer areas: end-system (host standards) and network (internetworking standards).

6.2.3.1 End-System Security Standards

Security standards for host end-systems are included in the following subsections.

6.2.3.1.1 Host Security Standards

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 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.

6.2.3.1.1.1 Security Algorithms

To support interoperability using encrypted messages, products must share a common communication protocol. This protocol must include a common cryptographic message syntax, a common cryptographic algorithm, and a common mode of operation (e.g., cipher block chaining).

This section identifies security standards that shall be used for the indicated types of cryptographic algorithms: hashing, message digest, digital signatures, message encryption, and key exchange. If message digest or hash algorithms are required, Key Recovery will be implemented in a certificate management hierarchy. In FORTEZZA applications the following standards are mandated.

- FIPS PUB 180-1, Secure Hash Algorithm-1, 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, Key Exchange Algorithm (KEA), NSA, 12 July 1994.

Note: Both the Key Exchange Algorithm (KEA) and the SKIPJACK Algorithm (FIPS-185) were declassified on 23 June 1998.

6.2.3.1.1.2 Security Protocols

The following standard is mandated for DoD systems required to exchange security attributes; for example, sensitivity labels:

- MIL-STD-2045-48501, Common Security Label, 1 September 1996.

Establishment of a certificate and key management infrastructure for digital signature is required for the successful implementation of the security architecture. This infrastructure is responsible for the proper creation, distribution, and revocation of end-users' public-key certificates. The following standard is mandated:

- ITU-T Rec. X.509 (ISO/IEC 9594-8.2), Version 3, The Directory: Authentication Framework, 1997.

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 Allied Communications Publication 120, Common Security Protocol. The following messaging security protocol is mandated for DoD message systems required to exchange sensitive but unclassified and classified organizational messaging:

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

The following standard is mandated for individual messages that use digital certificates issued by the DoD PKI to protect sensitive but unclassified individual messaging (e-mail):

- IETF RFC 2311, S/MIME version 2, Message Specification, March 1998.

The following key management protocol is mandated:

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

6.2.3.2 Network Security Standards

Systems processing classified information must use Type 1 NSA-approved encryption products to provide both confidentiality and integrity security services within the network.

When network-layer security is required, the following security protocol is mandated:

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

The following standard is mandated for DoD systems required to exchange security attributes; for example, sensitivity labels:

- MIL-STD-2045-48501, Common Security Label, 1 September 1996.

6.2.3.3 Transmission Media Security Standards

There are currently no security standards mandated for transmission media.

6.2.4 Information Modeling, Metadata, and Information Exchange Security Standards

At this time, no information modeling, metadata, and information exchange standards are mandated. Process models and data models produced should be afforded the appropriate level of protection.

6.2.5 Human-Computer Interface Security Standards

At this time, no human-computer interface security standards are mandated.

6.2.6 Web Security Standards

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 is supporting TLS development, it is expected that there will be no further development of the SSL protocol by Netscape. The following standard is mandated:

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

6.3 Emerging Standards

The emerging standards listed in this subsection are expected to be elevated to mandatory status when implementations of the standards mature.

6.3.1 Introduction

The emerging security standards described in this section are drawn from work being pursued by ISO, IEEE, IETF, Federal standards bodies, and consortia such as the Object Management Group (OMG). 6.3 is structured to mirror the overall organization of the JTA so that readers can easily link security topics with the related subject area in the sections of the JTA (information processing; information transfer; information modeling, metadata, and information exchange; and human-computer interface) and their subsections.

6.3.2 Information Processing Security Standards

Information processing security standards are emerging in applications software and application platform entity areas.

6.3.2.1 Application Software Entity Security Standards

Emerging application software entity standards include Web security standards.

6.3.2.1.1 Web Security Standards

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.

6.3.2.2 Application Platform Entity Security Standards

For the application platform entity, security standards are emerging for software engineering, operating systems, and distributed computing services.

6.3.2.2.1 Software Engineering Services Security

For software engineering services, security standards are emerging for Generic Security Service (GSS)-Application Program Interface (API) and POSIX areas.

6.3.2.2.1.1 Generic Security Service-Application Program Interface Security

The Generic Security Service-Application Program Interface (GSS-API), as defined in RFC 1508, September 1993 (IETF), 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. RFC 1508 defines GSS-API services and primitives at a level independent of an underlying mechanism and programming language environment. RFC 2743, "GSS-API, Version 2.0," J. Linn, Update 1 January 2000, revises RFC 1508, making specific, incremental changes in response to implementation experience and liaison requests. The following standard is emerging:

- IETF RFC 2743, Generic Security Service Application Program Interface, Version 2, Update 1 January 2000.

The IETF, "Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)," C. Adams, December 1998, extends the GSS-API (RFC 1508) for non-session protocols and applications requiring protection of a generic data unit (such as a file or message) 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 in which data needs to be protected without any online 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 days or years later. The following standard is emerging:

- IETF RFC 2479, Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API), December 1998.

6.3.2.2.2 Operating System Services Security

Operating system services security standards are emerging in the following areas: evaluation criteria and authentication.

6.3.2.2.2.1 Evaluation Criteria Security Standards

See 6.2 for a description of the Common Criteria. More information on Common Criteria Protection Profiles is available on NIST's Web home page.

For the application platform entity, the following standards are considered emerging for the acquisition of operating systems consistent with the required level of trust:

- For Basic Robustness/C2 systems: Controlled Access Protection Profile, Version 1.d, NSA 8 October 1999.

– For Medium Robustness/B1 systems: Labeled Security Protection Profile, Version 1.b, NSA 8 October 1999.

6.3.2.2.2.2 Authentication Security Standards

IETF RFC 2289, "A One-Time Password System," February 1998, 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 released by Bellcore. The following standard is emerging:

– IETF RFC 2289, A One-Time Password System, February 1998.

When Remote Dial-In Authentication is required, the following standard is emerging:

– IETF RFC 2138, Remote Authentication Dial In User Service (RADIUS), April 1997.

6.3.2.2.3 Distributed Computing Services Security Standards

Distributed Computing Environment (DCE) Authentication and Security Specification C311, August 1997, is a draft Open Group Specification for DCE.

The Common Object Request Broker Architecture (CORBA) Security Services define a software infrastructure that supports access control, authorization, authentication, auditing, delegation, non-repudiation, and security administration for distributed-object-based systems. This infrastructure can be based on existing security environments and can be used with existing permission mechanisms and login facilities. The key security functionality is confined to a trusted core that enforces the essential security policy elements. Since the CORBA Security Services are intended to be flexible, two levels of conformance may be provided. Level 1 provides support for a default system security policy covering access control and auditing. Level 1 is intended to support applications that do not have a default policy. Level 2 provides the capability for applications to control the security provided at object invocation and also for applications to control the administration of an application-specific security policy. Level 2 is intended to support multiple security policies and to provide the capability to select separate access control and audit policies. The following standards are emerging:

– C311, DCE Authentication and Security Specification, August 1997.
– OMG document formal/2000-06-25, Security Services Specification, Version 1.5, May 2000.

6.3.3 Information Transfer Security Standards

Security standards are emerging for the following information transfer areas: end-systems (host standards) and network (internetworking standards).

6.3.3.1 End-System Security Standards

Emerging end-system security standards include host standards discussed in the following subsection.

6.3.3.1.1 Host Security Standards

Emerging security standards for host end-systems in security protocols are discussed in the following subsection.

6.3.3.1.1.1 Security Protocols

In mid-1996, some significant improvements were proposed to the Secure/Multipurpose Internet Mail Extensions (S/MIME) messaging security protocol and the underlying encapsulation protocol, PKCS#7. With these improvements, S/MIME will provide a business-quality security protocol for both

the Internet and X.400 messaging environments. The improvements include: (1) algorithm independence, (2) support for digitally signed receipts, (3) support for mail lists, and (4) support for sensitivity labels in signed and unsigned/encrypted messages. This effectively merges S/MIME and Message Security Protocol (MSP) 4.0/ACP-120. In November 1997, the IETF formed the S/MIME security protocol working group to create Internet standards based on S/MIME and these improvements. The following is an emerging standard:

– IETF RFC 2633, S/MIME Version 3, Message Specification, June 1999.

It is expected that the Trusted Systems Interoperability Group (TSIG), Trusted Information for Exchange for Restricted Environments (TSIX (RE) 1.1) will adopt MIL-STD-2045-48501 as a replacement for its Common Internet Protocol Security Options (CIPSO) labeling standard.

The following IEEE-approved standard for Local Area Network (LAN) security and Metropolitan Area Network (MAN) security is emerging:

– IEEE 802.10, Standard for Interoperable LAN/MAN Security (SILS) 1998, Key Management (Clause 3, IEEE 802.10c-1998 (supplement), Architecture (Clause 1.4) (supplement).

This IEEE standard provides specifications for security association management (Manual, Key Distribution Center, and Certification-based), security labeling and security services including data confidentiality, connectionless integrity, data origin authentication and access control. The Key Management Protocol (KMP) defined in Clause 3 is applicable to the Secure Data Exchange (SDE) protocol contained in the standards as well as other security protocols.

6.3.3.1.1.2 Medium-Assurance Public-Key Infrastructure Security Standards

6.3.3.1.1.2.1 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>.

6.3.3.1.1.2.2 Certificate Profiles

The DoD medium-assurance certificate profile implements the Federal PKI certificate profile, which in turn implements the Internet Engineering Task Force (IETF) profile, which in turn implements the ITU-T X.509 profile. Emerging certificate profile standards are:

- ITU-T X.509, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997, as profiled by: IETF RFC 2459.
- IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999, as profiled by TWG-98-07.
- TWG-98-07, Federal PKI X.509 Certificate and CRL Extensions Profile, 9 March 1998, as profiled by DoD Certificate Profile, as defined in X.509 Certificate Policy for the United States Department of Defense, Version 1.5, 13 December 1999.

6.3.3.1.1.2.3 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 standards are emerging:

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

– RSA Laboratories Public Key Cryptography Standard (PKCS) #15, Cryptographic Token Information Format Standard, version 1.0, 23 April 1999.

6.3.3.1.1.2.4 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, Informational RFC.
– IETF RFC 2314, PKCS #10, Certification Request Syntax, Version 1.5, March 1998, Informational RFC.

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.

6.3.3.1.1.2.5 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.

6.3.3.1.1.2.6 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, 8 January 1999. (This replaces DES with Triple DES, as specified in ANSI X9.52).

The following standard is emerging for PKI Class 3 implementations:

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

The following standard is emerging for encryption of sensitive but unclassified (SBU) data:

– AES Proposal: Rijndael by Joan Daemen and Vincent Rijmen, 9 March 1999, Version 2.

6.3.3.2 Network Security Standards

Emerging network standards are listed in 6.3.3.2.1.

6.3.3.2.1 Internetworking 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)," November 1998, S. Kent and R. Atkinson, 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. 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.

Draft FIPS 46-3 Data Encryption Standard (DES). 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 draft FIPS 46-3 Data Encryption Standard. IETF RFC 2420. The PPP Triple-DES Encryption Protocol (3DESE) is a complement to FIPS 46-3.

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).

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.
- Draft FIPS 46-3, Data Encryption Standard (DES).
- IETF RFC 2420, The PPP Triple-DES Encryption Protocol (3DESE) as a complement to FIPS 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.

The following IEEE-approved standard for Local Area Network (LAN) security and Metropolitan Area Network is emerging:

- IEEE 802.10, IEEE Standard for Interoperable LAN/MAN Security (SILS), 1998; Key Management (Clause 3), IEEE 802.10c-1998 (Supplement) and Security Architecture Framework (Clause 1), IEEE Std. 802.10a-1999 (Supplement).

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.

Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network. The following standard is emerging for securing specific terminal and X-Windows sessions:

- Draft-IETF-secsh-architecture-05.txt, Secure Shell (SSH) Protocol Architecture, May 2000.

6.3.3.2.2 Firewall Standards

The following emerging standards will apply to Firewall devices in Basic Robustness environments:

- U.S. Government Traffic Filtering Firewall for Low Risk Environments, Version 1.1, April 1999.
- U.S. Government Application-level Firewall Protection Profile for Low Risk Environments, July 20, 1999.

The following emerging standards will apply to Firewall devices in Medium Robustness environments:

- U.S. DoD Traffic Filtering Firewall For Medium Robustness, Version 1.0, 26 January 2000.
- U.S. DoD Application-level Firewall for Medium Robustness Environments, Version 1.0, 7 February 2000.

6.3.3.2.3 Virtual Private Network (VPN)

The following standard is emerging for VPN devices:

- Virtual Private Network Protection Profile for Protecting Sensitive Information, Version 1.0, 26 February 2000.

6.3.3.2.4 Intrusion Detection Systems

The following standards are emerging for Intrusion Detection devices:

- Intrusion Detection System Analyzer Protection Profile, 30 December 1999.
- Intrusion Detection System Sensor Protection Profile, 30 December 1999.
- Intrusion Detection System Scanner Protection Profile, 4 January 2000.

6.3.4 Information Modeling, Metadata, and Information Exchange Security Standards

There are no emerging standards in this area at this time.

6.3.5 Human-Computer Interface Security Standards

Refer to 6.3.3.1.1.2 for information pertaining to Medium-Assurance Public-Key Infrastructure Security Standards.

C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance Domain

C4ISR.1 Domain Overview

C4ISR.1.1 Purpose

The C4ISR Domain identifies elements (i.e., standards, interfaces, and service areas) specific to the functional areas of command, control, communications, computers, intelligence, surveillance, and reconnaissance that are additions to those standards listed in the JTA Core. These additions are common to the majority of C4ISR systems and support the functional requirements of C4ISR systems.

C4ISR.1.2 Background

The scope and elements listed in JTA Version 1.0 focused on C4I. Version 2.0 expanded the scope to include the areas of C4ISR, Modeling and Simulation, Weapon Systems, and Combat Support. The sections describing these areas are referred to as domain annexes.

C4ISR.1.3 Domain Description

The C4ISR 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:

- Support properly designated commanders in the exercise of authority and direction over assigned and attached forces across the range of military operations.
- Collect, process, integrate, analyze, evaluate, or interpret available information concerning foreign countries or areas.
- Systematically observe aerospace, surface or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means.
- Obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.

This will specifically address the information technology (IT) aspect of the C4ISR Domain. It should be noted that this does not include those systems or other IT components specifically identified as belonging to the Combat Support Domain or whose primary function is the support of day-to-day administrative or support operations at fixed-base locations. Examples of such systems include acquisition, finance, human resources, legal, logistics, and medical systems, and items such as general-purpose LANs, computer hardware and software, telephone switches, transmission equipment, and outside cable plant. The position of the C4ISR Domain in the JTA Hierarchy Model is shown in Figure C4ISR-1.

C4ISR.1.4 Scope And Applicability

The elements listed in this domain are mandated for use on all emerging systems or upgrades to existing systems developed to meet the functional area of C4ISR. Users of this document are encouraged to review other domain annexes to better gauge which domain is applicable.

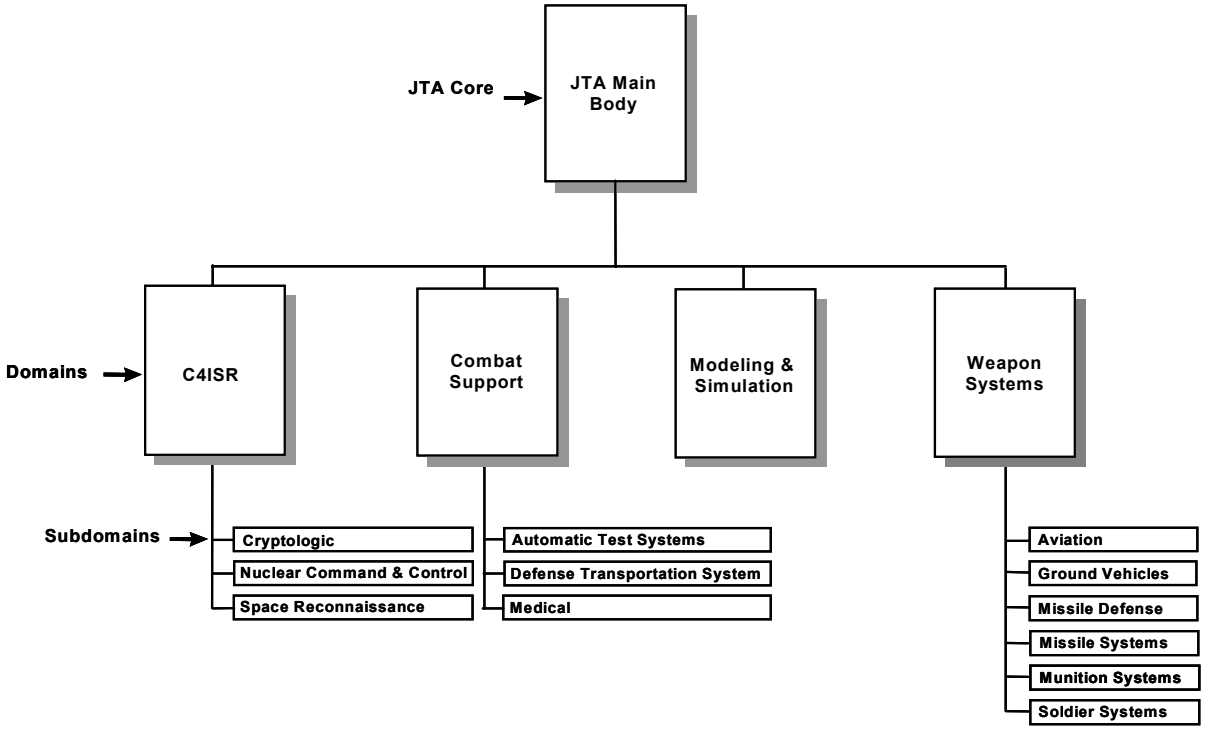


Figure C4ISR-1: JTA Hierarchy Model

C4ISR.1.5 Technical Reference Model

This domain uses the DoD Technical Reference Model cited in 1.5 of the JTA as its framework. Additional service areas required to support the C4ISR Domain are addressed in C4ISR.3, Domain-Specific Service Areas.

C4ISR.1.6 Domain Organization

The C4ISR Domain consists of three sections. C4ISR.1 contains the overview, C4ISR.2 contains Information Technology standards that are additions to those contained in the JTA Core, and C4ISR.3 is reserved for those elements that are domain-specific because they do not map directly to the JTA Core service areas.

C4ISR.2 Additions to the JTA Core

C4ISR.2.1 Introduction

The following sections map to the service areas of the main body of the JTA. They identify standards, profiles, and practices that are applicable to the C4ISR Domain, but have not yet been selected for inclusion in the JTA Core.

C4ISR.2.2 Information Processing Standards

C4ISR.2.2.1 Introduction

The information processing standards and profiles described in this section promote seamless interoperability for C4ISR systems through the use of standardized interfaces for application platforms and software.

C4ISR.2.2.2 Mandated Standards

The following sections identify the mandatory standards, profiles, and practices for information processing that shall be used in the development and acquisition of C4ISR systems. These are in addition to those listed in the Core, which are mandated for all systems that utilize information technology.

C4ISR.2.2.2.1 Still Imagery Data Interchange

The National Imagery Transmission Format Standard (NITFS) allows for Support Data Extensions (SDEs), which are a collection of data fields that provide space within the NITF file structure for adding functionality. Documented and controlled separately from the NITFS suite of standards, SDEs extend NITF functionality with minimal impact on the underlying standard document. SDEs may be incorporated into an NITF file while maintaining backward compatibility because the identifier and byte count mechanisms allow applications developed prior to the addition of newly defined data to skip over extension fields they are not designed to interpret.

Imagery Chip, Version B (ICHIPB) is a system-independent NITF SDE that, when included with NITF image chips, will support mensuration of non-dewarped imagery. This NITF SDE holds the support data analysts need when using imagery software to mensurate or determine detailed geospatial parameters on pixel-based features within image chips. There is no mechanism in the standard NITF format to pass a standardized set of data with an image chip such that a user can easily apply imagery software to that image. The following standard is mandated for NITF systems that use National Technical Means (NTM), Tactical/Airborne imagery, or Commercial Satellite imagery:

- STDI0002, 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.

The Profile for Imagery Access Extensions (PIAE) SDE is designed to provide an area to place fields not available in the NITF but which were documented in the canceled Standards Profile for Imagery Access (SPIA). The PIAE was developed to align the SPIA and NITF for product information and adds descriptive detail associated with products. The following standard is mandated for NITF systems that use imagery from National Technical Means (NTM), Tactical/Airborne imagery, or Commercial Satellite imagery:

- STDI0002, 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.

The Airborne SDE supersedes the VIMAS SDE and SAR SDEs described in version 1.0 of the NITFS Compendium of Controlled Extensions. The Airborne SDE incorporates all NITF tagged records relevant to SAR, Electro-Optical, Multispectral, and Hyperspectral primary imagery. Systems that use NITF imagery from airborne sensors shall be designed to extract data from the records described in this SDE. The following standard is mandated for NITF systems that exploit Tactical/Airborne imagery:

- STDI0002, 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.

The History Tag, Version A (HISTOA) Softcopy History Tag, provides a history of any softcopy-processing actions applied to an NITF image. These extensions describe the format for support information within an NITF file containing National System Imagery. The following standard is mandated for NITF systems that exploit NTM:

- STDI0002, 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.

C4ISR.2.2.3 Emerging Standards

The Air Group IV/SIAR Working Group under the NATO Air Force Armaments Group (NAFAG) has developed NATO Secondary Imagery Format (NSIF) STANAG 4545. The aim of this agreement is to achieve interoperability for transmission of Electronic Secondary Imagery among NATO C3I Systems. This STANAG was developed in cognizance with the International Organization for Standardization (ISO) Basic Imagery Interchange Format (BIIF) and the US MIL-STD-2500B on National Imagery Transmission Format (NITF). The following standard is emerging:

– STANAG 4545, NATO Secondary Imagery Format (NSIF), 27 November 1998.

C4ISR.2.2.3.1 Common Ground Moving Target Indicator Data Format

The Common Ground Moving Target Indicator (CGMTI) Data Format is emerging as a de facto U.S./NATO data format for the dissemination of GMTI imagery from airborne and spaceborne GMTI sensor platforms. It is being developed as a product of the CGMTI Format Working Group, which was established to define and develop a standard that facilitates the transmission, processing, fusion, and display of GMTI data. Details of the Working Group are available at the CGMTI Web site, URL <http://www.rl.af.mil/programs/cgmti/>.The following document is identified as an emerging standard for systems that disseminate GMTI data:

– Common Ground Moving Target Indicator (CGMTI), Data Format Document, DRAFT Version 1.01d2, 25 July 2000.

C4ISR.2.3 Information Transfer Standards

C4ISR.2.3.1 Introduction

The information transfer standards and profiles described in this section promote seamless communications and information transfer interoperability for C4ISR systems through the use of standardized interfaces for end-systems, networks, transmission media, and systems management.

C4ISR.2.3.2 Mandated Standards

The following sections identify the mandatory standards, profiles, and practices for information transfer that shall be used in the development and acquisition of C4ISR systems. These are in addition to those listed in the Core, which are mandated for all systems that utilize information technology.

C4ISR.2.3.2.1 Transmission Media

Transmission media refers to the physical paths used to transfer information among Components within the same system or among different systems.

C4ISR.2.3.2.1.1 Radio Communications

This section addresses standards that facilitate the interoperability of C4ISR systems that utilize the portion of the electromagnetic spectrum below 300 GHz for wireless communication.

C4ISR.2.3.2.1.1.1 Common Data Link Standards

The Common Data Link (CDL) is a flexible, multipurpose radio link-based digital communication technology developed by the Government for use in imagery and signals intelligence collection systems. It provides standard waveforms that follow a line-of-sight microwave path (link) and allows both full-duplex and simplex communications between airborne/space-based platforms and surface-based terminals. The CDL system supports air-to-land/sea surface, and air-to-satellite (relay/beyond line-of-sight) communications modes.

The term CDL refers to a family of interoperable data link implementations that offer alternate levels of capabilities for different applications/platforms. Five classes (Class I through Class V) of CDL have been defined. The Class I CDL standard addresses land/sea surface terminals that provide remote operation of airborne platforms operating up to 80,000 feet at mach 2.3 or less. The current land-based implementation of Class I CDL is the Miniature Interoperable Surface Terminal (MIST). The current sea-based implementation of Class I CDL is the Common High Bandwidth Data Link Surface Terminal (CHBDL-ST). Classes II through V cover the remainder of the defined CDL systems and are based on maximum altitude ceilings and sometimes platform mach number: Class II to 150,000 feet at mach 5 or less; Class III to 500,000 feet; Class IV to 750 nautical miles and is part of a satellite; lastly Class V that operates above 750 nautical miles and is part of a relay satellite. The majority of DoD CDL interoperability and standardization efforts have been focused on the Class I line-of-sight CDL system specification.

The Office of the Assistant Secretary of Defense for C3I (OASD[C3I]) designated CDL as the DoD standard in a policy memorandum (OASD/C3I Common Data Link Policy Memorandum, 13 December 1991). A similar policy memorandum was released to mandate the use of the Tactical CDL (OASD[C3I] Tactical Data Link Policy Memorandum, 18 October 1994). The following mandated standards apply for unified configuration control and standardized communications paths between airborne reconnaissance platforms that contain multiple sensors:

- System Specification for the CDL Segment, Specification 7681990, Revision D, 29 January 1997.
- System Description Document for CDL, Specification 7681996, 5 May 1993.

C4ISR.2.3.2.1.1.2 Unattended MASINT Sensor Communication Standards

Unattended Measurement and Signature Intelligence (MASINT) Sensors (UMSs) are small, autonomously powered, disposable systems that can be deployed by airborne platforms or ground personnel. UMS can contain one or more types of sensors (seismic, acoustic, IR, magnetic, chemical, or radiological) that transmit alarm messages or data when triggered by enemy activity. The SEIWG-005 standard specifies the frequencies, data formats, and protocols for this class of sensors in order to relay the data back via communication links and data relays, to a common exploitation station. The following standard is mandated for use in UMS systems:

- Interface Specification, Radio Frequency Transmission Interfaces for DoD Physical Security Systems, SEIWG-005, 15 December 1981.

C4ISR.2.3.3 Emerging Standards

The Program Management Office for Night Vision/Reconnaissance and Target Acquisition (PM NV/RSTA) has developed the Sensor Link Protocol (SLP) for use as a common local network interface between RSTA sensor systems and a host computer system. It is anticipated that SLP will evolve to provide a stable sensor interface baseline within the Intelligence and Electronic Warfare (I/EW) community. The following standard is emerging:

– ICD-SLP-200, September 14, 1998. Interface Control Document (ICD) Title: Sensor Link Protocol.

C4ISR.2.4 Information Modeling, Metadata and Information Exchange Standards

C4ISR.2.4.1 Introduction

The information modeling, metadata, and information exchange standards and profiles described in this section facilitate interoperability between C4ISR systems through the use of standardized activity models, data models, data definitions, and formatted messages.

C4ISR.2.4.2 Mandated Standards

The following sections identify the mandatory standards, profiles, and practices for information modeling, metadata, and information exchange that shall be used in the development and acquisition of C4ISR systems. These are in addition to those listed in the, which are mandated for all systems that utilize information technology.

C4ISR.2.4.2.1 Information Exchange Standards

Information Exchange refers to the exchange of information among mission-area applications within the same system or among different systems.

C4ISR.2.4.2.1.1 Target/Threat Data Interchange Standards

The National Target/Threat Signature Data System (NTSDS) has been designated as a migration system, in accordance with guidance from ASD (C3I) and by the Intelligence Systems Board (ISB). NTSDS provides the DoD signature data community (e.g., ISR and MASINT) signature data from multiple, geographically distributed sites via a unified national system. NTSDS Data Centers employ standard data parameters and formats for stored target signatures for national and DoD customers. The following data standards are mandated for the DoD signature data community when interchanging national target/threat data:

- NTSDS Database Implementation Description & Core Schema Definition, Version 1.2a, 19 September 1997.
- NTSDS Supplemental Schema Definition, Version 1.1, 24 September 1997.

C4ISR.2.4.3 Emerging Standards

There are currently no emerging standards identified for this service area of the C4ISR Domain.

C4ISR.2.5 Human-Computer Interface Standards

C4ISR.2.5.1 Introduction

The human-computer interface standards and profiles described in this section facilitate interoperability between C4ISR systems through the use of standardized user interfaces, style guides, and symbology.

C4ISR.2.5.2 Mandated Standards

There are currently no mandated standards identified in this service area of the C4ISR Domain.

C4ISR.2.5.3 Emerging Standards

There are currently no emerging standards identified in this service area of the C4ISR Domain.

C4ISR.2.6 Information Security Standards

C4ISR.2.6.1 Introduction

The information security standards and profiles described in this section facilitate interoperability between C4ISR systems through the use of standardized security interfaces for systems that process, transport, model, or exchange information.

C4ISR.2.6.2 Mandated Standards

There are currently no mandated standards identified in this service area of the C4ISR Domain.

C4ISR.2.6.3 Emerging Standards

There are currently no emerging standards identified in this service area of the C4ISR Domain.

C4ISR.3 Domain-Specific Service Areas

C4ISR.3.1 Introduction

The following sections map to service areas that apply to the C4ISR Domain, but not to the JTA Core. The standards, profiles, and practices identified are applicable only in the context of these service areas.

C4ISR.3.2 Payload-Platform Interface

C4ISR.3.2.1 Introduction

The interface standards identified in this section address interoperability requirements for the integration of a C4ISR payload (e.g., sensor package, communications relay) into a manned or unmanned aerospace platform. It is recognized that vehicle interface characteristics are often driven by the requirements of legacy technologies or other onboard systems. In these cases, the JTA rule set described in Section 1 of the JTA Core, and as interpreted by individual Service/Agency JTA Implementation Plans, should be used to determine mandate applicability.

C4ISR.3.2.2 Mandated Standards

The following sections identify the mandatory standards, profiles, and practices for the integration of a C4ISR payload into a manned or unmanned aerospace platform. It should be noted that the standards in this section apply to the platform only to the extent to which they directly affect the interoperability of onboard C4ISR systems.

At the present time, these mandates apply only to airborne reconnaissance systems.

C4ISR.3.2.2.1 Internal Communications

Internal communications provide information transfer capabilities between the platform and the onboard C4ISR systems, subsystems, and components. This section identifies the standards necessary to facilitate interoperability within and between these entities.

C4ISR.3.2.2.1.1 Fibre Channel

Fibre Channel is an efficient, high-speed, serial data communication technology for use in many environments including near-real-time high-speed data transfer, and local/campus networking environments. The Fibre Channel Physical and Signaling standards pertain to first three layers of the Fibre Channel stack (FC0, FC1, and FC2). FC0 addresses the physical media, FC1 discusses the data-encoding scheme, and FC2 addresses the framing protocol and flow control. The media chosen for Fibre Channel can accommodate speeds of 133, 266, and 531 Mbps and 1.06, 2.12, and 4.25 Gbps. The following standard is mandated for network communications internal to airborne reconnaissance platforms where Fibre Channel is used:

- ANSI X3.230-1994/AM 2-1996, Information Technology – Fibre Channel – Physical and Signaling Interface (FC-PH), with amendments, 24 May 1999.

C4ISR.3.2.2.1.2 FireWire

FireWire describes a serial bus that provides the same services as modern IEEE-standard parallel buses. It has a 64-bit address space, control registers, and a read/write/lock operations set that conforms to IEEE Std 1212-1991, Command and Status Register (CSR). The following standard is mandated for serial bus communications internal to airborne reconnaissance platforms where FireWire is used:

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

C4ISR.3.2.2.2 Vehicle/Sensor Telemetry

Commands to various SIGINT, IMINT, and MASINT front-end equipment flow through airborne telemetry systems to onboard LANs. Sensor commands and acknowledgments may include position changes, mode changes, fault isolation commands, and others. The following telemetry standard is mandated for airborne reconnaissance systems:

- Telemetry Group, Range Commanders Council, Telemetry Standards, IRIG 106-96, Secretariat, Range Commanders Council, U.S. Army White Sands Missile Range, New Mexico, Chapter 4, Pulse Coded Modulation Standards, Chapter 8 - MIL-STD-1553 Department of Defense Interface Standard for Digital Time Division Command/Response Multiplex Data Bus, 21 March 1996.

C4ISR.3.2.2.3 Mission Recorder

Mission recorders are used to capture the raw, pre-processed sensor data together with associated navigation, timing, and ancillary data. Additionally, a computer-controlled interface for basic recorder functions such as start, stop, shuttle, fast-forward, and rewind is included.

In conjunction with recording the raw sensor data, timing data will be recorded (on a separate track) in accordance with the standards defined below. The DCRSi 240 rack mount and modular ruggedized systems are one inch, transverse scan, rotary digital recorders capable of recording and reproducing at any user data rate from 0 to 30 Mbytes/s (0-240 Mbps). Specific compatibility information on the DCRSi 240 recorder can be found in the published AMPEX Digital Instrumentation Recorder DCRSi 240 User Manual. The ANSI digital recording standard, providing data compatibility and tape interchangeability, is provided by the X3.175 series. The Instrumentation Group IRIG-B standard was written specifically for analog magnetic tape storage. In conjunction with the migration to all digital systems, mission-recorder standards will be re-evaluated to emphasize digital and de-emphasize analog.

C4ISR.3.2.3 Emerging Standards

There are currently no emerging standards identified in this service area of the C4ISR Domain.

C4ISR.CRY: Cryptologic Subdomain

C4ISR.CRY.1 Subdomain Overview

The Cryptologic Subdomain supports the objectives that provide the framework for meeting the Cryptologic community's requirements.[1] First, the Cryptologic Subdomain provides the foundation for interoperability and the seamless flow of information between and among all cryptologic systems and the associated service components in a collaborative and secure environment. Second, it establishes the minimum set of standards and technical guidelines for development and acquisition of new, upgraded, and demonstration systems necessary to achieve interoperability as well as reductions in costs and fielding times. Finally, it promotes interoperability with other components of the Intelligence Community (IC).

C4ISR.CRY.1.1 Purpose

The Cryptologic Subdomain mandates the minimum set of standards and guidelines for cryptologic systems and subsystems. This includes National and Tactical Cryptologic systems and subsystems. The provides the technical foundation for migrating United States Cryptologic System (USCS) systems toward a common Unified Cryptologic System architecture as directed by the Director, NSA (DIRNSA) and the Director, Central Intelligence (DCI).

C4ISR.CRY.1.2 Background

Faced with the challenges of keeping pace with changing intelligence requirements, budgetary uncertainty, and technological revolutions, the Director, National Security Agency, under the auspices of the Deputy Secretary of Defense and the Director, Central Intelligence, commissioned the Unified Cryptologic Architecture (UCA) study. The primary goal of the UCA study was to provide an architecture that would ensure an interoperable and secure USCS by 2010. The result of this study was the introduction of the UCA Operational, Systems, and Technical Architectures. The UCA Technical Architecture (UCA-TA) is complementary to the JTA and will be used in conjunction with the JTA Core and the JTA C4ISR Domain by all members of the Cryptologic community.

C4ISR.CRY.1.3 Subdomain Description

The Cryptologic Subdomain mandates standards for the Cryptologic community. The objective is to facilitate the exchange and exploitation of cryptologic data across the IC and the Department of Defense (DoD).

C4ISR.CRY.1.4 Scope

The scope of this includes the service areas of the JTA Core and C4ISR Domain, (Information Processing, Information Transfer, Information Modeling, Metadata and Information Exchange, human-computer Interface and Information Security Standards). This also addresses additional areas unique to the Cryptologic community including Special-Purpose Devices, backplanes, and circuit cards.

---

[1] Cryptologic Community defines entities composed of the NSA, elements of the military departments and the CIA performing SIGINT activities, and elements of an other department or agency of the Federal Government that may, from time to time, be so authorized, and the Information Systems Security activities that protect these SIGINT activities. SIGINT is defined as intelligence information comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted.

C4ISR.CRY.1.5 Applicability

This subdomain applies to all National and Tactical cryptologic systems, subsystems, and demonstration systems. It applies to all new acquisitions and upgrades to existing systems and subsystems that perform SIGINT and/or SIGINT-related activities. A cryptologic system is defined as any system within DoD that collects, processes, and/or manages SIGINT.

C4ISR.CRY.1.6 Subdomain Organization

The subdomain is divided into three sections. Section 1 contains the overview. This section defines the purpose and scope of the annex and provides background information. Section 2 contains standards for the Cryptologic community that are in addition to the standards in the JTA Core and the C4ISR domain service areas. Section 3 contains services and interfaces unique to the Cryptologic community.

C4ISR.CRY.2 Standards in Addition to the JTA Core and C4ISR Domain

C4ISR.CRY.2.1 Introduction

This part of the Cryptologic Subdomain establishes the minimum set of rules governing the information technology for cryptologic systems. The scope includes standards for information processing; information transfer; information modeling, metadata, and information exchange; information security; and human-computer interface.

C4ISR.CRY.2.2 Information Processing Standards

C4ISR.CRY.2.2.1 Introduction

The information processing standards and profiles described in this section promote seamless interoperability for cryptologic systems through the use of standardized interfaces for application platforms and software.

C4ISR.CRY.2.2.2 Mandated Standards

There are no additional mandated standards in this section.

C4ISR.CRY.2.2.3 Emerging Standards

There are no emerging standards in this section.

C4ISR.CRY.2.3 Information Transfer Standards

C4ISR.CRY.2.3.1 Introduction

The information transfer standards and profiles described in this section promote seamless communications and Information Transfer interoperability for cryptologic systems through the use of standardized interfaces for end-systems, networks, transmission media, and systems management.

C4ISR.CRY.2.3.2 Mandated Standards

There are no additional mandated standards in this section.

C4ISR.CRY.2.3.3 Emerging Standards

There are no emerging standards in this section.

C4ISR.CRY.2.4 Information Modeling, Metadata, and Information Exchange Standards

C4ISR.CRY.2.4.1 Introduction

The information modeling, metadata, and information exchange standards and profiles described in this section facilitate interoperability between cryptologic systems through the use of standardized activity models, data models, data definitions, and formatted messages.

C4ISR.CRY.2.4.2 Mandated Standards

There are no additional mandated standards in this section.

C4ISR.CRY.2.4.3 Emerging Standards

There are no emerging standards in this section.

C4ISR.CRY.2.5 Human-Computer Interface Standards

C4ISR.CRY.2.5.1 Introduction

The human-computer interface standards and profiles described in this section facilitate interoperability between cryptologic systems through the use of standardized user interfaces, style guides, and symbology.

C4ISR.CRY.2.5.2 Mandated Standards

There are no additional mandated standards in this section.

C4ISR.CRY.2.5.3 Emerging Standards

There are no emerging standards in this section.

C4ISR.CRY.2.6 Information Security Standards

C4ISR.CRY.2.6.1 Introduction

The information security standards and profiles described in this section facilitate interoperability between cryptologic systems through the use of standardized security interfaces for systems that process, transport, model, or exchange information.

C4ISR.CRY.2.6.2 Mandated Standards

There are no additional mandated standards in this section.

C4ISR.CRY.2.6.3 Emerging Standards

There are no emerging standards in this section.

C4ISR.CRY.3 Subdomain-Specific Services and Interfaces

C4ISR.CRY.3.1 Introduction

Some cryptologic processing is performed using special-purpose devices (SPDs) that may be embedded within larger host systems or remotely located devices. Cryptologic systems encompass both real-time and non-real-time SPDs. The communications processing, signal processing, and mathematical analysis are performed in real-time by embedded systems that require speeds at least three orders of magnitude higher than traditional C4I systems. Real-time systems also require deterministic scheduling and robust fault tolerance.

C4ISR.CRY.3.2 Mandated Standards

C4ISR.CRY.3.2.1 Small-Scale Special-Purpose Devices

A Small-Scale Special-Purpose Device (SPD) consists of one or more special-purpose boards (may be Government-developed) hosted by a DII COE-compliant computer. These boards use Application Specific Integrated Circuits (ASICs) and Programmable Logic Devices (PLDs) typically designed and developed for the cryptologic community.

Cryptologic systems using PCI cards shall comply with the following mandated standard:

- Peripheral Component Interconnect (PCI) Standard, Version 2.2, 1999.

Cryptologic systems using PCMCIA cards shall comply with the following mandated standard:

- PC Card Standard, Release 7.0, March 1997 (The PC Card standard is a Personal Computer Memory Card International Association (PCMCIA) standards body and trade association standard).

C4ISR.CRY.3.2.2 Backplanes and Circuit Cards

To keep pace with a dynamic threat environment, Cryptologic systems often require the ability to quickly insert new technology. Standards for backplanes and circuit cards facilitate interoperability and modernization and can provide a “plug and play” capability.

Cryptologic systems using VME backplanes and circuit cards shall comply with the following mandated standard:

- ANSI/VITA 1-1994, American National Standard for VME64.

Cryptologic systems using VXI backplanes and circuit cards shall comply with the following mandated standard:

- IEEE 1155-1992, IEEE Standard for VMEbus Extensions for Instrumentation (VXI).

C4ISR.CRY.3.2.3 Conduction Cooling

Cryptologic systems that require conduction cooling of circuit cards shall comply with the following mandated standard:

- IEEE 1101.2-1992, IEEE Standard for Mechanical Core Specifications for Conduction Cooled Eurocards.

C4ISR.CRY.3.3 Emerging Standards

C4ISR.CRY.3.3.1 Backplanes and Circuit Cards

CompactPCI (cPCI) is a competing bus standard that uses the same form factor as VME and the protocols of the much smaller PCI standard, which is emerging.

  – CompactPCI (cPCI), Version 1.0, 1996.

C4ISR.NCC: Nuclear Command and Control Subdomain

C4ISR.NCC.1 Subdomain Overview

C4ISR.NCC.1.1 Purpose

The Nuclear Command and Control (NCC) Subdomain identifies elements (i.e., standards, interfaces, and service areas) specific to the functional areas of nuclear command and control that are additions to those standards listed in the JTA Core and in the C4ISR Domain. These additions support the functional requirements of nuclear command and control (C^2) systems.

C4ISR.NCC.1.2 Background

This NCC Subdomain to the Joint Technical Architecture (JTA) has been developed to provide standards for programs being developed or maintained by USAF/AFMC/ESC/ND.

C4ISR.NCC.1.3 Subdomain Description

The NCC Subdomain to the JTA mandates the minimum set of standards and guidelines for nuclear C^2 systems.

C4ISR.NCC.1.4 Scope and Applicability

This part of the C4ISR Domain establishes the minimum set of rules governing information technology within nuclear command and control systems. The scope includes standards for information processing; information transfer; information modeling, metadata, and information exchange; human-computer interface; and information security.

The Nuclear Command and Control Subdomain constitutes only a part of the larger command and control part of C4ISR. As such, this subdomain does not cover technical architecture details for any part of the C4ISR spectrum other than the nuclear C^2 portion. Nuclear C^2 can use a variety of strategic and tactical C^2 systems, but the standards listed in this subdomain apply to these systems when used for nuclear C^2 missions. This annex covers nuclear C^2 from the JCS and nuclear CINC down to the last human in the loop prior to the nuclear weapon. The scope of this subdomain ***excludes*** the following:

- Nuclear (and non-nuclear) weapon systems.
- Munition-specific communications links (e.g., links between a Launch Control Center and a missile silo).
- Integrated Tactical Warning and Attack Assessment (ITW/AA) systems.

The JTA mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. The main body of the JTA (the “Core”) provides the standards that are applicable across the entire DoD information technology spectrum. If a service area in the Core applies to an NCC system being developed, and there is no corresponding service area in the C4ISR Domain, then the standard(s) listed in a Core service area apply. The mandates found in the C4ISR Domain are intended to augment those found in the Core. If additional service area standards are found in the C4ISR Domain, the developer must select the service area standards from both the Core and the C4ISR Domain. Similarly, the NCC Subdomain is intended to augment the C4ISR Domain. Applicable service area mandates found in the NCC Subdomain must be used in addition to the service area mandates found in the C4ISR Domain and the Core. When multiple mandates are required in this process, the mandate selection offering the best technical and business solution is the preferred decision.

The NCC Subdomain may list multiple standards for individual service areas. Similarly, the Core and the subdomain may offer multiple solutions within a single service area. For these cases, it is not required that the developer implement all standards listed. A subset should be selected based on technical merit and design/cost constraints. Future versions of this subdomain will have detailed information on standards implementation and standards profiles. The intent, as previously stated, is to promote a minimum set of standards for interoperability among NCC systems.

C4ISR.NCC.1.5 Technical Reference Model

This subdomain uses the DoD Technical Reference Model cited in 1.5 of the JTA as its framework.

C4ISR.NCC.1.6 Subdomain Organization

The organization of this subdomain is intended to mirror the organization of the C4ISR Domain to the greatest extent possible. Each section of the subdomain, except for Part 1 (Overview), is divided into three subsections as follows. The first subsection, Introduction, is for information only. It defines the purpose and scope of the subsection and provides background descriptions and definitions unique to the section. The second subsection contains additional mandated standards for the identified service area. The third subsection, Emerging Standards, provides an abbreviated description of candidates that are expected to move into the mandated subsection within a short period. As defined within the JTA Core, this transition should occur within three years of publication of the standard in the emerging subsection.

C4ISR Application Platform Entity service areas are addressed in Section C4ISR.NCC.2 as additions to the JTA Core and C4ISR Domain. Additional application software entity service areas required to support NCC subdomain systems will be addressed in Section C4ISR.3, Domain-Specific Service Areas.

C4ISR.NCC.2 Additions to C4ISR Domain Service Areas

C4ISR.NCC.2.1 Introduction

This section provides standards available to this subdomain in addition to those listed in the JTA Core and C4ISR Domain.

C4ISR.NCC.2.2 Information Processing Standards

C4ISR.NCC.2.2.1 Introduction

This subdomain provides additional information processing standards.

C4ISR.NCC.2.2.2 Mandated Standards

There are currently no additional mandated standards applicable to this subdomain with respect to Information Processing Standards.

C4ISR.NCC.2.2.3 Emerging Standards

This version of the NCC Subdomain does not identify any emerging standards for information processing.

C4ISR.NCC.2.3 Information Transfer Standards

C4ISR.NCC.2.3.1 Introduction

Proper handling of NCC information is vital to national security. Information transfer standards and profiles described in this section cover dissemination and data link mandates for NCC systems. This section identifies systems and the interface standards required for interoperability between and among NCC systems and are in addition to the systems described in the JTA Core and the C4ISR Domain.

C4ISR.NCC.2.3.2 Mandated Standards

Additional mandated standards for information transfer for the NCC Subdomain are provided in this section.

For radio subsystems operating in the LF/VLF frequency bands, the following standards specify the special modes used by Air Force and Navy forces in support of the USSTRATCOM mission.

For sending and receiving High Data Rate (HIDAR)-mode communications the following standard is mandated:

- HDR-SSS-01-S-REC0, Very Low Frequency/Low Frequency (VLF/LF) High Data Rate (HIDAR) Mode Standard.

For sending and receiving Minimum Essential Emergency Communications Network (MEECN) Message-Processing Mode (MMPM) communications the following standard is mandated:

- NAVELEX 28687-0119-404, MEECN Message Processing Mode Standard.

C4ISR.NCC.2.3.3 Emerging Standards

This version of the NCC Subdomain does not identify any emerging standards for information transfer.

C4ISR.NCC.2.4 Information Modeling, Metadata, and Information Exchange Standards

C4ISR.NCC.2.4.1 Introduction

This section identifies standards applicable to information modeling and exchange of information for NCC systems. Information Modeling, Metadata, and Information Exchange Standards pertain to activity models, data models, data definitions, and information exchange among NCC systems.

C4ISR.NCC.2.4.2 Mandated Standards

The following standards for NCC for Emergency Action Messages (EAMs) are mandated:

- Emergency Action Procedures (EAP), Chairman Joint Chiefs of Staff (CJCS), Volume V, “CJCS Control Orders (U),” revised annually (U.S. TOP SECRET).
- EAP CJCS Volume VII, “EAM Dissemination and Force Report Back (U),” revised annually (U.S. TOP SECRET).

C4ISR.NCC.2.4.3 Emerging Standards

This version of the NCC Subdomain does not identify any emerging standards for information modeling, metadata and information exchange.

C4ISR.NCC.2.5 human-computer Interface Standards

C4ISR.NCC.2.5.1 Introduction

This subsection identifies the mandatory standards, profiles, and practices for human-computer interfaces within the NCC subdomain. The human-computer interface (HCI) is an extremely important NCC function.

C4ISR.NCC.2.5.2 Mandated Standards

This section will provide standards that uniquely apply to the HCI of NCC systems.

C4ISR.NCC.2.5.3 Emerging Standards

This section contains emerging HCI standards applicable to Nuclear C^2 systems.

To reduce training requirements, the standard HCI for all EAM injection processors will be consistent with the following emerging standard:

– HMI DIRECT ICD, "Human-Machine Interface (HMI) Design Criteria," CDRL 135C-03,V3.0, 5 March 99.

C4ISR.NCC.2.6 Information Security Standards

C4ISR.NCC.2.6.1 Introduction

Information security standards protect information and the processing platform resources. They must often be combined with security procedures, which are beyond the scope of the information technology service areas, to fully meet operational security requirements. Security services include security policy, accountability, assurance, user authentication, access control, data integrity and confidentiality, non-repudiation, and system availability control.

C4ISR.NCC.2.6.2 Mandated Standards

There are currently no additional mandated standards applicable to this subdomain with respect to Information Security Standards.

C4ISR.NCC.2.6.3 Emerging Standards

This version of the NCC Subdomain does not identify any emerging standards for information security.

C4ISR.NCC.3 Subdomain-Specific Service Areas

This version of the NCC Subdomain does not define any additional service areas.

C4ISR.SR: Space Reconnaissance Subdomain

C4ISR.SR.1 Subdomain Overview

C4ISR.SR.1.1 Purpose

The Space Reconnaissance (SR) Subdomain (SRS) to the C4ISR Domain identifies the minimum set of technical supporting interfaces between SR information technology (IT) systems and other Department of Defense (DoD) systems. The IT definition used within the SRS is found in JTA Appendix F.

The standards contained here are mandated for SR IT interfaces in addition to those standards found in the C4ISR Domain and in the JTA. The SRS will provide the foundation for the seamless flow of information and interoperability among all future and upgraded SR space and associated ground IT systems, IT technology concept demonstrations, and with related DoD IT systems. Standards used by SR legacy systems to support internal interfaces (i.e., interfaces to non-DoD systems) have not been examined and cannot be presumed to be JTA-compliant.

C4ISR.SR.1.2 Background

Space Reconnaissance IT standards represent the communities engaged in all aspects of creating, deploying, and employing space reconnaissance assets for national defense. The standards within JTA (including the SRS) support a range of functions. The SRS supplies a special focus on space-related functions unique within JTA. The SRS identifies additional standards that have been determined to be unique to SR communications and data processing. Standards not unique to SR are contained in the C4ISR Domain or in the JTA Core. The location and application of standards within the JTA Core, C4ISR Domain and SRS are in accordance with the element normalization rules described in 1.8. Future versions of the SRS will address standards not previously identified, or not yet mature (under the JTA rule set), but expected to be developed into SRS-mandated standards. When identified, these standards will be placed in the emerging standards sections in each of the subdomain's service areas.

C4ISR.SR.1.3 Subdomain Description

The SRS adds to the standards and guidance required for the Space Reconnaissance Subdomain and is meant to complement both the C4ISR Domain and the JTA Core. The SRS contains information on standards implementation and standards profiles.

The SRS will be maintained by the SRS Working Group chaired by the National Reconnaissance Office (NRO) with all changes made in concert with the normal JTA revision procedures. Modifications to the SRS will be coordinated with the established working group for the SRS.

C4ISR.SR.1.4 Scope and Applicability

JTA compliance, where applicable, is required for acquisition of upgraded and new SR IT systems as well as advanced technology demonstrations. The SRS scope comprises SR IT system standards for interfaces external to DoD IT systems. The standards mandated in the JTA Core, C4ISR Domain, and SRS are applicable to the external SR IT interfaces. The SRS includes those pending SRS IT systems whose system specifications and design are intended for near-term acquisition and which include DoD interfaces, where appropriate. The SRS is also applicable where needed for the seamless flow of information and interoperability among SR systems with airborne and other intelligence, surveillance, and reconnaissance systems and is intended to complement their subdomains to the C4ISR Domain.

C4ISR.SR.1.5 DoD Technical Reference Model

The DoD Technical Reference Model (TRM) is derived from the original Technical Architecture Framework for Information Management (TAFIM) reference model and Society of Automotive Engineers (SAE) Generic Open Architecture (GOA) model. GOA provides extensions to support real-time computing environments such as those found in weapon systems. The TRM is primarily a software-based model. It was originally developed to cover information technology within DoD. The TRM framework concept can be extended to cover SR external interface with DoD systems. However, domain-specific standards such as those required to cover all national space reconnaissance systems do not fully fit within this software-based model and so work continues as noted below.

C4ISR.SR.1.5.1 SR TRM Defined

Various reference models are being evaluated for SR applicability. In the interim, the SRS uses the DoD Technical Reference Model (TRM) to cover SR system external interfaces with DoD IT systems. Where exceptions to the TRM are required, it will be noted in this subdomain. The DoD TRM is shown in Figure 1-4 of the JTA.

C4ISR.SR.1.6 Subdomain Organization

The organization of this Subdomain follows the JTA-approved format for developing domain and subdomains. The SRS contains three parts. C4ISR.SR.1 is the Overview. C4ISR.SR.2 includes mandatory standard profiles, practices, and emerging standards that are applicable to the SR Subdomain. Emerging standards provide an abbreviated description of candidates expected to move into the mandated subsection within a short period. As defined within the Core of the JTA, this transition should occur within three years of publication of the standard in the emerging subsection. C4ISR.SR.3 is reserved for those mandates that are subdomain-specific because they do not map directly to the JTA Core service areas.

C4ISR.SR.2 Additions to C4ISR Domain Service Areas and JTA Core

C4ISR.SR.2.1 Introduction

The SRS, in conjunction with the JTA Core and the C4ISR Domain, provides the technical foundation for migrating SR IT systems toward a technical architecture that provides interoperable interfaces to DoD systems. This section of the SRS lists the minimum, mandatory set of standards for SR systems. This section includes information processing; information transfer; information modeling, metadata, and information exchange; human-computer interface; and information security standards. This part of the SRS does not contain rules for the physical, mechanical, or electrical components of systems, even when these are related to information technology.

C4ISR.SR.2.2 Information Processing Standards

C4ISR.SR.2.2.1 Introduction

C4ISR.SR.2.2.2 Mandated Standards

This version of the SRS does not specify any additional standards for information processing.

C4ISR.SR.2.2.3 Emerging Standards

The following standard is emerging for systems that require the use of an application program interface (API) for calendaring and scheduling applications:

– C321, Calendaring and Scheduling API (XCS), Open Group Technical Standard, ISBN 1-85912-076-8, April 1995.

C4ISR.SR.2.3 Information Transfer Standards

C4ISR.SR.2.3.1 Introduction

Information transfer standards are used to disseminate National and Tactical intelligence information to Joint service tactical units. This section identifies interface standards required for interoperability between SR IT and other DoD ISR systems in addition to the standards cited in the JTA Core and C4ISR Domain.

C4ISR.SR.2.3.2 Mandated Standards

The following additional information transfer standard is mandated for SR communication systems:

- GR-253, Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria, Rev01, Bellcore, December 1997.

C4ISR.SR.2.3.2.1 Point-to-Point Standards

The following hardware-related information transfer standard is mandated for SR communication systems:

- TIA/EIA-422B, Electrical Characteristics of Balanced Voltage Digital Interface Circuits, May 1994.

C4ISR.SR.2.3.3 Emerging Standards

This version of the SRS does not identify any emerging information transfer standards.

C4ISR.SR.2.4 Information Modeling, Metadata, and Information Exchange Standards

C4ISR.SR.2.4.1 Introduction

C4ISR.SR.2.4.2 Mandated Standards

This version of the SRS does not specify any additional standards for information modeling, metadata, and information exchange. An ongoing effort by the NRO will identify applicable standards for future versions of this.

C4ISR.SR.2.4.3 Emerging Standards

This version of the SRS does not identify any emerging standards for information modeling, metadata, and information exchange. An ongoing effort by the NRO will identify any emerging standards for future versions of the JTA.

C4ISR.SR.2.5 Human-Computer Interface Standards

C4ISR.SR.2.5.1 Introduction

C4ISR.SR.2.5.2 Mandated Standards

This version of the SRS does not specify any additional standards for human-computer interfaces.

C4ISR.SR.2.5.3 Emerging Standards

This version of the SRS does not identify any emerging standards for human-computer interfaces. An ongoing effort by the NRO will identify any emerging standards for future versions of the JTA.

C4ISR.SR.2.6 Information Security Standards

C4ISR.SR.2.6.1 Introduction

C4ISR.SR.2.6.2 Mandated Standards

This version of the SRS does not specify any additional standards for information security.

C4ISR.SR.2.6.3 Emerging Standards

This version of the SRS does not identify any emerging standards for information security. An ongoing effort by the NRO will identify any emerging standards for future versions of the JTA.

C4ISR.SR.3 Subdomain-Specific Service Areas

There are no subdomain-specific service areas identified at this time.

CS: Combat Support Domain

CS.1 Domain Overview

CS.1.1 Purpose

The Combat Support (CS) Domain has been developed to integrate agile combat support elements and other domains with a common technical architecture for information exchange. The goals for the Combat Support (CS) Domain are: 1) improve applications interoperability, promote improved business practices, and reduce operations costs within the Combat Support Domain, and 2) improve interoperability and increase combat support information access with C4ISR systems.

CS.1.2 Background

There are numerous information technology services that support warfighter activities. These services need to be interoperable with the rest of the DoD community.

CS.1.3 Domain Description

The Combat Support 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 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. As illustrated in Figure CS-1, the domain has three subdomains: Automatic Test Systems (CS.ATS), Defense Transportation System (CS.DTS), and Medical (CS.MED).

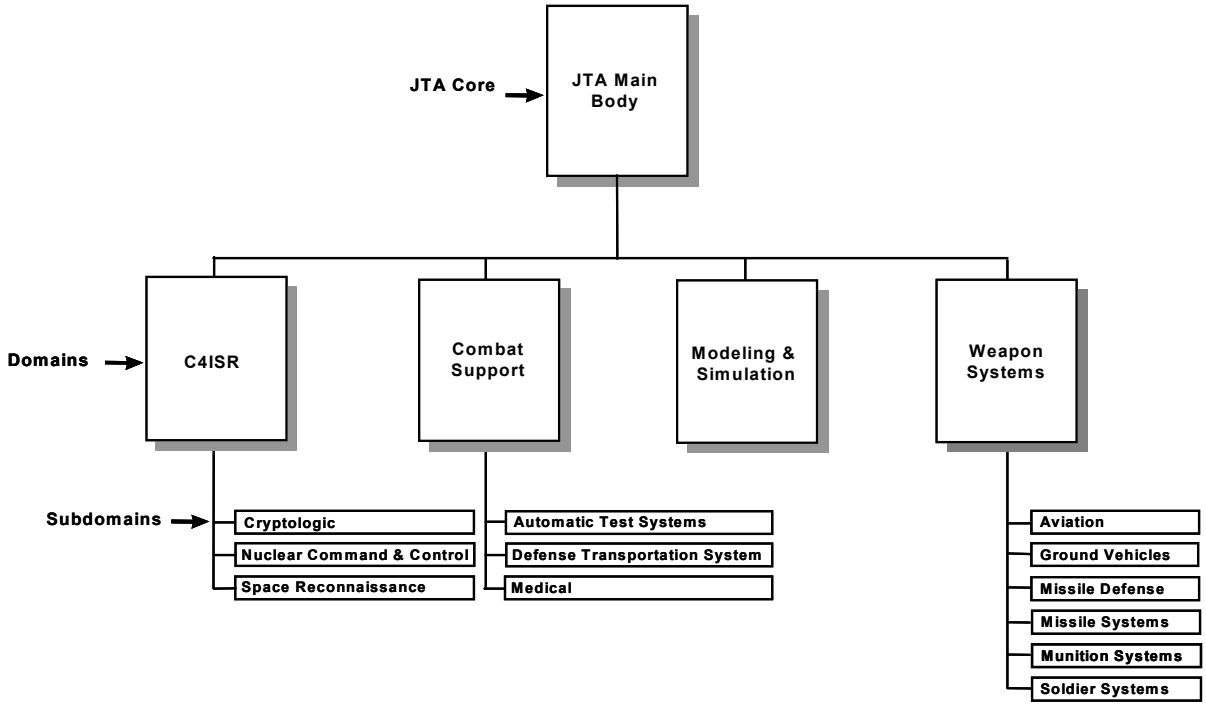


Figure CS-1: JTA Hierarchy Model

CS.1.4 Scope and Applicability

The Combat Support Domain identifies standards applicable to DoD Combat Support Elements (e.g., Logistics, EDI, CALS, Medical, Transportation).

CS.1.5 Technical Reference Model

This domain uses the Technical Reference Model (TRM) cited in 1.5 of the JTA as its framework. Combat Support Application Platform Entity service areas are addressed in Section CS.2 as additions to the JTA Core. Additional Application Software Entity service areas required to support Combat Support Domain systems are addressed in Section CS.3 as domain-specific service areas.

CS.1.6 Domain Organization

The Combat Support Domain consists of three sections. CS.1 contains the overview, CS.2 contains those information technology mandated and emerging standards that are additions to the standards contained in the Core, and CS.3 is reserved for those mandated and emerging standards for combat support that are domain-specific, not associated with a Core service area.

CS.2 Additions to JTA Core

CS.2.1 Introduction

The Combat Support Domain embraces the principles established in the JTA Core. Only those paragraphs from the Core that have additions are included below.

CS.2.2 Information Processing Standards

CS.2.2.1 Introduction

CS.2.2.2 Mandated Standards

CS.2.2.2.1 Document Interchange

Continuous Acquisition and Life-Cycle Support (CALS) has developed a set of standards that apply to this service area. CALS Standard Generalized Markup Language (SGML) profiles the standard ISO 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 Markup Language (HTML) is also a subset of SGML, it is not sufficiently robust enough for Technical Manual (TM)/ Technical Order (TO) development. [Extensible Markup Language (XML) may replace both CALS SGML and HTML in the future.] CALS also has a standard for archiving documents (MIL-STD-1840C). The mandated standards for the CALS Document Interchange Service Area 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.

CS.2.2.2.2 Graphics Data Interchange

CALS has developed a metadata standard, MIL-PRF-28003B, 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:

- ISO/IEC 8632-1:1999, Information technology – Computer graphics – Metafile for the storage and transfer of picture description information – Part 1: Functional specification, as profiled by

MIL-PRF-28003B, Digital Representation for Communication of Illustration Data: CGM Application Profile, 30 April 2000.

- ISO/IEC 8632-3:1999, Information technology – Computer graphics – Metafile for the storage and transfer of picture description information – Part 3: Binary encoding, as profiled by MIL-PRF-28003B, Digital Representation for Communication of Illustration Data: CGM Application Profile, 30 April 2000.
- ISO/IEC 8632-4:1999, Information technology – Computer graphics – Metafile for the storage and transfer of picture description information – Part 4: Clear text encoding, as profiled by MIL-PRF-28003B, Digital Representation for Communication of Illustration Data: CGM Application Profile, 30 April 2000.
- MIL-PRF-28002C, Performance Specification, Requirements for Raster Graphics Representation in Binary Format, 30 September 1997.

CS.2.2.2.3 Product Data Interchange

Several standards exist for exchanging product data. The ANSI/US PRO/IPO-100-1996 and MIL-PRF-28000B standards define a neutral data format that allows the digital exchange of information between Computer-Aided Design (CAD) and Computer-Aided Manufacturing (CAD/CAM) systems. ANSI/US PRO-100-1996 supports digital design and manufacturing information about an object sufficient to support manufacturing and construction only. MIL-PRF-28000B contains applications subsets and protocols that form profiles of IGES Version 5.3. The following standard is mandated:

- ANSI/US Product Data Association (PRO)-100-1996, Initial Graphics Exchange Specification (IGES), V5.3, 23 September 1996, as profiled by MIL-PRF-28000B, Digital Representation for Communications of Product Data: IGES Application Subsets and IGES Application Protocols, 30 September 1999.

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 ANSI/IEEE 1076. 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.
- ANSI/IEEE 1076:1993, IEEE Standard VHDL Language Reference Manual.
- MIL-STD-1840C, Automated Interchange of Technical Information (AITI), 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. (See CS.DTS.2.2.2.1 for two-dimensional standard.) The following standard is mandated:

- ANSI/AIM-BC1-1995, Uniform Symbology Specification Code 39, 16 August 1995.

CS.2.2.2.4 Electronic Data Interchange

Electronic Data Interchange (EDI) is a new Base 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), 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://snad.ncsl.nist.gov/dartg/edi/fededi.html>.

The DoD EDI Standards Management Committee (EDISMC) was established to coordinate 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 (FWGs). DoD FWGs have been established in the following areas: Logistics, Finance, Healthcare, Transportation, Procurement, and Communication, Command and Control. EDISMC-approved implementation conventions may be submitted to the FESMCC for approval as Federal implementation conventions. Not all DOD ICs are submitted to the FESMCC for federal approval. For more information, visit the web site 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. HL7 can be found in Combat Support Medical Subdomain. The following standards are mandated:

- ANSI ASC X12 Electronic Data Interchange, as profiled by FIPS PUB 161-2, Electronic Data Interchange, 22 May 1996.
- ISO 9735 UN/EDIFACT, Application Level Syntax Rules, as profiled by FIPS PUB 161-2, Electronic Data Interchange, 22 May 1996.

CS.2.2.3 Emerging Standards

CS.2.2.3.1 Product Data Interchange

ISO 10303, 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 Computer-Aided Design/Computer-Aided Manufacturing (CAD/CAM) applications. STEP supports the entire life cycle of a product, independent of 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 10303-1:1994, Industrial automation systems and integration – Product data representation and exchange – Part 1, Overview and fundamental principles.
- ISO 10303-11:1994, Industrial automation systems and integration – Product data representation and exchange – Part 11:Description methods: The EXPRESS language reference manual.
- ISO/TR 10303-12:1997, Industrial automation systems and integration – Product data representation and exchange – Part 12: Description methods: The EXPRESS-I language reference manual.
- ISO 10303-21:1994, Industrial automation systems and integration – Product data representation and exchange – Part 21: Implementation methods: Clear text encoding of the exchange structure.
- ISO 10303-22:1998, Industrial automation systems and integration – Product data representation and exchange – Part 22: Implementation methods:Standard data access interface.
- ISO 10303-31:1994, Industrial automation systems and integration – Product data representation and exchange – Part 31: Conformance testing methodology and framework: General Concepts.

- ISO 10303-32:1998, Industrial automation systems and integration – Product data representation and exchange – Part 32: Conformance testing methodology and framework: Requirements on testing laboratories and clients.
- ISO 10303-41:1994, Industrial automation systems and integration – Product data representation and exchange – Part 41: Integrated generic resources: Fundamentals of product description and support.
- ISO 10303-42:1994, Industrial automation systems and integration – Product data representation and exchange – Part 42: Integrated generic resources: Geometric and topological represenation.
- ISO 10303-43:1994, Industrial automation systems and integration – Product data representation and exchange – Part 43: Integrated generic resources: Representation structures.
- ISO 10303-44:1994, Industrial automation systems and integration – Product data representation and exchange – Part 44: Integrated generic resources: Product structure configuration.
- ISO 10303-45:1998, Industrial automation systems and integration – Product data representation and exchange – Part 45: Integrated generic resources: Materials.
- ISO 10303-46:1994, Industrial automation systems and integration – Product data representation and exchange – Part 46: Integrated generic resources: Visual presentation.
- ISO 10303-47:1997, Industrial automation systems and integration – Product data representation and exchange – Part 47: Integrated generic resources: Shape variation tolerances.
- ISO 10303-49:1998, Industrial automation systems and integration – Product data representation and exchange – Part 49: Integrated generic resources: Process structure and properties.
- ISO 10303-101:1994, Industrial automation systems and integration – Product data representation and exchange – Part 101: Integrated application resources: Draughting.
- ISO 10303-105:1996, Industrial automation systems and integration – Product data representation and exchange – Part 105: Integrated application resources: Kinematics.
- ISO 10303-201:1994, Industrial automation systems and integration – Product data representation and exchange – Part 201: Application protocol:Explicit draughting.
- ISO 10303-202:1996, Industrial automation systems and integration – Product data representation and exchange – Part 202: Application protocol: Associative draughting.
- ISO 10303-203:1994, Industrial automation systems and integration – Product data representation and exchange – Part 203: Application protocol: Configuration controlled design.
- ISO 10303-224:1999, Industrial automation systems and integration – Product data representation and exchange – Part 224: Application protocol: Mechanical product definition for process planning using machining features.

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 13584-20:1998, Industrial automation systems and integration – Parts library – Part 20: Logical resource: Logical model of expressions.
- ISO/IEC 13584-42:1998, Industrial automation systems and integration – Parts library – Part 42: Description methodology: Methodology for structuring part families.

CS.2.3 Information Transfer Standards

There are no mandated or emerging standards for the Combat Support Information Transfer Standards section.

CS.2.4 Information Modeling, Metadata, and Information Exchange Standards

CS.2.4.1 Electronic Fingerprint Information Exchange Standards

The electronic exchange of fingerprint information with automated fingerprint identification and analysis systems requires fingerprints to be electronically captured to image quality standards and to be formatted and documented in standard formats that are essential to interoperability. The following standard is mandated for the capture, fingerprint image compression/decompression, and exchange of electronic fingerprint information for the purpose of interoperating with criminal justice automated fingerprint information systems and repositories.

- ANSI/NIST-ITL 1-2000, Data Format for the Interchange of Fingerprint, Facial, and Scar Mark and Tattoo (SMT) Information, July 2000 (revision, redesignation and consolidation of ANSI/NIST-CSL 1-1993 and ANSI/NIST-ITL 1a-1997).

CS.2.5 Human-Computer Interface Standards

There are no mandated or emerging standards for the Combat Support Human-Computer Interface Standards section.

CS.2.6 Information 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.

CS.3 Domain-Specific Service Areas and Interfaces

CS.3.1 Electronic Business/Electronic Commerce

CS.3.1.1 Introduction

The Electronic Business/Electronic Commerce (EB/EC) Section provides standards useful for any DoD effort involved in electronic business operations. DoD focus on EB/EC has been limited primarily to acquisition-centric transactions. This limited scope has precluded DoD from taking full advantage of the significant process improvement and reengineering opportunity available through the implementation of EB/EC concepts and technology. EB/EC within DoD must now be thought of in a significantly larger perspective, which permits support of Finance, Procurement, Logistics, Personnel, Medical, Transportation, and Acquisition functions.

CS.3.1.2 Mandated Standards

CS.3.1.2.1 Smart Card Technology Standards

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 7816-1:1998, Identification Cards – Integrated Circuit(s) cards with contacts – Part 1: Physical characteristics.
- ISO/IEC 7816-2:1999, Identification Cards – Integrated Circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts.

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

CS.3.1.3 Emerging Standards

CS.3.1.3.1 Smart Card Technology Standards

The standards for both contact and contactless Smart Cards are still evolving and being specified. ISO 7816 series is for contact Smart Cards while ISO 10536, 14443, and 15693 specify the standards for various types of contactless smart cards. The following Smart Card standards are emerging:

- ISO/IEC 7816-8:1998, Identification Cards – Integrated circuit(s) card with contacts – Part 8, Security architecture and related interindustry commands.
- ISO/IEC 7816-9:1999, Identification Cards – Integrated circuit(s) card with contacts – Part 9: Enhanced interindustry commands.
- ISO/IEC 7816-10:1998, Identification Cards – Integrated circuit(s) card with contacts – Part 10: Electronic signals and answer to reset for synchronous cards.
- ISO/IEC 10536-4:1995 Identification Cards – Contactless integrated circuit(s) card; Part 4, Answer to reset and transmission protocols.
- ISO/IEC 14443-1:1998, Identification Cards – Contactless integrated circuit(s) cards – Proximity integrated circuit(s) cards – Part 1: Physical characteristics.
- ISO/IEC 14443-2:1999, Identification Cards – Contactless integrated circuit(s) cards – Proximity integrated circuit(s) cards – Part 2: Radio Frequency Interface.
- ISO/IEC 14443-3:1999, Identification Cards – Contactless integrated circuit(s) cards – Proximity integrated circuit(s) cards – Part 3: Initialization and anti-collision.
- ISO/IEC 14443-4:1999, Identification Cards – Contactless integrated circuit(s) cards – Proximity integrated circuit(s) cards – Part 4 Transmission protocols.
- ISO/IEC 15693-1:1999, Identification Cards – Contactless integrated circuit(s) – Vicinity cards – Part 1: Physical characteristics.
- ISO/IEC 15693-2:1999, Identification Cards – Contactless integrated circuit(s) – Vicinity cards – Part 2: Air interface and initialization.
- ISO/IEC 15693-3:1999, Identification Cards – Contactless integrated circuit(s) – Vicinity cards – Part 3: Protocols.
- ISO/IEC 15693-4:1996, Identification Cards – Contactless integrated circuit(s) – Vicinity cards – Part 4: Registration of applications and issuers.

Page intentionally left blank.

CS.ATS: Automatic Test Systems Subdomain

CS.ATS.1 Subdomain Overview

CS.ATS.1.1 Purpose

The Automatic Test Systems (ATS) Subdomain identifies additions to the Combat Support Domain Core elements (i.e., standards, interfaces, and service areas) listed in JTA Core of this document. These additions are common to the majority of ATSs and support the functional requirements of these systems.

The purpose of the ATS Subdomain is to:

- Provide the foundation for a seamless flow of information and interoperability among all Department of Defense (DoD) ATS.
- Mandate standards and guidelines for system development and acquisition that will significantly reduce cost, development time, and fielding time for improved systems, while minimizing the impact on program performance wherever possible.
- Improve the test acquisition process by creating an ATS framework that can meet functional and technical needs, promote automation in software development, and the re-hostability and portability of Test Program Sets (TPSs).
- Communicate to industry DoD's intention to use open systems products and implementations. DoD will buy commercial products and systems that use open standards to obtain the most value for limited procurement dollars.

CS.ATS.1.2 Background

From 1980 to 1992, DoD's investment in depot and factory ATSs exceeded $35 billion with an additional $15 billion for associated support. Often, application-specific test capability was procured by weapon systems acquisition offices with little coordination among DoD offices. This resulted in a proliferation of different custom equipment types with unique interfaces that made DoD appear to be a variety of separate customers. To address this problem, DoD enacted policy changes requiring that "Automatic Test System capabilities be defined through critical hardware and software elements." In response, the joint service Automatic Test Systems (ATS) Research and Development (R&D) Integrated Product Team (IPT), known as ARI, has worked toward the definition of an ATS architecture based on open system principles. A summary of the ARI's work is presented in this subdomain . The ATS Subdomain will aid in satisfying the requirements of DoD Regulation 5000.2-R to migrate DoD-designated tester families toward a common architecture.

The policy changes listed below require DoD offices to take a unified corporate approach to acquisition of ATSs.

- DoD Regulation 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information System Acquisition Programs, paragraph 4.3.3.4, March 15, 1996, brings a cost-effective approach to the acquisition of ATS. This policy requires hardware and software needs for depot- and intermediate-level applications to be met using DoD-designated families and commercial equipment with defined interfaces and requires the management of ATS as a separate commodity through a DoD Executive Agent Office (EAO). The policy also requires that the introduction of unique types of ATS into DoD field, depot, and manufacturing operations be minimized. Change 3 of DoD 5000.2-R, dated March 23, 1998,

requires that the ATS selection "shall be based on a cost and benefit analysis that ensures that the ATS chosen is the most beneficial to the DoD over the system life cycle."

- Secretary of Defense Memorandum on Specifications and Standards, 29 June 1994, directs that DoD procurements be made first by performance definition, second by commercial standards, and finally (and only with waiver) by military standards.

The use of open standards in ATSs has been projected to provide the following five benefits.[1]

- Improve the test acquisition process by creating an ATS framework that can meet functional and technological needs, and promote automation in software development, re-hostability, and portability of TPSs.
- Decrease the use of custom hardware from approximately 70 percent today to 30 percent.
- Reduce engineering costs 70 percent.
- Reduce TPS integration time and cost 50 to 75 percent.
- Provide an iterative improvement in the quality of test by the reuse and refinement of libraries.

CS.ATS.1.3 Subdomain Description

An ATS has three major components: Automated Test Equipment (ATE), TPSs, and the Test Environment. The ATE consists of test and measurement instruments, a host computer, switching, communication buses, a receiver, and system software. The host computer controls the test and measurement equipment and execution of the TPS. The system software controls the test station and allows TPSs to be developed and executed. Examples of system software include operating systems, compilers, and test executives. The TPS consists of software to diagnose Units Under Test (UUT), a hardware fixture that connects the UUT to the ATE, and documentation that instructs the station operator on how to load and execute the TPS. The Test Environment includes a description of the ATS Architecture, programming and test specification languages, compilers, development tools, a standard format for describing UUT design requirements, and test strategy information that allows TPS software to be produced at a lower cost.

A high-level overview of a typical ATS is shown in Figure CS.ATS-1. This architecture is expanded into more detail in the hardware and software technical reference models introduced in Section CS.ATS.1.5. The interfaces in the technical reference models are discussed in more detail in CS.ATS.2 and CS.ATS.3.

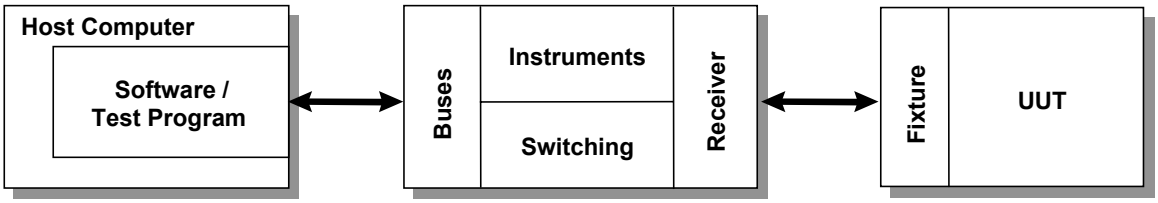


Figure CS.ATS-1: Generic ATS Architecture

[1] Institute for Defense Analysis (IDA) Investment Strategy Study. Alexandria, VA: Institute for Defense Analysis (IDA), 1993.

CS.ATS.1.4 Scope and Applicability

The following factors guided the selection of interfaces in the ATS Subdomain.

- Hardware and Software – Hardware and software associated with the supported test domains and software interfaces required to build ATS were included.
- Signal Types – The scope was limited to digital, analog, Radio Frequency (RF), and microwave electrical signals.
- Testing Levels – The interface standards in the ATS Subdomain are mandated for factory, depot, intermediate, and operational/organizational levels of ATS.

The standards selected for inclusion in the ATS Subdomain were found to be key for the generic, open system architecture of ATSs. The standards are based on commercial, open system technology, have implementations available, and are strongly supported in the commercial marketplace. Standards in the ATS Subdomain meet the following criteria:

- Availability – The standards are currently available.
- Commercial Acceptance – The standards are used by several different commercial concerns.
- Efficacy – The standards increase the interoperability of ATS hardware and software.
- Openness – Mandated standards are all open, commercial standards.

Standards that are commercially supported in the marketplace with validated implementations available in multiple vendors' mainstream commercial products took precedence over other standards. Publicly held standards were generally preferred. International or national industry standards were preferred over military or other Government standards. Many standards have optional parts or parameters that can affect interoperability. In some cases, a standard may be further defined by a standards profile, which requires certain options to be present to ensure proper operation and interoperability.

Previously, each of the Services had established its own sets of standards (e.g., technical architectures). The ATS Subdomain is envisioned as a single, generic, open system architecture in DoD ATS. The ATS Subdomain shall be used by anyone involved in the management, development, or acquisition of new or improved ATSs within DoD. System developers shall use the ATS Subdomain to ensure that new and upgraded ATSs, and the interfaces to such systems, meet interoperability requirements. System integrators shall use this document to facilitate the integration of existing and new systems. Operational requirements developers shall be cognizant of the ATS Subdomain in developing requirements and functional descriptions. ATS is a subdomain of the Combat Support Domain of the JTA.

CS.ATS.1.5 Technical Reference Model

CS.ATS.1.5.1 Hardware

The hardware interfaces in a typical ATS are shown in Figure CS.ATS-2. Interfaces are only mandated if they affect the interoperability or life-cycle costs of DoD ATS, and are supported by widely accepted commercial standards. Interfaces are not mandated if they are not supported by commercial standards or do not affect the interoperability or life-cycle costs of DoD ATS. Interfaces that are not supported by commercial standards are included as emerging standards if they affect the interoperability or life-cycle costs of DoD ATS.

The interfaces shown in Figure CS.ATS-2 are listed alphabetically by mnemonic below:

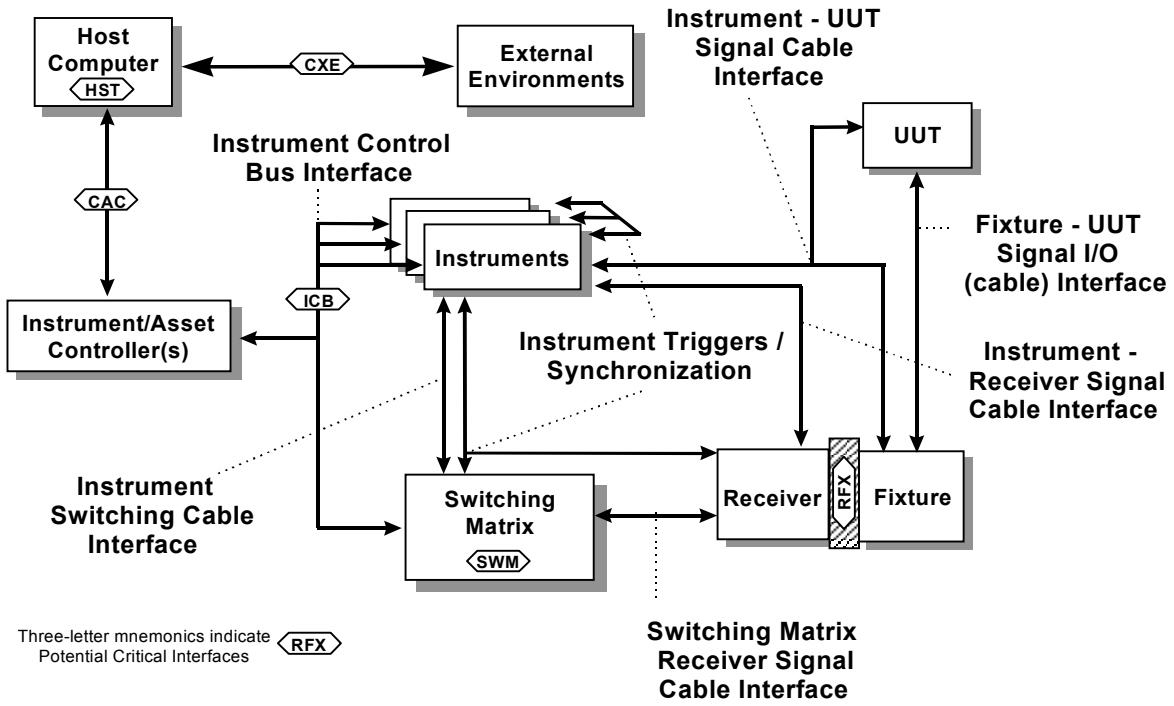


Figure CS.ATS-2: Hardware Interfaces

- **Computer Asset Controller Interface (CAC)** describes the communication paths between the host computer and instrument controllers in a distributed system.
- **Computer to External Environments (CXE)** describes the communication methods between a host ATS and remote systems.
- **Host Computer Interface (HST)** describes the processing architecture of the primary control computer in which the TPS is executed and through which the operator interfaces.
- **Instrument Control Bus (ICB)** interface describes the connection between the host computer or instrument controller and the test and measurement instruments in the ATS.
- **Receiver/Fixture Interface (RFX)** describes the interface between the receiver (part of the ATS) and the Fixture (part of the TPS). The RFX establishes an electrical and mechanical connection between the UUT and the ATS.
- **Switching Matrix Interface (SWM)** describes switch paths that connect ATS test and measurement instruments to pins on the RFX.

CS.ATS.1.5.2 Software

The software interfaces are introduced using two reference models: a runtime view and a TPS development view. The interfaces applicable to the runtime view are shown in Figure CS.ATS-3. These interfaces describe information processing flows as the TPS diagnoses a UUT. The TPS development interfaces are shown in Figure CS.ATS-4.

In these diagrams, Host Computer refers to computers that run the ATS and instrument asset controllers and computers that are subordinate to the host. The runtime diagram presents a generic template for the functional organization of software processes. Subsets of this structure will appear on individual processors in a distributed-processing architecture. On any processor, if components shown on this

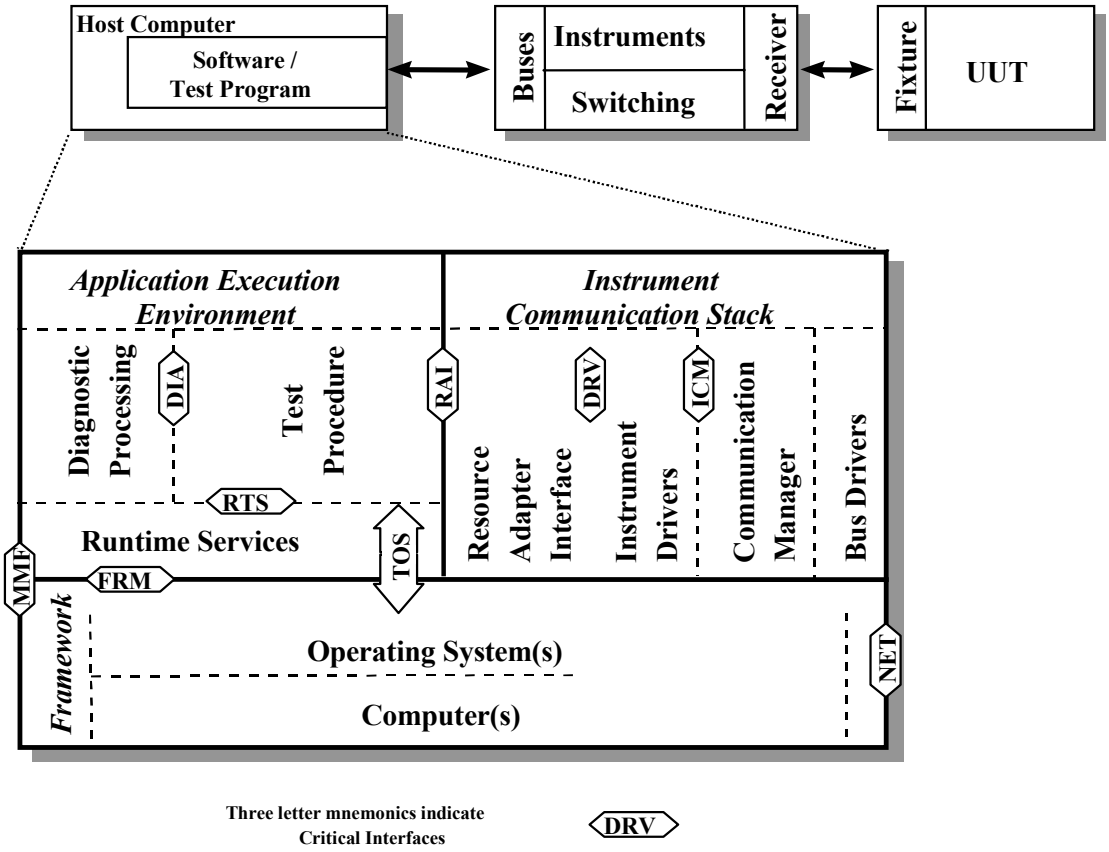


Figure CS.ATS-3: Test Program Sets Runtime Interfaces

diagram are present and interact, their interactions must comply with the interface requirements identified in this document.

The interfaces depicted in the runtime view of Figure CS.ATS-3 are listed alphabetically by mnemonic below:

- **Diagnostic Processing (DIA)** is the interface protocol linking execution of a test with software diagnostic processes that analyze the significance of the test results and suggest conclusions or additional actions required.
- **Instrument Driver API (DRV)** is the API through which instrument drivers accept commands from, and return results to, Generic Instrument Classes.
- **Framework (FRM)** is a collection of system requirements, software protocols, and business rules (e.g., software installation) affecting the operation of test software with its host computer and operating system (OS).
- **Instrument Command Language (ICL)** is the language in which instrument commands and results are expressed as they enter or leave the instrument.
- **Instrument Communication Manager (ICM)** is the interface between the instrument drivers and the Communication Manager that supports communication with instruments independent of the bus or other protocol used (e.g., VXI, IEEE-488.2, RS-232).

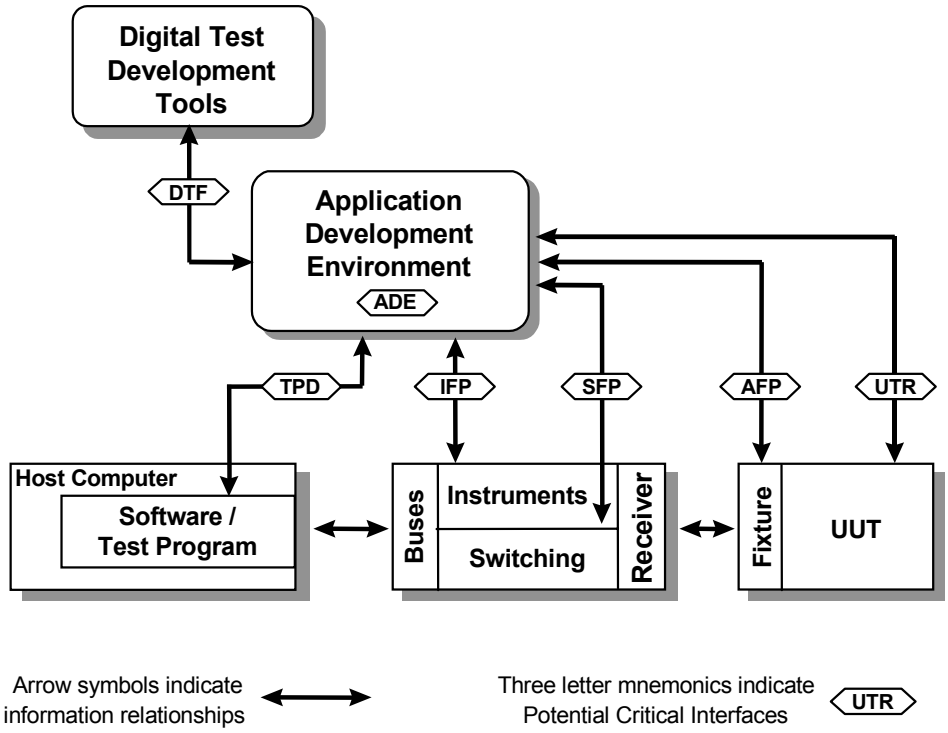


Figure CS.ATS-4: Test Product Sets Development Interfaces

- **Multimedia Formats (MMF)** denotes the formats used to convey text, audio, video, and three-dimensional physical model information from multimedia authoring tools to the Application Development Environment (ADE), Application Execution Environment, and host framework.
- **Network Protocol (NET)** is the protocol used to communicate with external environments, possibly over a Local or Wide Area Network. The software protocol used on the CXE hardware interface is represented by the NET software interface.
- **Resource Adapter Interface (RAI)** is the interface through which instrument drivers accept commands from, and return results to, test procedures or runtime services serving the Test Program.
- **Runtime Services (RTS)** denotes the services needed by a TPS not handled by the services supplied by the DRV, FRM, GIC, and NET, (e.g., error reporting, data logging).
- **Test Program to Operating System (TOS)** denotes system calls to the host OS made directly from the TPS.

The interfaces depicted in the development view of Figure CS.ATS-4 are listed alphabetically by mnemonic below:

- **Application Development Environments (ADE)** is the interface by which the test engineer creates and maintains a TPS, whether captured in the form of a text or graphical language.
- **Adapter Function and Parametric Data (AFP)** is the information and formats used to define to the ADE the capabilities of the test fixture, how the capabilities are accessed, and the associated performance parameters.

- **Instrument Function and Parametric Data (IFP)** is the information and formats used to define to the ADE the load, sense, and drive capabilities of the instruments; how these capabilities are accessed; and the associated performance parameters.
- **Switch Function and Parametric Data (SFP)** is the information and formats used to define to the ADE the interconnect capabilities of the switch matrix, how these capabilities are accessed, and associated performance parameters.
- **Test Program Documentation (TPD)** is a plain-language representation of information about the TPS for use by the TPS maintainer.
- **UUT Test Requirements (UTR)** is the information and formats used to define to the ADE the load, sense, and drive capabilities that must be applied to the UUT to test it, including the minimum performance required for a successful test.

CS.ATS.1.6 Subdomain Organization

The ATS Subdomain consists of three main sections. Figure CS.ATS-1 contains the overview, Figure CS.ATS-2 contains the additions to the JTA Core service areas for ATS, and Figure CS.ATS-3 contains the domain-specific service areas for ATS. A list of sources is provided in . In cases where the ATS Subdomain does not address an interface to be used in an ATS, the JTA takes precedence. In cases where the JTA and ATS Subdomain specify different standards for the same interface, the ATS Subdomain takes precedence.

CS.ATS.1.7 Configuration Management

Configuration management of the ATS Subdomain will be the responsibility of the joint service ARI. All changes will be approved by the ATS EAO with coordination from the ATS Management Board (AMB).

CS.ATS.2 Additions to the JTA Core

CS.ATS.2.1 Introduction

The standards in the ATS Subdomain apply in addition to the standards in the Combat Support Domain and the JTA Core.

CS.ATS.2.2 Information Processing Standards

CS.ATS.2.2.1 Introduction

CS.ATS.2.2.2 Mandated Standards

CS.ATS.2.2.2.1 Data Interchange Services

CS.ATS.2.2.2.1.1 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 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 in this version of the JTA.

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

CS.ATS.2.2.2.1.2 Digital Test Data Formats

Digital Test Data Formats (DTFs) describe the sequence of logic levels necessary to test a digital 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 in this version of the JTA:

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

CS.ATS.2.2.3 Emerging Standards

CS.ATS.2.2.3.1 Data Interchange Services

CS.ATS.2.2.3.1.1 Resource Adapter Interface

The Resource Adapter Interface (RAI) provides a generic method for obtaining instrumentation services. These services isolate TPSs from test instruments by allowing test requirements to be described in TPSs rather than instrument-specific functions or commands that would tie TPSs to specific instruments. The RAI makes it easier to interchange instruments and instrument drivers, and allows virtual instruments to be developed. DoD is working with industry consortiums such as the VXI plug&play Systems Alliance and the Interchangeable Virtual Instruments Foundation to develop a common solution.

The following standards are emerging:

- VPP-3.1, VXI plug&play Systems Alliance: Instrument Drivers Architecture and Design Specification Revision 4.1 December 4, 1998.
- VPP-3.2, VXI plug&play Systems Alliance: Instrument Driver Functional Body Specification Revision 5.0 December 4, 1998.
- VPP-3.3, VXI plug&play Systems Alliance: Instrument Driver Interactive Developer Interface Specification Revision 3.0 December 4, 1998.
- VPP-3.4, VXI plug&play Systems Alliance: Instrument Driver Programmatic Developer Interface Specification Revision 2.2 December 4, 1998.

Interchangeable Virtual Instruments (IVI) Foundation Standards:

- IVI-4 Aug 98: IviScope Class.
- IVI-5 Aug 98: IviDmm – Digital Multimeter Class.
- IVI-6 Aug 98: IviFGen – Function Generator/Arbitrary Waveform Generator Class.
- IVI-7 Aug 98: IviPower – Power Supply Class.
- IVI-8 Aug 98: IviSwitch – Switch Matrix/Multiplexor Class.

CS.ATS.2.2.3.1.2 Diagnostic Processing Standards

The diagnostic processing interface resides between the test procedure or runtime services supporting the TPS and a diagnostic reasoner, diagnostic controller, or other diagnostic process. Diagnostic tools

are most frequently encountered in one of three forms: expert systems, decision-tree systems, and model-based reasoners. Other diagnostic tools are expert systems known as the Fault Isolation System and the Expert Missile Maintenance Advisor; decision-tree systems including Weapon System Testability Analyzer, System Testability and Maintenance Program, System Testability Analysis Tool, and AUTOTEST; and model-based reasoners including Intelligent-Computer-Aided Test, Portable Interactive Troubleshooter, Artificial-Intelligence Test, and Adaptive Diagnostic System.

Standardization in this area would allow tools to be written that can translate test strategy information to various test programming languages. Additionally, the tools would be interchangeable since one could use any tool to obtain the same output source code.

The following standards are emerging:

- IEEE 1232-1998, Artificial Intelligence Exchange and Service Tie to All Test Environments (AI-ESTATE) Overview and Architecture.
- IEEE 1232.1-1997, Trial Use Standard for AI-ESTATE Data and Knowledge Specification.
- IEEE 1232.2-1998, Trial Use Standard for AI-ESTATE Service Specification.

CS.ATS.2.2.3.1.3 UUT Test Requirements Data Standards

High re-host costs in the past have been associated with the failure to record or preserve the signal-oriented action capabilities *as required* as opposed to *as used.* This problem is most visible in the allocation phase of TPS development. When a TPS is transported or re-hosted, the resources requested by the TPS must be allocated to assets in the target ATS. This task would be simplified if UUT test requirements were available in the form of load specifications, measurement requirements, and stimuli requirements that must appear at the UUT interface.The following standard is emerging:

- IEEE Computer Society Test Technology Technical Committee, Test Requirements Model (TeRM).

CS.ATS.2.3 Information Transfer Standards

CS.ATS.2.3.1 Introduction

CS.ATS.2.3.2 Mandated Standards

CS.ATS.2.3.2.1 Instrument Communication Manager Standards

The 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 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, Hewlett-Packard and National Instruments—the two 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, 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 specification is mandated:

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

CS.ATS.2.3.3 Emerging Standards

CS.ATS.2.3.3.1 Maintenance Test Data and Services

Maintenance Test Data and Services (MTDs) provide a standard representation of maintenance data in the test environment. MTD enhances runtime execution of the test program by capturing and using information developed during maintenance activities. This directly interfaces with the DIA interface by providing information that can supplement diagnostic capabilities.

The following standards are emerging:

- IEEE P1522, IEEE Testability Standard.
- IEEE 1545-1999, Trial Use Standard for Parametric Data Logging and Format.

CS.ATS.2.3.3.2 Product Design Data

Product Design Data (PDD) originates in the design process and is needed for the development and sustainment of test and diagnostics. PDD includes information about structures that are present in the product solely or principally to support test and diagnostics and facilitates the transfer of information from CAD workstations to the TPS development, reducing errors and development time. PDD supports the back-annotation of test and maintenance information into the design environment, reducing sustainment costs.

The following standard is emerging:

- ANSI/EIA 682:1996, EDIF Electronic Design Interchange Format, Version 399, Reference Manual and Information Model.

CS.ATS.2.3.3.3 Built-In Test Data

Built-in Test Data (BTD) provides a standard representation of Built-in Test (BIT) data into the test environment. BTD will improve runtime execution of test programs by providing guidance to the diagnostic services within an ATS. During TPS development, candidate BIT requirements can be evaluated by contrasting the impact on design and production against maintenance and diagnostic test. Cost-effective BIT requirements can then be imposed as design constraints. New initiatives in the area of BIT architecture and information exchange mechanisms are also being evaluated.

The following standards are emerging:

- IEEE 1149.1-1990, IEEE Standard Test Access Port and Boundary-Scan Architecture.
- IEEE P1149.4-1999, Mixed-Signal Test Bus.
- IEEE 1149.5-1995, IEEE Standard for Module Test and Maintenance Bus (MTM-Bus) Protocol.
- IEEE 1545-1999, Standard for Parametric Data Log Format, 1999.

CS.ATS.2.4 Information Modeling, Metadata, and Information Exchange Standards

CS.ATS.2.4.1 Introduction

CS.ATS.2.4.2 Mandated Standards

There are currently no mandated standards applicable to the ATS Subdomain with respect to Information Modeling, Metadata, and Information Exchange Standards as specified in Section 2.4 of the JTA.

CS.ATS.2.4.3 Emerging Standards

There are currently no emerging standards identified in this section of the ATS Subdomain.

CS.ATS.2.5 Human-Computer Interface Standards

CS.ATS.2.5.1 Introduction

CS.ATS.2.5.2 Mandated Standards

There are currently no mandated standards applicable to the ATS Subdomain with respect to Human-Computer Interface Standards as specified in Section 5 of the JTA.

CS.ATS.2.5.3 Emerging Standards

There are currently no emerging standards identified in this section of the ATS Subdomain.

CS.ATS.2.6 Information Security Standards

CS.ATS.2.6.1 Introduction

CS.ATS.2.6.2 Mandated Standards

There are currently no mandated standards applicable to ATS with respect to Information Security as specified in Section 6 of the JTA.

CS.ATS.2.6.3 Emerging Standards

There are currently no emerging standards identified in this section of the ATS Subdomain.

CS.ATS.3 Subdomain-Specific Service Areas

CS.ATS.3.1 Software Engineering Services

There are currently no mandated or emerging standards identified in this section.

CS.ATS.3.2 Data/Information Services

CS.ATS.3.2.1 Introduction

CS.ATS.3.2.2 Mandated Standards

This version of the ATS Subdomain does not contain any domain-specific mandated standards in the area of data/information services.

CS.ATS.3.2.3 Emerging Standards

This version of the ATS Subdomain does not contain any domain-specific emerging standards in the area of data/information services.

CS.ATS.3.3 Platform/Environment Services

CS.ATS.3.3.1 Introduction

CS.ATS.3.3.2 Mandated Standards

CS.ATS.3.3.2.1 System Framework Standards

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:

- Compatible ADEs.
- Instrument Drivers.
- Operating System.
- Required Documentation and Installation Support.
- Requirements for the Control Computer Hardware.
- Soft Front Panel.
- VISA Interface and I/O Software.
- VXI Instruments, VXI slot0, System Controller, VXI Mainframe.

A system designed using a VXI-plug&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, VXI plug&play System Alliance System Frameworks Specification, Revision 4.0, 29 January 1996.

CS.ATS.3.3.3 Emerging Standards

CS.ATS.3.3.3.1 Receiver/Fixture Interface

The Receiver/Fixture (RFX) and generic pin map interfaces represent a central element of the ATS through which the majority of stimulus and measurement reach the UUT. Standardization of the RFX and pin map allows the same fixture to be used on multiple ATSs. A standard pin map restricts the types of signals present at different positions on the receiver. Standardization of this interface increases the interoperability of test program sets, resulting in lower re-host costs.

The following standard is emerging:

- IEEE P1505, Receiver Fixture Interface (RFI) Standard.

CS.ATS.3.3.3.2 Switching Matrix Interface

The Switching Matrix (SWM) interface and ATS receiver/fixture pin map represent a central element of the ATS for connecting ATS instrumentation to the UUT through a switch matrix. The SWM allows a variety of instruments to be connected to multifunction terminals identified by a standard receiver/fixture pin map. The combination of standardizing the SWM interface and a common

receiver/fixture pin map gives the ATS the capability to accommodate any fixture that conforms to the pin map. Standardization of the SWM interface and receiver/fixture pin map increases interoperability by ensuring that ATS instruments needed to test a UUT can be switched to pins required by the fixture.

The following standard is emerging:

– IEEE P1552-1999, Standard Architecture for Test Systems (SATS).

CS.ATS.3.3.4 Other Interfaces

The interfaces described in this section are provided for completeness of the ATS Subdomain and to make readers aware that these interfaces have been addressed. Standards for these interfaces are not mandated, because they were not found to be key for the generic open system architecture for ATS.

CS.ATS.3.3.4.1 Computer Asset Controller Interface

The Computer Asset Controller (CAC) interface describes the communication paths between the host computer and instrument controllers in a distributed system. These interfaces may be internal or external to the host computer. Examples of internal interfaces are Industry Standard Architecture (ISA) and Peripheral Component Interface (PCI). Examples of external interfaces are IEEE-488, RS-232, Ethernet, Multisystem Extension Interface, and Modular System Interface Bus.

CS.ATS.3.3.4.2 Host Computer Interface

The Host Computer (HST) interface describes the processing architecture of the primary control computer in which the TPS is executed and through which the operator interfaces. Portions of the HST interface affect the interoperability of ATS. These requirements are included in the Frameworks software interface.

CS.ATS.3.3.4.3 Instrument Control Bus Interface

The Instrument Control Bus (ICB) interface describes the connection between the host computer or instrument controller and the test and measurement instruments in the ATS. Examples of these interfaces are IEEE-488, VME, and VME Extensions for Instrumentation (VXI).

CS.ATS.3.3.4.4 Instrument Command Language

The Instrument Command Language (ICL) interface describes how instrument commands and results are expressed as they enter or leave test and measurement instruments. The requirements for this interface are satisfied by the DRV and GIC interfaces.

CS.ATS.3.3.4.5 Application Development Environments

The ADE interface describes how the test engineer creates and maintains a TPS, whether it is captured in the form of a text or graphical language. This interface was not mandated, because the requirements for the ADE are restricted by the FRM interface.

Page intentionally left blank.

CS.DTS: Defense Transportation System Subdomain

CS.DTS.1 Subdomain Overview

CS.DTS.1.1 Purpose

The Defense Transportation System (DTS) Subdomain for the Combat Support Domain identifies additions to standards, interfaces, and service areas contained in the Department of Defense (DoD) Joint Technical Architecture (JTA) Core and Combat Support Domain that pertain to the DTS. Also included are additional standards central to the interoperability of existing DTS information systems.

CS.DTS.1.2 Background

The Defense Transportation System is an integrated cargo- and personnel-delivery system providing worldwide transportation functions for DoD. It consists of 35 core information systems with interfaces to countless DoD, Federal, state government and law-enforcement agencies nationwide. The DTS must be able to readily exchange information with commercial suppliers. Information concerning the 35 DTS systems can be found in the Defense Transportation System Enterprise Architecture, Version 1.0, 31 August 1999 at: <https://business.transcom.mil/J6/j6a/arch1.html> (For use by .mil addresses only).

CS.DTS.1.3 Subdomain Description

The Transportation System Subdomain includes the information systems, information, personnel, and facilities engaged in providing transportation support functions within DoD. These consist of component systems that support discrete functional areas within the DTS subdomain, such as:

- Modeling and Simulation
- Financial billing, payment, and tracking
- Transport of cargo and personnel

CS.DTS.1.4 Scope and Applicability

This subdomain applies to all new and existing information systems that make up the Defense Transportation System including upgrades to systems. The standards specified in the JTA Core, the Combat Support Domain, and the Modeling and Simulation Domain, combined with those in this document, comprise the minimum set of standards for the DTS.

CS.DTS.1.5 Technical Reference Model

The Defense Transportation System Subdomain uses the technical reference model specified in the JTA.

CS.DTS.1.6 Subdomain Organization

This subdomain consists of three main sections. The first section provides an overview, the second identifies additions to the standards in the JTA Core and the Combat Support Domain, and the third identifies DTS subdomain-specific service areas.

CS.DTS.2 Additions to JTA Core and Combat Support Domain

CS.DTS.2.1 Introduction

This section identifies additional standards (mandatory and emerging) unique to the DTS subdomain of the Combat Support Domain.

CS.DTS.2.2 Information Processing Standards

CS.DTS.2.2.1 Introduction

CS.DTS.2.2.2 Mandated Standards

CS.DTS.2.2.2.1 Product Data Interchange

To promote interoperability among military activities and commercial vendors, DoD has adopted standards endorsed by the commercial industry in lieu of developing unique military standards. The current DoD standards include those adopted for the linear bar code (Code 39 approved November 1982) and 2D bar code (PDF-417, approved July 1995).

Bar code standards are used to easily identify packages and products. Linear bar codes such as AIM BC-1 have limited data storage capability, typically a maximum 17 characters. A two-dimensional (2D) material-handling standard was developed to allow for greater storage, up to 1,850 characters. 2D bar codes can also sustain considerable damage and still be read. ANSI MH10.8.3M describes the use of two-dimensional symbols (e.g., PDF-417) in conjunction with unit loads and transport packages to convey data between trading partners. Additionally, it specifies the structure, syntax, and coding of dates when using two-dimensional symbols. The following standard is mandated:

- PDF-417, as profiled by ANSI MH10.8.3M-1996, Material Handling – Unit Loads and Transport Packages – Two-Dimensional Symbols.

PDF-417 answers the need to capture, store, and transfer large amounts of data inexpensively. It can exchange complete data files (such as text, numerics, or binary) and encode graphics, fingerprints, shipping manifests, electronic data interchange (EDI) messages, equipment calibration instructions, and much more. It provides a powerful communications capability— without the need to access an external database.

CS.DTS.2.3 Information Transfer Standards

There are no mandated or emerging standards for the DTS Information Transfer Standards Section.

CS.DTS.2.4 Information Modeling, Metadata, and Information Exchange Standards

There are no mandated or emerging standards for the DTS Information Modeling, Metadata, and Information Exchange Standards Section.

CS.DTS.2.5 Human-Computer Interface Standards

There are no mandated or emerging standards for the DTS Human-Computer Interface Standards Section.

CS.DTS.2.6 Information Security Standards

CS.DTS.2.6.1 Introduction

CS.DTS.2.6.2 Mandated Standards

There are no mandated standard for the DTS Information Security Section.

CS.DTS.2.6.3 Emerging Standards

CS.DTS.2.6.3.1 Internetworking Security Standards

Secure Shell is a protocol used to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. The following Secure Shell standards are emerging:

- draft-IETF-secsh-transport-07.txt, SSH Transport Layer Protocol, May 2000.
- draft-IETF-secsh-userauth-07.txt, SSH Authentication Protocol, May 2000.
- draft-IETF-secsh-connect-07.txt, SSH Connection Protocol, May 2000.

CS.DTS.3 Subdomain-Specific Service Areas

There are no subdomain-specific service areas for the Defense Transportation System Subdomain.

Page intentionally left blank.

CS.MED: Medical Subdomain

CS.MED.1 Subdomain Overview

CS.MED.1.1 Purpose

The Medical (MED) Subdomain identifies additions to the standards, interfaces, and service areas contained in the Department of Defense (DoD) Joint Technical Architecture (JTA) Core and Combat Support Domain that pertains to medical systems. These additions are common to the majority of systems in the Medical Subdomain and support the interoperability requirements of those systems.

CS.MED.1.2 Background

The Military Health System (MHS), formerly the Military Health Services System (MHSS), is an integrated healthcare delivery system that provides health care to its beneficiary population largely consisting of active-duty personnel and their dependents. It is a global enterprise composed of over 600 military treatment facilities located around the world. The dynamic nature of the MHS, together with the mobility of the beneficiary community, makes it important to ensure that the right information is in the right place at the right time. Furthermore, the MHS requires the ability to exchange this information within DoD, and with other Federal agencies and industry.

The healthcare enterprise is a unique and rapidly evolving industry. Because of this changing environment, it becomes even more critical that the MHS maintain the ability to readily exchange information both within and outside DoD. Within this medical subdomain are established and emerging standards that will be building blocks used in the design, development, and integration of information systems. Standardization is a key enabler within the strategic direction of the MHS information management program to provide support for the business needs of the military healthcare enterprise.

CS.MED.1.3 Subdomain Description

The Medical Subdomain includes the information systems, information, personnel, and facilities engaged in providing healthcare and medical support functions within DoD. These consist of component systems that support discrete functional areas within the Medical Subdomain, such as:

- Clinical: provision and management of healthcare services.
- Logistics: provision of materiel, facilities, equipment, and technology supporting delivery and management of healthcare services.
- Resources: management of financial and human resources and oversight of managed healthcare.
- Executive Information/Decision Support: oversight and coordination of enterprise-level operations and planning.
- Theater: delivery of healthcare services in a contingency situation.
- Infrastructure: provision and management of shared MHS resources.

These information systems provide the ability to capture, store, transmit, and process medical information at military treatment facilities and other sites around the world. In addition, they interface with commercial medical service providers.

CS.MED.1.4 Scope and Applicability

This Subdomain applies to all new and upgraded medical information systems.

The standards specified in the JTA Core and the Combat Support Domain to the JTA, combined with those in this Subdomain, comprise the minimum set of standards for the MHS.

CS.MED.1.5 Technical Reference Model

The Medical Subdomain uses the DoD Technical Reference Model, Version 1.0, 5 November 1999, as the basis for its technical reference model view.

CS.MED.1.6 Subdomain Organization

This Subdomain consists of two main sections. The first section provides an overview. The second identifies additions to the standards in the JTA Core and the Combat Support Domain for the Medical Subdomain.

CS.MED.2 Additions to JTA Core and Combat Support Domain

CS.MED.2.1 Introduction

This section identifies additional standards (mandatory and emerging) unique to the Medical Subdomain of the Combat Support Domain.

CS.MED.2.2 Information Processing Standards

CS.MED.2.2.1 Introduction

CS.MED.2.2.2 Mandated Standards

The following medical-specific standards concerning medical Electronic Data Interchange (EDI), retail pharmacy claims EDI, medical still imagery data interchange, and medical information exchange have been identified by the Medical Subdomain in addition to the standards found in the JTA Core and CS.2.2.1 of the Combat Support Domain.

CS.MED.2.2.2.1 Medical Electronic Data Interchange

Health Level Seven (HL7) is a standard for EDI in healthcare environments. It standardizes the format and protocol for the exchange of formatted messages containing medical data among medical software applications. It is to be used for the interchange of medical data, specifically patient records and clinical, epidemiological, and regulatory data. The use of the HL7 standards under these specified conditions is in accordance with Federal Information Processing Standard Publication (FIPS PUB) 161-2, EDI. HL7 standards should not be used for healthcare insurance administrative applications (such as for enrollments, claims, and claim payments) or the Government procurement cycle (such as registration of vendors, requests for quotes, purchase order, shipping notice, or payment advice).

The following standard is mandated for medical EDI:

- Health Level Seven (HL7), Version 2.3.1, Application Protocol for Electronic Data Exchange in Healthcare Environments, 1999.

CS.MED.2.2.2.2 Retail Pharmacy Claims Electronic Data Interchange

The National Council for Prescription Drug Programs (NCPDP) has published a standard for retail pharmacy claims EDI. This standard applies to the transmission of prescription drug and pharmaceutical care benefit/distribution and delivery information including online, real-time drug utilization review, and financial claims data between pharmacies and trading partners.

The following standards are mandated for retail pharmacy claims EDI:

- NCPDP Telecommunication Standard, Version 3.2, 1992.

- NCPDP Batch Transactions, Version 1.0, 1996.

CS.MED.2.2.2.3 Medical Still Imagery Data Interchange

The Digital Imaging and Communications in Medicine (DICOM) standard describes a means for formatting and exchanging images and associated information. It applies to the operation of the interface used to exchange data among medical imaging devices.

The DICOM standard was developed jointly by the medical user community, represented by the American College of Radiology (ACR), and medical equipment manufacturers, represented by the National Electrical Manufacturers Association (NEMA). It has since been adopted by the European Committee for Standardization (CEN) Technical Committee (TC) 251 and the Japanese Industry Association for Radiation Apparatus (JIRA).

The following standard is mandated for medical still imagery data interchange:

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

CS.MED.2.2.2.4 Medical Information Exchange Standards

There are many widely accepted standards for the format and content of medical information to be exchanged among medical-application software entities. In particular, the International Society for Blood Transfusion (ISBT) has developed a standard, ISBT 128, for bar-coding blood donor label information on blood bags. Also, the Universal Product Number (UPN) System, published by the Health Industry Business Communications Council, is a standard for identifying medical and surgical products in the supply chain. Reference the following Health Industry Business Communications Council Web site for more information: <http://www.hibcc.org/upndb.htm>.

The following medical information exchange standards are mandated for the specific purposes indicated:

- ISBT 128, Bar Code Symbology and Application Specification for Labeling of Whole Blood and Blood Components, 1995 (for bar-coding blood donor number label information on blood bags).
- Universal Product Number (UPN) System, 1996 (for identifying medical and surgical products in the supply chain).

CS.MED.2.2.3 Emerging Standards

Emerging standards for commercial EDI that are applicable to the Medical Subdomain are discussed below. These standards are added to the emerging information processing standards specified in 2.3.1 of the JTA Core and Section CS.2.2.3.1 of the Combat Support Domain.

CS.MED.2.2.3.1 Commercial Electronic Data Interchange

Final rules implementing the Health Insurance Portability and Accountability Act (HIPAA) will require the use of revised versions of standards for health insurance EDI developed by the ANSI ASC X12 Insurance Subcommittee (X12N).

The following standards are emerging for commercial EDI of some specific transactions for health insurance as published in the Federal Register/Vol. 63, No. 88/Thursday, May 7, 1998/Proposed Rules:

- X12N 270, Version 004010X092, Health Care Eligibility/Benefit Inquiry.
- X12N 271, Version 004010X092, Health Care Eligibility/Benefit Information Response.

- X12N 276, Version 004010X093, Health Care Claim Status Request.
- X12N 277, Version 004010X093, Health Care Claim Status Response.
- X12N 278, Version 004010X094, Health Care Services Request for Review and Response.
- X12N 820, Version 004010X061, Payroll Deducted and Other Group Premium Payment for Insurance Products.
- X12N 834, Version 004010X095, Health Care Benefits and Enrollment and Maintenance.
- X12N 835, Version 004010X091, Health Care Claim Payment/Advice.
- X12N 837, Version 004010X096, Health Care Claim: Institutional.
- X12N 837, Version 004010X097, Health Care Claim: Dental.
- X12N 837, Version 004010X098, Health Care Claim: Professional.

Reference the following Federal web sites for more information on EDI: <http://www.ec.fed.gov/> and <http://www.edi.itsi.disa.mil/>.

CS.MED.2.2.3.2 Retail Pharmacy Claim Electronic Data Interchange

Final rules implementing the Health Insurance Portability and Accountability Act (HIPAA) require the use of National Council for Prescription Drug Programs (NCPDP) standards for the transmission of prescription drug and pharmaceuticals.

For all health plans (with annual receipts greater than $5 million), including TRICARE, the expected compliance date for use of the HIPAA standard electronic transactions and code sets is no later than 24 months after the effective date of the final rule. (The effective date of the final rule will be 60 days after the final rule is published in the Federal Register.)

The following NCPDP standard is emerging:

- NCPDP Telecommunications Standard, Version 5.1, 1999.

CS.MED.2.3 Information Transfer Standards

CS.MED.2.3.1 Introduction

CS.MED.2.3.2 Mandated Standards

There are no information transfer standards applicable to the Medical Subdomain beyond those in 3.2 of the JTA Core and CS.2.3 of the Combat Support Domain.

CS.MED.2.3.3 Emerging Standards

There are no emerging Information Transfer standards applicable to the Medical Subdomain beyond those in 3.3 of the JTA Core and CS.2.3 of the Combat Support Domain.

CS.MED.2.4 Information Modeling, Metadata, and Information Exchange Standards

CS.MED.2.4.1 Introduction

CS.MED.2.4.2 Mandated Standards

There are no information modeling, metadata, and information exchange standards applicable to the Medical Subdomain beyond those in 4.2 of the JTA Core and CS.2.4 of the Combat Support Domain.

CS.MED.2.4.3 Emerging Standards

There are no emerging information modeling, metadata, and information exchange standards applicable to the Medical Subdomain beyond those in 4.3 of the JTA Core and CS.2.4 of the Combat Support Domain.

CS.MED.2.5 Human-Computer Interface Standards

CS.MED.2.5.1 Introduction

CS.MED.2.5.2 Mandated Standards

There are no mandated standards for human-computer interfaces (HCIs) applicable to the Medical Subdomain beyond those in 5.2 of the JTA Core and CS.2.5 of the Combat Support Domain.

CS.MED.2.5.3 Emerging Standards

There are no emerging standards for HCIs applicable to the Medical Subdomain beyond those in 5.3 of the JTA Core and CS.2.5 of the Combat Support Domain.

CS.MED.2.6 Information Security Standards

CS.MED.2.6.1 Introduction

CS.MED.2.6.2 Mandated Standards

There are no mandated information security standards applicable to the Medical Subdomain beyond those specified in 6.2 of the JTA Core and CS.2.6 of the Combat Support Domain. However, the *Military Health Services System (MHSS) Automated Information System (AIS) Security Policy Manual*, Version 1.0, April 1996, published by OASD(HA), contains information security policies, procedures, and guidance (not standards) for the MHS. System configuration and administration in accordance with the latest version of this document is necessary to ensure the secure operation of the MHS.

CS.MED.2.6.3 Emerging Standards

There are no emerging information security standards applicable to the Medical Subdomain beyond those specified in 6.3 of the JTA Core and CS.2.6 of the Combat Support Domain. However, as required by HIPAA, Federal regulations governing the security and privacy of medical data are pending.

Page intentionally left blank.

M&S: Modeling and Simulation Domain

M&S.1 Domain Overview

M&S.1.1 Purpose

The Modeling and Simulation (M&S) Domain identifies additions to the JTA Core elements (standards, interfaces, and service areas) listed in the JTA Core. These additional standards are key to the Interoperability of M&S within DoD among themselves and real-world systems.

M&S.1.2 Background

In 1992, DoD established a vision for modeling and simulation, as stated in the DoD M&S Master Plan. "Defense modeling and simulation will provide readily available, operationally valid environments for use by the DoD Components

- To train jointly, develop doctrine and tactics, formulate operational plans, and assess warfighting situations.
- To support technology assessment, system upgrade, prototype and full-scale development, and force structuring.

"Common use of these environments will promote a closer interaction between the operations and acquisition communities in carrying out their respective responsibilities. To allow maximum utility and flexibility, these modeling and simulation environments will be constructed from affordable, reusable components interoperating through an open systems architecture" (Executive Council for Modeling & Simulation).

Department of Defense Directive 5000.59*,* DoD Modeling and Simulation (M&S) Management, January 4, 1994; and DoD 5000.59-P, DoD Modeling and Simulation (M&S) Master Plan (MSMP), October 1995, outline DoD policies, organizational responsibilities, and management procedures for M&S and provide a comprehensive strategic plan to achieve DoD's vision of readily available, authoritative, interoperable, and reusable simulations.

Objective 1 of the DoD MSMP 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 the interoperability of all types of simulations among themselves and with C4I systems, as well as to facilitate the reuse of M&S components." The efficient and effective use of models and simulations across DoD and supporting industries requires a common technical framework for M&S to facilitate interoperability and reuse. This common technical framework consists of:

- A high-level architecture (HLA) to which simulations must conform.
- Conceptual models of the mission space (CMMS) to provide a basis for the development of consistent and authoritative M&S representation.
- Data standards to support common understanding of data across models, simulations, and real-world systems.

The HLA is a progression from the previous architectures and associated standards that have been developed and used successfully for specific classes of simulation. These include Distributed Interactive Simulation (DIS) protocol standards, which support networked, real-time, platform-level virtual simulation; and the Aggregate-Level Simulation Protocol (ALSP), which is used to support distributed, logical-time, constructive simulations. The HLA provides a common architecture for all

classes of simulation and, consequently, the HLA supersedes both the DIS and ALSP standards. Transition of simulations from use of other standards is underway in accordance with DoD M&S policy.

M&S.1.3 Domain Description

This domain provides a set of standards affecting the definition, design, development, execution, and testing of models and simulations. DoD modeling and simulation ranges from high-fidelity engineering simulations to highly aggregated, campaign-level simulations involving joint forces. Increasingly, DoD and supporting industries are integrating and operating a mix of computer simulations, actual warfighting systems, weapon 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 life cycle. Figure M&S-1 shows the position of the M&S Domain in the JTA Hierarchy Model.

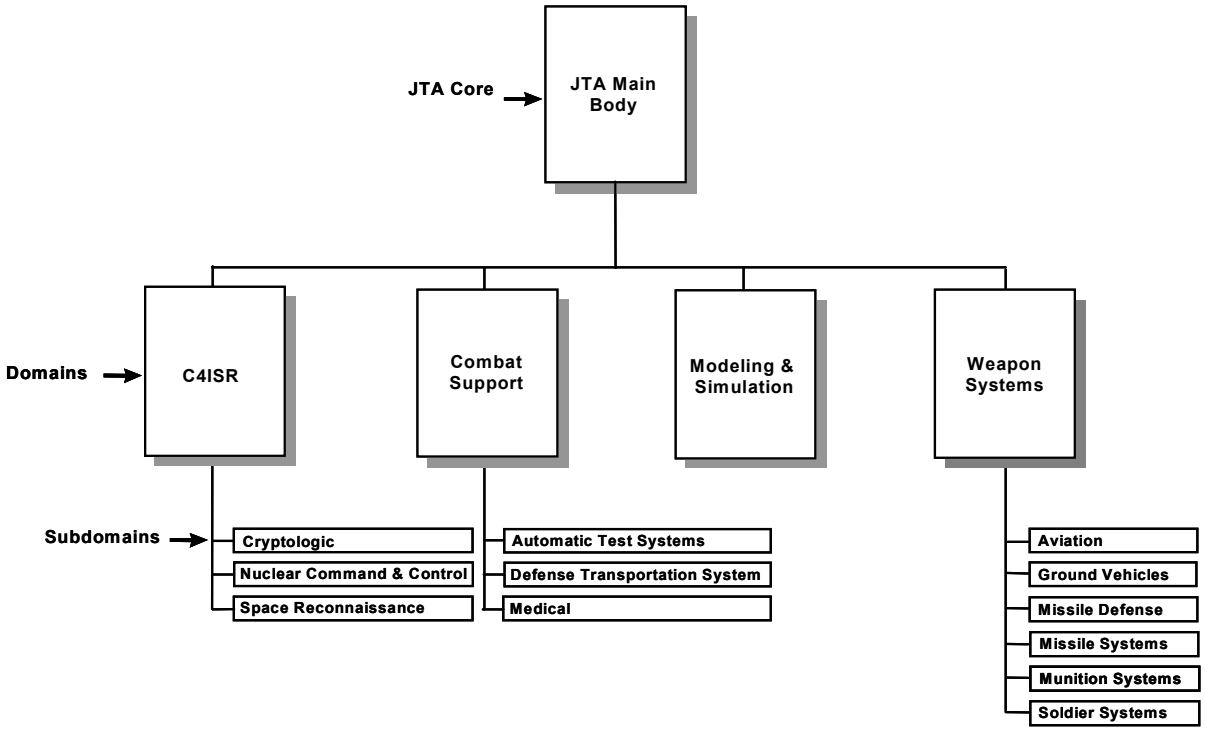


Figure M&S-1: JTA Hierarchy Model

M&S.1.4 Scope and Applicability

The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) in 1996 designated the HLA as the standard technical architecture for all DoD simulations. The HLA is a technical architecture that applies to all classes of simulations, including virtual simulations, constructive simulations, and interfaces to live systems. The virtual simulation class comprises human-in-the-loop simulators. The constructive simulation class includes wargames and other automated simulations that represent actions of people and systems in the simulation. The live simulation class includes C4I interfaces, weapon systems/platforms with embedded collective training, and instrumented ranges. The method of implementation is at the discretion of the responsible Service, Staff, or Agency.

M&S developed as an integral part of a weapon system or C4I system, or as an embedded simulation, will fall under the mandates of the JTA main body, this domain, and any other applicable domains. Interoperability of embedded simulations will be governed by this domain.

The HLA and related M&S standards listed here address those key technical aspects of simulation design necessary to foster interoperability and reuse, but avoid overly constraining implementation details. They are intended for use in simulations addressing a full range of training, analysis, and acquisition requirements, each of which may have different objectives that dictate different representational details, timing constraints, processing demands, etc. The M&S technical standards in this domain provide the framework within which specific systems, targeted against precise requirements, can be developed. While many of these systems will operate in computational environments considered standard and that fall within the spectrum of the other JTA standards, some may require massively parallel processing or other unique laboratory configurations, bringing with them their own set of requirements. Simulation developers should follow those standards required for the environment in which the simulation is implemented.

Mandates listed in this domain are in addition to those listed in the JTA Core.

M&S.1.5 Technical Reference Model

There is no separate Technical Reference Model established for the M&S Domain.

M&S.1.6 Domain Organization

The Modeling and Simulation Domain consists of three sections. M&S.1 contains the overview, Section M&S.2 contains those Information Technology mandated and emerging standards that are additions to the standards contained in the Core, and Section M&S.3 is reserved for those mandates for modeling and simulation that are domain-specific because they do not map directly to the Core service areas.

M&S.2 Additions to the JTA Core

M&S.2.1 Introduction

The following standards apply in addition to those found in the JTA Core. On September 10, 1996, the Under Secretary of Defense for Acquisition and Technology (USD[A&T]) designated the HLA as the standard technical architecture for all DoD simulations. The HLA, as mandated, is defined by the HLA Rules, the HLA Interface Specification, and the HLA Object Model Template Specification. Compliance criteria have been set forth in the compliance checklist, which was developed as part of the HLA, along with the HLA test procedures. These form the technical basis for HLA compliance. Current versions are listed and available at the Defense Modeling and Simulation Office Web site at <http://www.dmso.mil>.

M&S.2.2 Information Processing Standards

M&S.2.2.1 Introduction

In addition to those mandates for information processing standards described in Section 2 of the JTA, the following are unique mandates applicable to the Modeling and Simulation Domain.

M&S.2.2.2 Mandated Standards

M&S.2.2.2.1 HLA Framework and Rules

The HLA 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 the HLA Runtime Infrastructure (RTI) time management services, and certain restrictions on attribute ownership and updates. The following standard is mandated:

- U.S. Department of Defense, High-Level Architecture (HLA) – Rules, Version 1.3, 5 February 1998. (20 April 1998 Document Release).

M&S.2.2.2.2 HLA Federate 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.
- U.S. Department of Defense, High-Level Architecture Interface Specification, Version 1.3, dated 2 April 1998.

M&S.2.2.2.3 HLA Object Model Template

The HLA Object Model Template (OMT) 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. The HLA OMT 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. The following standard is mandated:

- U.S. Department of Defense, High-Level Architecture Object Model Template Specification, Version 1.3, 5 February 1998 (20 April 1998 document release).

M&S.2.2.3 Emerging Standards

The Standards Board of the Institute of Electronic and Electric Engineers (IEEE) voted on September 21, 2000, to accept the HLA as an IEEE standard. As a result of that decision, DMSO is building a Runtime Infrastructure (RTI) to the new HLA 1516.1 specification. Prior to use by the DoD it must be verified. In addition, DMSO produced tools will also be migrated to the 1516 specification. Therefore, the following standards are emerging:

- IEEE 1516-2000, IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Framework and Rules.
- IEEE P 1516.1-2000, IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Federate Interface Specification, DRAFT 1 dated 20 April 1998.
- IEEE P 1516.2-2000, IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Object Model Template (OMT) dated 5 February 1998 (20 April 1998 Document Release).

M&S.2.3 Information Transfer Standards

There are no additional Information Transfer Standards applicable to modeling and simulation beyond those specified in Section 3 of the JTA.

M&S.2.4 Information Modeling, Metadata, and Information Exchange Standards

M&S.2.4.1 Introduction

In addition to those mandated standards for Information Modeling, Metadata, and Information Exchange Standards described in 4.2 of the JTA, the following mandated standards are applicable to the Modeling and Simulation Domain.

M&S.2.4.2 Mandated Standards

M&S.2.4.2.1 Federation Execution Details Data Interchange Format

This Data Interchange Format (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 RTI and other HLA initialization tools. The Federation Execution Details (FED) DIF is part of the HLA Interface Specification referenced above. The following standard is mandated:

- Federation Execution Details Data Interchange Format, Version 1.3, February 1998.

M&S.2.4.2.2 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. The following standard is mandated:

- Object Model Template Data Interchange Format (OMT DIF), Version 1.3, February 1998.

M&S.2.4.2.3 Standard Simulator Database Interchange Format

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. The following standard is mandated:

- MIL-STD-1821, Standard Simulator Data Base (SSDB) Interchange Format (SIF) Design Standard, 17 June 1993, with Notice of Change 1, 17 April 1994, and Notice of Change 2, 17 February 1996.

M&S.2.4.3 Emerging Standards

M&S.2.4.3.1 Synthetic Environment Data Representation and Interchange Specification (SEDRIS)

SEDRIS facilitates interoperability among heterogeneous information technology applications by providing complete and unambiguous interchange of environmental data. The range of applications addressed in the SEDRIS development includes entertainment, training, analysis, and system acquisition and support for visual, computer-generated active elements, and sensor perspectives. In addition, SEDRIS provides a standard interface for GIS systems, which are key components in the generation of complex integrated databases for simulation applications. The SEDRIS data interchange specification supports the pre-runtime distribution and runtime specification of source data, three-dimensional models, and integrated databases that describe the physical environment for both simulation and operational use. The following SEDRIS standards are emerging:

- WD 18023: SEDRIS Functional Specification (including the SEDRIS Data Model, the Read and Write APIs, and the SEDRIS Transmittal Format), Version 1, 21 January 2000.
- WD 18024: SEDRIS Language Bindings: C, Version 1, 21 January 2000.
- WD 18025: Environmental Data Coding Specification (EDCS), Version 1, 21 January 2000.
- WD 18026: Spatial Reference Model (SRM), Version 1, 21 January 2000.

M&S.2.4.3.2 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 that 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 the 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 Model Data Dictionary process.

M&S.2.5 Human-Computer Interface Standards

There are no additional Human-Computer Interface standards applicable to modeling and simulation beyond those specified in Section 5 of the JTA.

M&S.2.6 Information Security Standards

There are no additional Information Security standards applicable to modeling and simulation beyond those specified in Section 6 of the JTA.

M&S.3 Domain-Specific Service Areas

There are no domain-specific services areas for the Modeling and Simulation Domain.

WS: Weapon Systems Domain

WS.1 Domain Overview

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.[1]

WS.1.1 Purpose

This identifies standards for the Weapon Systems (WS) Domain including information standards and analogous standards applicable to weapon systems.

WS.1.2 Background

This domain follows the JTA Core document structure to facilitate the identification and traceability of the Weapon Systems Domain additions to the standards mandated in the main body of the JTA. Therefore, the Weapon Systems Domain consists of three sections including: Domain Overview, Mandated Standards, and Emerging Standards.

Weapon Systems mandated standards result from consensus concerning the need for the standards and the maturity of their commercial implementations within the Weapon Systems Domain or within the majority of its subdomains.

Currently there are sections within the Weapon Systems Domain and its subdomains that do not specify mandated additions to the JTA Core. However, due to their hard real-time and embedded-system requirements, the Weapon Systems Subdomains are evaluating the available real-time standards for possible mandate as additions to each section of the JTA, where appropriate.

WS.1.3 Domain Description

Weapon systems have special attributes (e.g., timeliness, embedded nature, space and weight limitation), adverse environmental conditions, and critical requirements (e.g., survivability, low power/weight, and dependable hard real-time processing) that drive system architectures and make system hardware and software highly interdependent and interrelated. The position of the Weapon Systems Domain in the JTA Hierarchy Model is shown in Figure 1-3.

WS.1.4 Scope And Applicability

A domain is defined as a distinct functional area that can be supported by a family of systems with similar requirements and capabilities. The Weapon Systems Domain, in conjunction with the JTA Core, establishes the minimum set of rules governing the application of information technology between weapon systems, where 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 mission success[1]. The Weapon Systems Domain encompasses a subset of the JTA and the specific supporting standards profile. For the purposes of the JTA, the Weapon Systems Domain is that domain whose systems' 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 Weapon Systems Domain.

The Weapon Systems Domain is applicable to all weapon systems as defined in Joint Pub 1-02.

[1] Joint Pub 1-02, DoD Dictionary of Military and Associated Terms, 23 March 1994, as Amended through 1 September 2000.

For the purposes of the JTA, the Weapon Systems Domain is organized into subdomains to facilitate the identification of interoperability standards for common areas 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 upon 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 and therefore must consider the applicable standards from the pertinent subdomains. The current weapon systems subdomains are:

- **Aviation Subdomain** – Includes all DoD weapon systems on aeronautical platforms, except missiles—manned and unmanned, fixed-wing, and rotary-wing.
- **Ground Vehicle Subdomain** – Includes all DoD weapon systems on moving ground platforms, except missiles—wheeled and tracked, manned, and unmanned.
- **Missile Defense Subdomain** – Includes any system or subsystem (including associated Ballistic Missile/C4I systems) with a mission to detect, classify, identify, intercept, and destroy or negate the effectiveness of enemy aircraft or missiles before launch or while in flight so as to protect U.S. and coalition forces, people, and geopolitical assets.
- **Missile Systems Subdomain**– Includes Strategic and Theater Ballistic Missile Systems, Cruise Missile Systems, and rocket and missile systems used in diverse Battlefield Functional Areas including Fire Support, Close Combat, and Special Operations.
- **Munition Systems Subdomain** – Includes unmanned, remotely deployed target defeating systems that operate from a fixed position, provide/consume targeting data, have data links to control devices, and engage targets either autonomously or on demand.
- **Soldier Systems Subdomain** – Includes any system or subsystem integrating target location, target identification, target acquisition, enhanced survivability, navigation, position location, enhanced mobility, and command-and-control into a system worn or carried by an individual soldier in performance of assigned duties.

WS.1.5 DoD Technical Reference Model

WS.1.5.1 DoD TRM Views

The Weapon Systems Domain and subdomains use both the DoD Technical Reference Model (TRM) Service View and the Interface View, as described in 1.5. The Interface View is more applicable to real-time systems. Services are best described by the TRM Services View. Interface standardization in weapon systems is a goal of the Open Systems Joint Task Force (OSJTF) of DoD. Both views are needed to capture all of the standards required for the Weapon Systems Domain and subdomains to operate within the DoD enterprise.

Figure 1-4 depicts the two distinct views of the TRM. Both views are traceable to the POSIX Open Systems Environment (OSE) Reference Model. The Service View extends the POSIX model by decomposing its entities into the specific applications and services that support DoD information and computing systems. The Interface View is based on the Generic Open Architecture (GOA) framework (SAE AS 4893, 1 Jan. 1996) and provides a context for identifying the characteristics of exchanged information (logical interfaces) and the method or mechanism used for information transport (direct interfaces). A short explanation of the TRM is provided here; however, for more detail, readers are encouraged to review the TRM document.

The Interface View identifies both logical and direct interfaces. A logical interface defines requirements for peer-to-peer interchange of data. It identifies senders, receivers, data types, frequency of exchange, and formats. A direct interface identifies the characteristics of the information transfer medium. Simply stated, logical interfaces define *what* information is transferred; the direct interfaces define *how* the information is transferred. Logical interfaces are implemented with direct interfaces.

The Interface View expands the Application Platform entity within the POSIX model to include the three other layers: Systems Services Layer (which contains the Operating System Services and eXtended Operating System Services secondary layers), Resource Access Services Layer, and Physical Resources Layer. The Interface View includes the 4L, 3L, 2L, and 1L for peer-to-peer logical interfaces, and the 4D, 4X, 3X, 3D, 2D, and 1D direct interfaces. The Application Program Interface (API) of the POSIX model is synonymous with the 4D interface, while the External Environment Interface (EEI) is synonymous with the 1L and 1D interfaces treated as a pair. Thus the Interface View complements the Service View by expanding the Application Platform entity, and by providing language to describe both application-to-application logical interfaces, and the Application Platform-to-Application Platform logical interfaces (3L and 2L interfaces).

The Service View, unlike the Interface View, categorizes services available in the Applications Platform. The Application Platform service areas defined by the Service View include both runtime and pre-run-time services. The Service View addresses only 4D API interfaces and 1D/1L EEI interfaces. The Service View does not address 2L, 3L, or 4L peer-to-peer logical interfaces, 3X, 3D, or 2D direct interfaces, nor does it address the Resource Access Services Layer or the Physical Resources Layer.

Section WS.2 uses the Service View and identifies additions to the JTA Core standards, and WS.3 uses the layers identified in the Interface View as a context for classifying interface standards used in weapon system platforms. WS.2 and WS.3 both include emerging standards that represent current standards work within the Weapon Systems Domain.

WS.1.5.1.1 Performance Environment

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

WS.1.5.1.2 Application Hardware Environment

Within weapon systems, embedded-computing hardware and software components are highly interdependent in order to satisfy very demanding requirements. The TRM Service View often does not fit a general-purpose computing model very well. Therefore the TRM Interface View is used to capture such features as interconnect and open systems hardware standards.

WS.1.5.2 Hierarchy of TRM Views

In order to capture the diversity found in weapon subsystem design, a hierarchical approach to TRM Views is being established. From the TRM in Figure 1-4, the TRM Interface View will extend downward into the Weapon Systems Domain and subdomains to provide the basis for standards identification and traceability.

WS.1.6 Domain Organization

This domain is divided into three sections: the Overview in WS.1, the Additions to the JTA Core service areas in Section WS.2, and the domain-specific service areas and interfaces in WS.3. WS.2 follows the

JTA Core service-area structure. The structure of WS.3 will evolve as WS-specific service areas are identified and a common structure is coordinated among the other annexes.

WS.2 Additions to the JTA Core

WS.2.1 Introduction

The TRM Interface View provides for sufficient fidelity to identify critical functions, interfaces, and technical issues.

WS.2.2 Information Processing Standards

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

WS.2.2.1 Introduction

WS.2.2.2 Mandated Standards

There are no mandated standards for the Information Processing Standards section.

WS.2.2.3 Emerging Standards

WS.2.2.3.1 Operating System Services

The OSJTF is sponsoring and synchronizing Weapon Systems Domain involvement in the IEEE POSIX working groups. The following real-time-related standard is emerging:

- IEEE P1003.5f POSIX: Ada binding to 1003.21, January 1997.

WS.2.2.3.2 Real-Time Common Object Request Broker Architecture

The OMG Special Interest Group, Real-Time Common Object Request Broker Architecture (CORBA), is evaluating the need for real-time object-oriented standards and products to support real-time embedded systems. As more information becomes available from this group, the Weapon Systems Domain will consider adopting the standards as additions to the JTA information processing standards.

WS.2.3 Information Transfer Standards

There are no mandated or emerging standards for the Information Transfer Standards section.

WS.2.4 Information Modeling, Metadata, and Information Exchange Standards

This section fosters information exchange among Weapon Systems during their development and maintenance phases. During concept exploration and development, a large number 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.

WS.2.4.1 Introduction

WS.2.4.2 Mandated Standards

There are no mandated standards for the Information Modeling, Metadata, and Information Exchange standards.

WS.2.4.3 Emerging Standards

The following emerging standards are being considered for mandate by the Weapon Systems Domain as an addition to the JTA information modeling standards:

- 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.

WS.2.5 Human-Computer Interface Standards

This section provides a common framework for Human-Computer Interfaces (HCI) design and implementation in weapon systems. It complements and extends the DoD HCI Style Guide, Version 3.0, 30 April 1996. The objective is to standardize user interface design and implementation options across weapon systems, thus enabling applications within the Weapon Systems Domain to appear and behave consistently, resulting in higher productivity, shorter training time, and reduced development, operation, and support costs besides influencing commercial HCI development. This version mandates the design of graphical and character-based displays and controls for weapon systems.

In order to identify appropriate 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 HCIs 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 subdomain.

WS.2.5.1 Introduction

WS.2.5.2 Mandated Standards

There are no mandated standards additions for the Human-Computer Interface Standards section.

WS.2.5.3 Emerging Standards

The Weapon Systems Human-Computer Interface (WSHCI) Style Guide addresses guidelines applicable across most or all of the 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 U.S. Army document is proposed as the starting point to become the joint weapon system style guide and is an emerging standard:

- U.S. Army Weapon Systems Human-Computer Interface (WSHCI) Style Guide, Version 3, December 1999.

WS.2.6 Information Security Standards

There are no mandated or emerging standards for the Information Security Standards section.

WS.3 Domain-Specific Service Areas and Interfaces

WS.3.1 Introduction

The Interfaces View of the TRM, depicted in Figure 1-4, provides sufficient fidelity for identifying classes of interfaces to apply open systems interface standards to the design of real-time and embedded-hardware/software systems. The Interface View 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 TRM.

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

WS.3.2 Application Software Layer Interfaces

There are no additional mandated or emerging standards for the Application Software Layer Interfaces section.

WS.3.3 System Services Layer Interfaces

There are no additional mandated or emerging standards for the System Services Layer Interfaces section.

WS.3.4 Resource Access Services Layer Interfaces

There are no additional mandated or emerging standards for the Resource Access Services Layer Interfaces section.

WS.3.5 Physical Resources Layer Interfaces

WS.3.5.1 Introduction

WS.3.5.2 Mandated Standards

There are no mandated standards for the Physical Resources Layer Interfaces section.

WS.3.5.3 Emerging Standards

The following are being evaluated as emerging interface standards by the Weapon Systems Domain:

- IEEE P1386.1/D2.0, Physical/Environmental Layers for Peripheral Component Interface (PCI) Mezzanine Cards (PMC), April 1995.
- ATSC Document A/53, ATSC Digital Television Standard, 16 September 1995.

WS.3.6 Combat Identification 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 (approved Joint Combat Identification Master Plan, August 1995).

The increased lethality of weapon systems and the increase in the speed and ferocity with which air and land battles are fought have resulted in a greater need for capabilities that will aid warfighters in reducing fratricide. Positive visual identification of friends and foes (IFF) during battles fought under degraded natural and man-made conditions is difficult at best when opposing forces use dissimilar

equipment and tactics to those of our own forces. However, our modern world of changing alliances and the use of multi-national forces in United Nations (UN) peacekeeping efforts to quell geopolitical disturbances has made a difficult problem even tougher because friends and foes alike are now using identical combat platforms, creating a situational awareness (SA) nightmare.

WS.3.6.1 Identification Friend or Foe

The primary function of Identification Friend or Foe (IFF) is to establish the identity of all friendly systems within the surveillance volume of surface-to-air, air-to-air, and some air-to-ground Weapon System platforms. The need for Friend identification is to permit tactical action against all Foe (non-friendly) systems and to avoid tactical action against Friendly systems. This need is a key element in modern combat, as an object detected by a sensor, even beyond visual range, has to be identified and classified as early as possible so that, if necessary, either an appropriate defense can be prepared against the Foe or that steps can be taken to prevent the Friend from being engaged/attacked by Friendly forces.

WS.3.6.1.1 Introduction

WS.3.6.1.2 Mandated Standards

The following standards are mandated for new and upgraded Weapon Systems platforms requiring integrated or appliqué IFF capabilities:

- 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.

The following mandated standard provides a general description of required capabilities for military IFF systems:

- STANAG 4193, Part 1, Edition 2, 12 November 1990, with Amendment 1, 15 December 1997: NATO Standard Agreement Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders.

The following mandated standard defines the required anti-jamming capabilities of military IFF systems:

- STANAG 4193, Part 2, Edition 1, 12 November 1990 (SECRET): NATO Standard Agreement Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders.

The following mandated standard defines the required characteristics/capabilities of installed military IFF systems:

- STANAG 4193, Part 3, Edition 1, 12 November 1990, with Amendment 1, 31 January 1995: NATO Standard Agreement Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders.

The following mandated standard defines the required characteristics of military IFF systems to provide Mode S capabilities:

- STANAG 4193, Part 4, 28 November 1997: NATO Standard Agreement Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders.

WS.3.6.1.3 Emerging Standards

The following standard defines the required characteristics of military IFF systems to support the new Mode 5 capabilities:

– STANAG 4193 Part 5, Annex A through D, 4 September 1998 (SECRET NATO RESTRICTED): NATO Standard Agreement Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders.

WS.AV: Aviation Subdomain

WS.AV.1 Subdomain Overview

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 Aviation Subdomain include all DoD weapon systems on aeronautical platforms except missiles—manned and unmanned, fixed-wing and rotary-wing.

WS.AV.1.1 Purpose

This subdomain identifies standards for the Aviation Subdomain of the Weapon Systems Domain including information standards and analogous standards applicable to aviation systems.

WS.AV.1.2 Background

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

WS.AV.1.3 Subdomain Description

The subdomain description is given in Section WS.AV.1.

WS.AV.1.4 Scope And Applicability

This subdomain does not include any mandates at this time. Emerging standards are identified. Mandates are expected to be added in the next version of the JTA. Some proposed standards are identified.

WS.AV.1.5 Technical Reference Model

The technical reference model adopted for use in this subdomain is the Technical Reference Model (TRM), which is described in the Weapon Systems Domain. The TRM Service View and Interface View are used as applicable.

WS.AV.1.6 Subdomain Organization

This Subdomain is divided into three sections: the Overview in WS.AV.1, the additions to the JTA Core standards in WS.AV.2, and the Subdomain-Specific Services in WS.AV.3. WS.AV.2 follows the JTA Core service area structure. The structure of WS.AV.3 will evolve as aviation-specific service areas are identified and a common structure is coordinated among the other domains and subdomains.

WS.AV.2 Additions to the JTA Core

WS.AV.2.1 Introduction

This section identifies the standards for the Aviation Subdomain that are additional to standards in the JTA Core.

WS.AV.2.2 Information Processing Standards

WS.AV.2.2.1 Introduction

WS.AV.2.2.2 Mandated Standards

There are no mandated standards for the Information Processing Standards section.

WS.AV.2.2.3 Emerging Standards

There are no emerging standards for the Information Processing Standards section.

WS.AV.2.2.3.1 Service-Area Standards

There are no emerging service-area standards for the Information Processing Standards section.

WS.AV.2.2.3.1.1 Operating System Services

The Open Systems Joint Task Force (OSJTF) is sponsoring and synchronizing Weapon Systems Domain involvement in the IEEE Portable Operating System Interface (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.

WS.AV.2.3 Information Transfer Standards

There are no mandated or emerging standards for the Information Transfer Standards section.

WS.AV.2.4 Information Modeling, Metadata, and Information Exchange Standards

There are no mandated or emerging standards for the JTA Information Modeling, Metadata, and Information Exchange Standards section.

WS.AV.2.5 Human-Computer Interface Standards

WS.AV.2.5.1 Introduction

WS.AV.2.5.2 Mandated Standards

WS.AV.2.5.2.1 Symbology

There are no mandated standards for the Human-Computer Interface Standards section.

WS.AV.2.5.3 Emerging Standards

The following standard is emerging in this version of the JTA, but is proposed for the next version of the JTA:

- MIL-STD-1787C (USAF), Aircraft Display Symbology.

WS.AV.2.6 Information Security Standards

There are no mandated or emerging standards for the Information Security Standards section.

WS.AV.3 Subdomain-Specific Service Areas

WS.AV.3.1 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' (CAAs') 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 Air Traffic Management (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 in which 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.

WS.AV.3.1.1 Introduction

WS.AV.3.1.2 Mandated Standards

There are no mandated standards for Air Traffic Management Interoperability.

WS.AV.3.1.3 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 needed to interoperate with civil communications infrastructures—are considered emerging standards for the Aviation Systems Subdomain:

- 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, 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.

Page intentionally left blank.

WS.GV: Ground Vehicle Subdomain

WS.GV.1 Subdomain Overview

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 Ground Vehicle (GV) Subdomain include all DoD weapon systems on moving ground platforms except missiles—wheeled and tracked, manned and unmanned.

WS.GV.1.1 Purpose

This subdomain identifies standards for the Ground Vehicle Subdomain of the Weapon Systems Domain including information standards and analogous standards applicable to ground vehicle systems.

WS.GV.1.2 Background

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

WS.GV.1.3 Subdomain Description

The subdomain description is given in WS.GV.1.

WS.GV.1.4 Scope And Applicability

The scope of this subdomain is the entire Ground Vehicle Subdomain as defined in WS.GV.1.

WS.GV.1.5 Technical Reference Model

The Technical Reference Model used in this subdomain is the Technical Reference Model (TRM), which is described in the Weapon Systems Domain. The TRM Service View and Interface View are used as applicable.

WS.GV.1.6 Subdomain Organization

This Subdomain is divided into three sections: the Overview in WS.GV.1, the additions to the JTA Core standards in WS.GV.2, and the Subdomain-Specific Services in WS.GV.3. WS.GV.2 follows the JTA Core service area structure. The structure of WS.GV.3 will evolve as ground vehicle-specific service areas are identified and a common structure is coordinated among the other domain and subdomains.

WS.GV.2 Additions to the JTA Core

WS.GV.2.1 Introduction

This section identifies standards for the Ground Vehicles Subdomain in addition to the standards in the JTA Core.

WS.GV.2.2 Information Processing Standards

There are no mandated or emerging standards for the information processing Standards section.

WS.GV.2.2.1 Introduction

WS.GV.2.2.2 Mandated Standards

There are no mandated standards in this section.

WS.GV.2.2.3 Emerging Standards

The Army WSTAWG Operating Environment (OE) IPT has developed an emerging Application Program Interface (API) that is being evaluated for use by the Ground Vehicle Systems subdomain:

– Weapon Systems Technical Architecture Working Group (WSTAWG), Operating Environment (OE) Application Programmer's Interface (API), Volume I, OE Application Interface, Version 1.0, 12 June 1998.

WS.GV.2.3 Information Transfer Standards

There are no mandated or emerging standards for this section.

WS.GV.2.4 Information Modeling, Metadata, and Information Exchange Standards

There are no mandated or emerging standards for this section.

WS.GV.2.5 Human-Computer Interface Standards

There are no mandated or emerging standards for this section.

WS.GV.2.6 Information Security Standards

There are no mandated or emerging standards for this section.

WS.GV.3 Subdomain-Specific Service Areas and Interfaces

WS.GV.3.1 Introduction

The Interfaces View of the TRM, depicted in, provides sufficient fidelity for identifying classes of interfaces to apply open systems interface standards to the design of real-time and embedded hardware/software systems. The Interface View also facilitates the identification of critical functions and interfaces within the real-time and embedded-computing systems of the Ground Vehicle subdomain. Figure 1-4

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 TRM.

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

WS.GV.3.2 Application Software Layer Interfaces

There are no additional mandated or emerging standards for the Application Software Layer Interfaces section.

WS.GV.3.3 System Services Layer Interfaces

There are no mandated or emerging standards for the System Services Layer Interfaces section.

WS.GV.3.4 Resource Access Services Layer Interfaces

There are no mandated or emerging standards for the Resource Access Services Layer Interfaces section.

WS.GV.3.5 Physical Resources Layer Interfaces

WS.GV.3.5.1 Introduction

WS.GV.3.5.2 Mandated Standards

- 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.
- ANSI/VITA 1, VME64 Specification, 1994.
- SAE J 1850, Class B Data Communication Network Interface, 1 July 1995.
- ANSI X3.131, Information Systems - Small Computer Systems Interface - 2 (SCSI-2), 1994.
- Personal Computer Memory Card International Association (PCMCIA), PC Card Standard, March 1997.
- IEEE 1101.2, Standard for Mechanical Core Specifications for Conduction-Cooled Eurocards (ANSI), 1992.
- EIA 330, Electrical Performance Standards for Closed Circuit Television Camera 525/60 Interlaced 2:1 (ANSI/EIA 330-68), November 1966.
- EIA 343-A, Electrical Performance Standard for High Resolution Monochrome Closed Circuit Television Camera (November 1966), September 1969.
- PCI Industrial Computer Manufacturer's Group (PICMG): Compact PCI Specification, R2.1, September 1997.

The unique mission requirements of Ground Vehicle Systems dictate system and environmental constraints (e.g., long battery life, low power consumption, small size, light weight, shock-resistant, critical EMI-shielded constraints, all-weather operation) that make current the state-of-the-art digital and/or color video equipment unsuitable for use with Ground Vehicle Systems. Therefore, the following standards are mandated for Ground Vehicle Systems employing analog and/or monochrome video technology:

- EIA 170, Electrical Performance Standards – Monochrome Television Studio Facilities, November 1957.
- SMPTE 170M, Television - Composite Analog Video Signal - NTSC for Studio Applications, 1994.

WS.GV.3.5.3 Emerging Standards

The Ground Vehicle Systems Subdomain is also evaluating the Controller Area Network Bus (CANBUS) protocol and Class C networks documented in Society of Automotive Engineers (SAE) J1939 as an emerging standard for use in its heavy trucks and off road vehicles:

- SAE J1939, Recommended Practice for a Serial Control and Communications Vehicle Network, April 2000.

SAE J1708 defines a general-purpose serial data communications 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 physical adding/removing units to/from the line for the particular application. The following standard is emerging for ground vehicles:

– SAE J1708: Serial Data Communications Between Microcomputer Systems in Heavy-duty Vehicle Applications, October 1993.

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 following standard is emerging for Ground Vehicles:

– SAE J1587: Joint SAE/TMC Electronic Data Interchange Between Microcomputer Systems in Heavy-duty Vehicle Applications, July 1998.

WS.MD: Missile Defense Subdomain

WS.MD.1 Subdomain Overview

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 Defense Subdomain include any system or subsystem (including associated Ballistic Missile/C4I systems) with a mission to detect, classify, identify, intercept, and destroy or negate the effectiveness of enemy aircraft or missiles before launch or while in flight so as to protect U.S. and coalition forces, people, and geopolitical assets.

WS.MD.1.1 Purpose

This JTA subdomain identifies standards for missile defense systems. This version is focused primarily on active ballistic missile defense, with the intent of expanding this subdomain in the future.

WS.MD.1.2 Background

The following documents provide useful background information regarding missile defense (sorted by title), with particular emphasis on ballistic missile defense:

- *Draft Ballistic Missile Defense (BMD) Command, Control, and Communications (C3) Operational Requirements Document (ORD) (U)*, Air Force Space Command, AFSPC002-97-1, Working Draft, 1 April 1998, Secret (U.S. Only).
- *Battle Management Concept for Joint Theater Air and Missile Defense Operations, Joint Theater Air and Missile Defense Organization (JTAMDO)*, Final Draft, 11 September 1997.
- *BMD C3 ORD Requirements Incorporations into the NMD ORD (U)*, Air Force Space Command, 30 July 1998, Secret.
- *Capstone Theater Missile Defense (TMD) Cost and Operational Effectiveness Analysis (COEA)*, BMDO, 1996. Doctrine for Joint Theater Missile Defense. Joint Pub 3-01.5. February 22, 1996.
- *FY96 Analysis Of The Ballistic Missile Defense Interoperability Standards*, Fife et al., IDA-P-3277, Alexandria, VA: Institute For Defense Analyses.
- *JTAMD Mission Area Assessment (U)*, DoD J8, Draft, October 30, 1997, Secret. (Note that this document combines the capstone TMD COEA, TAD, and information on land attack cruise missiles).
- *National Ballistic Missile Defense (NBMD) Capstone Requirements Document (CRD) (U)*, U.S. Space Command, August 24, 1996, Secret (Release Can-US).
- *NMD Capability 1 and Capability 2 System Requirements Document (U)*, TRW Inc., May 6, 1998, BMC3 SE&I, Rosslyn, VA: TRW, Secret.
- *NMD Capability 2 System Requirements Document (U)*, TRW Inc., April 4, 1997, BMC3 SE&I, Rosslyn, VA: TRW, Secret.
- *Operational Requirements Document (ORD) for National Missile Defense (NMD) (U)*, draft, US Army Space and Strategic Defense Command, March 10, 1997, Secret.
- *Theater Air and Missile Defense Architecture for Joint Force Operations*, Bean et al., June 1997, MP 97W 105.

- *Theater Air and Missile Defense Master Plan*, September 1997, JTAMDO. POET control number MCNEIL 000396/97.
- *Theater Missile Defense (TMD) Command and Control (C2) Plan*, August 1996.
- *USACOM TMD Capstone Requirements Document (CRD) (U)*, U. S. Atlantic Command, Final Draft, March 2, 1998, Secret.
- *Command, Control, Communications, Computers, and Intelligence (C4I) Joint Tactical Data Link Management Plan*, Department of Defense, June 6, 1996.

WS.MD.1.3 Subdomain Description

For a description of this subdomain, see the background material in WS.MD.1.2. As discussed in some of these documents, there is a need for interoperability between Theater Missile Defense (TMD) family of systems (FoS), National Missile Defense (NMD) components, and other systems such as Space-Based Infrared System (SBIRS) to support their missions. Such interoperability would need to support activities such as minimum cueing, track exchange, and weapon coordination. This requires standards (e.g., in how such information should be transferred and on geospatial values). This JTA subdomain specifies such standards to support interoperability to fulfill missile-defense mission objectives.

WS.MD.1.4 Scope and Applicability

The scope of this subdomain is the entire domain of missile defense (as defined in the overview above). However, the standards listed within this version of the subdomain solely address support for active and passive defense[1] against theater and strategic ballistic missiles in flight, as a first step in evolving a comprehensive and complete set of standards for all missile defense systems. It is acknowledged that this evolution will require interaction with many communities to resolve standardization issues.

WS.MD.1.5 Technical Reference Model

Missile defense systems typically include one or more sensors, one or more weapons, and a communication infrastructure all coordinated by a Battle Management Command, Control, and Communications (BMC3) system (which also coordinates with external systems). At this time there is ongoing work to develop a tailored reference model and technical architecture profile for missile defense based on the TRM.

WS.MD.1.6 Subdomain Organization

This subdomain is divided into three sections: (1) the Overview in WS.MD.1; (2) the missile defense mandates and emerging standards additional to those in the JTA Core in WS.MD.2; and (3) the Subdomain-Specific Service Areas and Interfaces in WS.MD.3. WS.MD.2 follows the JTA Core service area structure. The structure of WS.MD.3 will evolve as missile defense-specific service areas are identified and a common structure is coordinated among the other domains.

WS.MD.2 Additions to the JTA Core

WS.MD.2.1 Introduction

This section identifies standards for the Missile Defense Subdomain that are additional to standards in the JTA Core.

[1] Missile defense can be viewed as having four pillars: active defense, attack operations, passive defense, and an overarching BMC4I. In this context, active defense is direct defensive action taken to nullify or reduce the effectiveness of hostile air action, such as the use of missile defense weapons. Attack operations includes activities such as directly attacking missile launchers. Passive defense is all other measures taken to minimize the effectiveness of a specific hostile air action, including deception and dispersion. The overarching BMC4I directs and coordinates all these activities.

WS.MD.2.2 Information Processing Standards

WS.MD.2.2.1 Introduction

WS.MD.2.2.2 Mandated Standards

There are no mandated standards in this section.

WS.MD.2.2.3 Emerging Standards

WS.MD.2.2.3.1 Navigation Standard

The following standard supports sharing of navigation-related data (e.g., position, velocity, and time) between missile defense systems. This standard is consistent with, and extends the mandates in, the JTA Core (in particular World Geodetic System [WGS84] and Coordinated Universal Time [UTC] U.S. Naval Observatory [USNO]). The following standard is emerging:

– Ballistic Missile Defense (BMD) Positioning, Navigation, and Timing (PNT) Standard, 20 July 2000, Ballistic Missile Defense Organization.

WS.MD.2.2.3.2 Real-Time Defense Information Infrastructure Common Operating Environment (DII COE)

Missile defense systems are, by their nature, a combination of hard and soft real-time systems. There is ongoing work to incorporate some soft real-time capabilities into the DII COE. The applicability of these capabilities is being evaluated.

WS.MD.2.3 Information Transfer Standards

WS.MD.2.3.1 Introduction

WS.MD.2.3.2 Mandated Standards

WS.MD.2.3.2.1 Time Synchronization

The time basis for NMD and TMD operations shall be UTC (USNO) as disseminated by the Navstar Global Positioning System (GPS). The GPS standards identified in 3.2.1.6 are mandated.

WS.MD.2.3.3 Emerging Standards

WS.MD.2.3.3.1 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.

WS.MD.2.4 Information Modeling, Metadata, and Information Exchange Standards

WS.MD.2.4.1 Introduction

WS.MD.2.4.2 Mandated Standards

WS.MD.2.4.2.1 Bit-Oriented Formatted Messages

The Tactical Digital Information Link (TADIL)-J/Link-16 message format is mandated as a mobile interoperable communication message format on all transportable missile defense systems, and for

Theater Air Missile Defense (TAMD) systems that must interoperate with them. This is specified by MIL-STD-6016A combined with all accepted Interface Change Proposals (ICPs) awaiting incorporation. Although this standard is in the JTA Core, this subdomain adds the additional requirement that this standard must be implemented for such systems and cannot be replaced with the alternatives listed in the JTA Core. Such systems may also support other message formats. The following standard is mandated for transportable missile defense systems.

- MIL-STD-6016A, Tactical Digital Information Link (TADIL) J Message Standard, 30 April 1999.

WS.MD.2.4.3 Emerging Standards

The Missile Defense Data Standardization Group is working to merge the Data Element Definitions (DEDs) developed for TMD, NMD, and the Joint Theater Air Missile Defense Organization (JTAMDO).

The NMD program is in the process of selecting communication mechanisms. An Integrated Product Team (IPT) formed to study the issue has recommended that NMD use a Variable Message Format (VMF)-based message set.

Ballistic Missile Defense Organization (BMDO) has formed the "Time and Geospatial Working Group" (TGWG) to identify additional time and geospatial issues and to develop cross-system resolutions of those issues.

WS.MD.2.5 Human-Computer Interface Standards

WS.MD.2.5.1 Introduction

WS.MD.2.5.2 Mandated Standards

WS.MD.2.5.2.1 Symbology

Operations can be identified as being engagement operations or force operations. Engagement operations are real-time or near-real-time operations involved in control of the engagement, providing for the acquisition, tracking, identification, management and dissemination of air track information, the alerting of the force to the presence of non-friendly aircraft, the cueing of weapon systems to engageable aircraft in their area of interest and for the distribution of battle management information. Engagement operations are typically supported by TADIL data links. Force operations are involved in the support of the operation, providing for the allocation of air defense resources, the assignment of operations and priorities of defended assets, and the coordination and implementation of firing restrictions and rules of engagement. Typically, force operations are non-real-time or near-real-time.

The use of military standards such as MIL-STD-1477B for engagement operations symbology is encouraged, but no symbology standard for engagement operations is mandated by the JTA. The following standard is mandated for the display of common warfighting symbology for force operations:

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

WS.MD.2.6 Information Security Standards

There are no mandates or emerging standards for this section.

WS.MD.3 Subdomain-Specific Service Areas and Interfaces

There are no subdomain-specific service areas and interfaces identified at this time.

WS.MS: Missile Systems Subdomain

WS.MS.1 Subdomain Overview

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 Strategic and Theater Ballistic Missile Systems; Cruise Missile Systems; and rocket and missile systems used in diverse Battlefield Functional Areas including Fire Support, Close Combat, and Special Operations. Note that Missiles which are components of U.S. National and Theater Missile Defense systems are not included in the Missile Systems Subdomain, but instead are covered in the Missile Defense Subdomain. The diversity of missions that missile systems must perform induces a variety of system solutions including shoulder-fired, line-of-sight direct fire, and non-line-of-sight indirect fire missiles and rockets; ground-launched, air-launched, and ship-launched or submarine-launched cruise missiles; surface-to-surface, surface-to-air, ship-to-ship, air-to-air, and air-to-ground missiles; and Inter-Continental, Intermediate Range, and Submarine-Launched Ballistic Missiles (ICBMs, IRBMs, and SLBMs respectively). Broadly, Missile Systems may be described in terms of the following subsystems: 1) missile, 2) launcher, 3) C3I (including fire control or battle management), and, in some cases, 4) sensor. These subsystems are designed and developed to deploy and function as a single Missile System in which all the subsystems are, to a certain degree, interdependent. The Missile System may have all of the subsystems collocated or distributed. For example, a sensing device may be onboard a missile or on the ground, in the air, or in space providing information to the missile via a high-performance data link. Also, a missile's fire control or battle management system may be collocated in the launch vehicle or geographically separate from the launch vehicle, but connected through a direct (physical), line-of-sight, or non-line-of-sight communications link.

WS.MS.1.1 Purpose

This subdomain builds on the Weapon Systems Domain by identifying Missile Systems subdomain-specific standards including information standards and analogous standards applicable to Missile Systems. (See 1.4.2 for relationships between Core, domain, and subdomain standards.)

WS.MS.1.2 Background

The standards in this subdomain are based on the ongoing work of the Joint weapons community.

WS.MS.1.3 Subdomain Description

For a description of this subdomain, see WS.MS.1. For the purpose of this subdomain, Missile Systems include all offensive missile and rocket systems.

WS.MS.1.4 Scope and Applicability

The scope of this subdomain is all DoD Missile Systems (as defined in WS.MS.1 and WS.MS.1.3). However, the standards listed in this version of the subdomain currently address only Army Missile and Rocket Systems. This is a first step in evolving a comprehensive and complete set of standards for Missile Systems for all the Services. It is acknowledged that this evolution will require extensive interaction with many communities to resolve standardization issues.

WS.MS.1.5 Technical Reference Model

The Technical Reference Model (TRM) used in this subdomain is the TRM described in the Weapon Systems Domain.

WS.MS.1.6 Subdomain Organization

This subdomain is divided into three sections: the Subdomain Overview in WS.MS.1, the Subdomain-Specific Standards in WS.MS.2, and the Subdomain-Specific Service Areas and Interfaces in WS.MS.3. WS.MS.2 follows the JTA Core service area structure. The structure of WS.MS.3 follows the structure of Section 3 of the Weapon Systems Domain.

WS.MS.2 Additions to JTA Core

WS.MS.2.1 Introduction

This section identifies the subdomain-specific mandated and emerging standards for the Missile Systems Subdomain.

WS.MS.2.2 Information Processing Standards

Currently, there are no subdomain-specific mandated or emerging standards in this section.

WS.MS.2.3 Information Transfer Standards

Currently, there are no subdomain-specific mandated or emerging standards in this section.

WS.MS.2.4 Information Modeling, Metadata, and Information Exchange Standards

Currently, there are no subdomain-specific mandated or emerging standards in this section.

WS.MS.2.5 Human-Computer Interface Standards

Currently, there are no subdomain-specific mandated or emerging standards in this section.

WS.MS.2.6 Information Security Standards

Currently, there are no subdomain-specific mandated or emerging standards in this section.

WS.MS.3 Subdomain-Specific Services and Interfaces

WS.MS.3.1 Introduction

The Interfaces View of the TRM, depicted in Figure 1-4, provides sufficient fidelity for identifying classes of interfaces to apply open systems interface standards to the design of real-time and embedded hardware/software systems. The Interface View 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 Interfaces View of the TRM.

WS.MS.3.2 Application Software Layer Interfaces

Currently, there are no subdomain-specific mandated or emerging standards in this section.

WS.MS.3.3 System Services Layer Interfaces

Currently, there are no subdomain-specific mandated or emerging standards in this section.

WS.MS.3.4 Resource Access Services Layer Interfaces

Currently, there are no subdomain-specific mandated or emerging standards in this section.

WS.MS.3.5 Physical Resources Layer Interfaces

This section identifies:

- 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
- The interface standards that support the direct connections between Physical Resources, such as those needed to enable buses and communications links to address processors or those needed to enable processors to address memory registers.

WS.MS.3.5.1 Introduction

WS.MS.3.5.2 Mandated Standards

Currently, there are no subdomain-specific mandated standards in this section.

WS.MS.3.5.3 Emerging Standards

Standards used across multiple Missile Systems and their platforms are expected to see continued use in the development of future Missile Systems and upgrades to existing systems.

The following standard is emerging for 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.

– 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.

The following industrial bus standard is emerging for applications requiring high-speed data transfer, rugged construction, excellent shock and vibration resistance, Plug'n Play capability, and the desire for future hot-swappable support.

– PCI Industrial Computer Manufacturers Group (PICMG): Compact PCI Specification, R2.1, September 1997.

The following standard is emerging 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.

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

The following standard is emerging for applications requiring hot-swappable peripherals that add memory, mass storage, and I/O capabilities to computers in a rugged, compact form factor.

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

The following standard is emerging when using a VME bus, an internal interconnect (backplane) bus intended for connecting processing elements to their immediate fundamental resources, and is cited to facilitate mechanical interchangeability of conduction-colled 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.

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

The following standards are also considered to be emerging:

- SAE J 1850, Class B Data Communication Network Interface, 1 July 1995.
- ANSI/VITA 1, VME64 Specification, 1994.

WS.MUS: Munition Systems Subdomain

WS.MUS.1 Subdomain Overview

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 DoD's inventory of weapon systems, many systems do not fit within the parameters of the well-defined Weapon Systems Subdomains of Missile Defense 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 sensors, control stations, combat communication systems, repeaters, and gateways. The Munition Systems Subdomain includes any system or subsystem that contains an explosive warhead (such as dumb, smart, and precision bombs, or mines and artillery shells) and that detects, classifies, identifies, intercepts, and destroys or negates the effectiveness of the enemy.

WS.MUS.1.1 Purpose

This subdomain builds on Weapon Systems Domain by identifying Munition Systems Subdomain-specific standards including information standards and analogous standards applicable to Munition Systems. (See 1.4.2 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 610.12A-1990) within the family of systems that constitute the subdomain.

This version is focused solely on Landmine Munition Systems, with the intent of expanding this subdomain in the future.

WS.MUS.1.2 Background

The standards in this subdomain are based on the work performed by the weapons community.

WS.MUS.1.3 Subdomain Description

Munition Systems included in this subdomain are those whose parameters cannot be accurately described within the parameters of the well-defined Weapon Systems Subdomains of Missile Systems, Soldier Systems, Ground Vehicle Systems, or Aviation Systems. These Munition Systems are primarily unattended and autonomous, with unique environmental and operational mission requirements (e.g., positive systems control and management, long-range remote communications, physical packages and platforms, security and survivability, performance, safety) that are not common to other subdomains. Their system elements may include combinations of autonomous and remotely commanded munitions with or without the following: onboard sensors, networked combat sensors and/or sensor suites, and control stations with integral combat communications, including combat communication systems, information processing gateways, and repeaters.

WS.MUS.1.4 Scope and Applicability

The scope of this subdomain is the entire Munition Systems Subdomain (as defined in the overview and subdomain description above). However, the standards listed within this version of the subdomain solely address support for Landmine Munition Systems, as a first step in evolving a comprehensive and complete set of standards for Munition Systems. It is acknowledged that this evolution will require interaction with many communities to resolve standardization issues.

WS.MUS.1.5 Technical Reference Model

The Technical Reference Model used in this subdomain is the Technical Reference Model (TRM) described in the Weapon Systems Domain.

WS.MUS.1.6 Subdomain Organization

This subdomain is divided into three sections: the Subdomain Overview in WS.MUS.1, the subdomain-specific standards in WS.MUS.2, and the subdomain-specific services and interfaces in WS.MUS.3. WS.MUS.2 follows the JTA Core service area structure. The structure of WS.MUS.3 follows the structure of Weapon Systems Domain WS.3.

WS.MUS.2 Additions to the JTA Core

WS.MUS.2.1 Introduction

This section identifies the subdomain-specific mandated and emerging standards for the Munition Systems Subdomain.

WS.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.

WS.MUS.2.2.1 Introduction

WS.MUS.2.2.2 Mandated Standards

Currently, there are no subdomain-specific mandated standards in this section.

WS.MUS.2.2.3 Emerging Standards

Currently, there are no subdomain-specific emerging standards in this section.

WS.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.

WS.MUS.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 Munition Systems Subdomain.

WS.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.

WS.MUS.2.6 Information Security Standards

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

WS.MUS.3 Subdomain-Specific Services and Interfaces

WS.MUS.3.1 Introduction

The Interfaces View of the TRM, depicted in Figure 1-4, provides sufficient fidelity for identifying classes of interfaces to apply open systems interface standards to the design of real-time and embedded-hardware/software systems. The Interface View also facilitates the identification of critical

functions and interfaces within the real-time and embedded-computing systems of the Munition Systems.

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 TRM.

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

WS.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.

WS.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.

WS.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.

WS.MUS.3.5 Physical Resources Layer Interfaces

This section identifies

- 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
- The interface standards that support the direct connections between Physical Resources, such as those needed to enable buses and communications links to address processors or those needed to enable processors to address memory registers.

WS.MUS.3.5.1 Introduction

WS.MUS.3.5.2 Mandated Standards

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.

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

The following industrial bus standard is mandated for applications requiring high-speed data transfer, rugged construction, excellent shock and vibration resistance, Plug'n Play capability, and the desire for future hot-swappable support.

- PCI Industrial Computer Manufacturers Group (PICMG): Compact PCI Specification, R2.1, September 1997.

The following standard is mandated for applications requiring hot-swappable peripherals that add memory, mass storage, and I/O capabilities to computers in a rugged, compact form factor.

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

WS.MUS.3.5.3 Emerging Standards

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

WS.SS: Soldier Systems Subdomain

WS.SS.1 Subdomain Overview

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 target location, target identification, target acquisition, enhanced survivability, navigation, position location, enhanced mobility, and command-and-control into a system worn or carried by an individual soldier in performance of assigned duties.

WS.SS.1.1 Purpose

This subdomain builds on the Weapon Systems Domain by identifying Soldier Systems Subdomain-specific standards including information standards and analogous standards applicable to Soldier Systems. (See 1.4.2 for relationships between JTA Core, domain, and subdomain standards.)

WS.SS.1.2 Background

The standards in this subdomain are based on the work performed by the weapons community.

The following documents provide useful background information regarding soldier systems with particular emphasis on fighting systems:

- The Soldier Integrated Protective Ensemble (SIPE), Army Concept Technology Demonstration (ACTD), U.S. Army Natick Research, Development and Engineering Command, September 1991.
- The Enhanced Integrated Soldier System (TEISS), Army Science Board Study, 30 March 1993.
- The Land Warrior Operational Requirements Document (ORD), HQ U.S. Army Training and Doctrine Command, 17 March 1994.

WS.SS.1.3 Subdomain Description

The systems of this subdomain integrate 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 capabilities are achieved through integration of Government-Furnished Equipment and the use of commercial-off-the-shelf technologies to meet the key performance parameters of soldier systems. These systems are optimized to minimize the total weight carried by the individual while minimizing the cognitive overload. These systems are required 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. Systems do not rely on any fixed infrastructure to meet the operational performance requirements.

WS.SS.1.4 Scope and Applicability

The scope of this subdomain is the entire Soldier Systems Subdomain as defined in Section WS.SS.1 above.

WS.SS.1.5 Technical Reference Model

The Technical Reference Model used in this subdomain is the Technical Reference Model (TRM) described in the Weapon Systems Domain.

WS.SS.1.6 Subdomain Organization

This subdomain is divided into four sections: the Subdomain Overview in WS.SS.1, the additions to the JTA Core in WS.SS.2, and the subdomain-specific standards in WS.SS.3. WS.SS.2 follows the JTA Section 3 service area structure.

WS.SS.2 Subdomain-Specific Standards

WS.SS.2.1 Introduction

This section identifies the subdomain-specific mandated and emerging standards for the Soldier Systems Subdomain.

WS.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.

WS.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.

WS.SS.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 Soldier Systems Subdomain.

WS.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.

WS.SS.2.6 Information Security Standards

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

WS.SS.3 Subdomain-Specific Services and Interfaces

WS.SS.3.1 Introduction

The Interfaces View of the TRM, depicted in Figure 1-4, provides sufficient fidelity for identifying classes of interfaces to apply open systems interface standards to the design of real-time and embedded hardware/software systems. The Interface View 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 TRM.

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

WS.SS.3.2 Application Software Layer Interfaces

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

WS.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.

WS.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.

WS.SS.3.5 Physical Resources Layer Interfaces

This section identifies:

- 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
- The interface standards that support the direct connections between Physical Resources, such as those needed to enable buses and communications links to address processors or needed to enable processors to address memory registers.

WS.SS.3.5.1 Introduction

WS.SS.3.5.2 Mandated Standards

The unique mission requirements of Soldier Systems dictate system and environmental constraints (e.g., long battery life, low power consumption, small size, light-weight, shock resistant, critical EMI-shielded constraints, all-weather operation, use with NBC protective gear) that make current state-of-the-art digital and/or color video equipment unsuitable for use with Soldier Systems. Therefore, the following standards are mandated for soldier systems employing analog and/or monochrome video technology:

- EIA 170, Electrical Performance Standards - Monochrome Television Studio Facilities, November 1957.
- SMPTE 170M, Television - Composite Analog Video Signal - NTSC for Studio Applications, 1994.

WS.SS.3.5.3 Emerging Standards

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

Page intentionally left blank.

Appendix A: Abbreviations and Acronyms

Note: Multiple acronyms are sometimes shown for the same term where the different acronyms are used in the document. For example, the text of the document consistently uses “Mbits/s” for “Megabits per second,” but the abbreviation “Mbps” is used in the titles of some standards.

AAL	ATM Adaptation Layer
ABBET	A Broad-Based Environment for Test
ABOR	Abort
ACC	Architecture Coordination Council
ACP	Allied Communications Publication
ACR	American College of Radiology
ACTD	Advanced Concept Technology Demonstration
ADE	Application Development Environment
ADS	Automatic Dependent Surveillance
AEP	Application Environment Profile
AES	Application Environment Specification
AES3	Audio Engineering Society 3
AFP	Adapter Function and Parametric Data Interface
AH	Authentication Header
AI-ESTATE	Artificial Intelligence-Exchange and Services Tie to All Test Environments
AIM	Advanced Information Management
AIS	Automated Information System
AITI	Automated Interchange of Technical Information
ALE	Automated Link Establishment
ALSP	Aggregate-Level Simulation Protocol
AMB	ATS Management Board
AMSS	Aeronautical Mobile Satellite Services
ANSI	American National Standards Institute
AOR	Area of Responsibility
API	Application Program Interface
AR	Airborne Reconnaissance
ARC	Equal Arc Second Raster Chart/Map
ARI	Automatic Test Systems (ATS) Research and Development (R&D) Integrated Product Team (IPT)
ASD	Assistant Secretary of Defense
ASD(C3I)/DoD CIO	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)/DoD Chief Information Officer
ASICs	Application-Specific Integrated Circuits
ATA	Army Technical Architecture
ATCRBS	Air Traffic Control Radar Beacon System

ATE	Automated Test Equipment
ATM	Asynchronous Transfer Mode
ATS	Automatic Test Systems
AV	Air Vehicle; Aviation
BER	Bit Error Rate
BGP	Border Gateway Protocol
BIIF	Basic Image Interchange Format
bits/s	Bits per second
B-ISDN	Broadband-Integrated Services Digital Network
BMC3	Ballistic Missile Command, Control, and Communications
BMD	Ballistic Missile Defense
BMDO	Ballistic Missile Defense Organization
BOOTP	Bootstrap Protocol
bps	Bits Per Second
BRI	Basic Rate Interface
BUFR	Binary Universal Format for Representation
C/S/A	CINCs/Services/Agencies
C2	Command and Control
C2CDM	Command and Control Core Data Model
C3	Consultation, Command and Control
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CA	Certification Authority
CAC	Computer Asset Controller
CAD	Computer-Aided Design
CADRG	Compressed ARC Digitized Raster Graphics
CAE	Common Application Environment
CAF	C4I Architecture Framework
CALS	Continuous Acquisition and Life-Cycle Support
CAM	Computer-Aided Manufacturing
CASI	Common ATM Satellite Interface
CBC	Cipher Block Chaining
CBR	Constant Bit Rate
CBS	Commission for Basic Systems
CCB	Change Control Board
CCEB	Combined Communications-Electronics Board

CCITT	International Telegraph & Telephone Consultative Committee (now ITU-T)
CCSDS	Consultative Committee for Space Data Systems
CDE	Common Desktop Environment
CDL	Common Data Link
CDMA	Code Division Multiple Access
CD-ROM	Compact Disk-Read Only Memory
CE	Controlled Extensions
CEN	European Committee for Standardization
CFS	Center for Standards
CGI	Computer Graphics Interface
CGM	Computer Graphics Metafile
CGMTI	Common Ground Moving Target Indicator
CHAP	Challenge Handshake Authentication Protocol
CHBDL-ST	Common High Bandwidth Data Link Surface Terminal
CI	Critical Interface
CIB	Controlled Image Base
CINC	Commander In Chief
CIPSO	Common Internet Protocol Security Options
CITA	Combined Interoperability Technical Architecture
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CLI	Call-Level Interface
CM	Configuration Management
CMC	Certificate Management Messages over Cryptographic Message Syntax
CMIP	Common Management Information Protocol
CMIS	Common Management Information Services
CMMS	Conceptual Models of the Mission Space
CMS	Cryptographic Message Syntax
CNR	Combat Net Radio
CNS	Communications Navigation, and Surveillance
COE	Common Operating Environment
COEA	Cost and Operational Effectiveness Analysis
COM	Common Object Model; Component Object Model
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off-the-Shelf
CRD	Capstone Requirements Document
CRLs	Certificate Revocation Lists
CRY	Cryptologic
CS	Combat Support
CSMA/CD	Carrier Sense Multiple Access with Collision Detection

CSP	Common Security Protocol
CSR	Command and Status Register
CTRS	Conventional Terrestrial Reference System
CXE	Computer to External Environments Interface
DAA	Designated Approving Authority
DAMA	Demand Assigned Multiple Access
DAP	Directory Access Protocol
DARPA	Defense Advanced Research Projects Agency
DAT	Digital Audio Tape
DBMS	Database Management System
DCE	Distributed Computing Environment
DCI	Director, Central Intelligence
DCOM	Distributed Component Object Model
DDA	DoD Data Architecture
DDDS	Defense Data Dictionary System
DDM	DoD Data Model
DDNS	Dynamic Domain Name System
DDRS	Defense Data Repository System
DED	Data Element Definitions
DES	Data Encryption Standard
3DESE	Triple-DES Encryption
DHCP	Dynamic Host Configuration Protocol
DIA	Defense Intelligence Agency; Diagnostic Processing Interface Protocol (ATS Subdomain)
DICOM	Digital Imaging and Communication In Medicine
DIF	Data Interchange Format
DIGEST	Digital Geographic Information Exchange Standard
DII	Defense Information Infrastructure
DIRNSA	Director, NSA
DIS	Distributed Interactive Simulation; Draft International Standard
DISA	Defense Information Systems Agency (formerly Defense Communications Agency [DCA])
DISN	Defense Information System Network
DITSCAP	DoD IT Security Certification & Accreditation Process
DLA	Defense Logistics Agency
DLWG	Data Link Working Group
DMS	Defense Message System
DMSO	Defense Modeling and Simulation Office
DMTD	Digital Message Transfer Device
DNC	Digital Nautical Chart
DNS	Domain Name System

DoD	Department of Defense
DoDD	DoD Directive
DoDIIS	DoD Intelligence Information Systems
DoDISS	DoD Index of Specifications and Standards
DoDSSP	DoD Single Stock Point
DOI	Domain of Interpretation
DPPDB	Digital Point Positioning Data Base
DRV	Instrument Driver Application Programming Interface
DSA	Digital Signature Algorithm
DSIC	Defense Standards Improvement Council
DSN	Defense Switched Network
DSP	Defense Standardization Program
DSS	Digital Signature Standard
DSS1	Digital Subscriber Signaling System No 1
DSSS	Direct Sequence Spread Spectrum
DSSSL	Document Style and Semantics Specification Language
DTD	Document Type Definition
DTF	Digital Test Data Format
DTIF	Digital Test Interchange Format
DTOP	Digital Topographic Data
DTS	Defense Transportation System
EAM	Emergency Action Message
EAP	Emergency Action Procedure
EB	Electronic Business
EC	Electronic Commerce
EAO	Executive Agent Office
ECAPMO	Electronic Commerce Acquistion Program Management Office
EDI	Electronic Data Interchange
EDIF	Electronic Data Interchange Format
EDISMC	EDI Standards Management Committee
EEI	External Environment Interface
EHF	Extremely High Frequency; Extra High Frequency
EIA	Electronics Industries Alliance
E-MAIL	Electronic Mail
EMI	Electro-Magnetic Interference
ESP	Encapsulating Security Payload
FDMA	Frequency Division Multiple Access
FED-STD	Federal Telecommunication Standard

FESMCC	Federal EDI Standards Management Coordinating Committee
FIPS	Federal Information Processing Standards
FOM	Federation Object Model
FP	File-Handling Protocol
FPLMTS	Future Public Land Mobile Telecommunications Systems
FPS	Frames Per Second
FRM	Framework Interface; Functional Requirements Model Functional Reference Model
FTP	File Transfer Protocol
FTR	Federal Telecommunications Recommendation
FWG	Functional Working Group
GeoSym	Geospatial Symbols for Digital Displays
GIC	Generic Instrument Class Interface
GIF	Graphics Interchange Format
GIS	Geographic Information 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
GV	Ground Vehicle
HCI	Human-Computer Interface
HDBK	Handbook
HF	High-Frequency
HFDL	High-Frequency Data Link
HIDAR	High Data Rate
HIPAA	Health Insurance Portability and Accountability Act
HISTOA	History Tag, Version A
HL7	Health Level 7
HLA	High-Level Architecture
HMAC	keyed-Hashing for Message Authentication
HST	Host Computer Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
Hz	Hertz
I&RTS	Integration and Runtime Specification

I/O	Input/Output
IAB	Internet Architecture Board
IATF	Information Assurance Technical Framework
IC	Intelligence Community
ICAO	International Civil Aviation Organization
ICB	Instrument Communication Bus Interface
ICD	Interface Control Document
ICHIPB	Imagery Chip, Version B
ICL	Instrument Command Language Interface
ICM	Instrument Communications Manager Interface
ICMP	Internet Control Message Protocol
ICP	Interface Change Proposal
IDEF0	Integrated Definition for Function Modeling
IDEF1X	Integrated Definition for Information Modeling
IDL	Interface Definition Language
IDUP	Independent Data Unit Protection
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IER	Information Exchange Requirement
IETF	Internet Engineering Task Force
I/EW	Intelligence and Electronic Warfare
IF	Intermediate Frequency
IFF	Identification of Friends and Foes
IFP	Instrument Function and Parametric Data Interface
IGES	Initial Graphics Exchange Specification
IGMP	Internet Group Management Protocol
IIOP	Internet Inter-ORB Protocol
ILMI	Interim Local Management Interface
IMA	Inverse Multiplexing for ATM
IMT	International Mobile Telecommunications
IP	Internet Protocol
IPC	Institute for Interconnecting and Packaging Electronic Circuits
IPCP	Internet Protocol Control Protocol
IPT	Integrated Product Team
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Next Generation Version 6
IR	Infrared
IS	Information System
ISA	Industry Standard Architecture
ISAKMP	Internet Security Association and Key Management Protocol

ISB	Intelligence Systems Board
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization, International Electrotechnical Commission
ISR	Intelligence, Surveillance, & Reconnaissance
ISS	Intelligence Systems Secretariat
IT	Information Technology
ITMRA	Information Technology Management Reform Act (of 1996)
ITSEC	European Information Technology Security Evaluation Criteria
ITSG	Information Technology Standards Guidance
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector
ITW/AA	Integrated Tactical Warning and Attack Assessment
JDBC	JAVA Database Connectivity
JFIF	JPEG File Interchange Format
JIEO	Joint Information Engineering Organization
JIRA	Japanese Industry Association for Radiation Apparatus
JPEG	Joint Photographic Experts Group
JRE	Joint Range Extension
JREAP	JRE Application Protocol
JSA	Joint Systems Architecture
JTA	Joint Technical Architecture
JTADG	Joint Technical Architecture Development Group
JTAMDO	Joint Theater Air and Missile Defense Organizations
JTAWG	Joint Technical Architecture Working Group
JTDLMP	Joint Tactical Data Link Management Plan
JTIDS	Joint Tactical Information Distribution System
JTF	Joint Task Forces
JV 2010	Joint Vision 2010
JVM	Java Virtual Machine
Kbits/s	Kilobits per second
Kbps	Kilobits per second
KEA	Key Exchange Algorithm
KHz	Kilohertz
KMP	Key Management Protocol
LAN	Local Area Network
LANE	Local Area Network Emulation

LCP	Link Control Protocol
LCSCES	Low Speed Circuit Emulation Service
LDAP	Lightweight Directory Access Protocol
LDAPv3	Lightweight Directory Access Protocol 3
LDR	Low Data Rate
LF	Low Frequency
LOS	Line-of-Sight
LPI	Low Probability of Intercept
LQM	Link Quality Monitoring
LRAs	Local Registration Authorities
LUNI	LANE User-Network Interface
M&S	Modeling and Simulation
MAC	Medium-Access Control
MAIS	Major Automated Information System
MAN	Metropolitan Area Network
MASINT	Measurement and Signature Intelligence
MASPS	Minimum Aviation Systems Performance Standards
MAU	Medium-Access Unit
Mbits/s	Megabits per second
Mbps	Megabits per second
MC&G	Mapping, Charting, and Geodesy
MCU	Multipoint Control Units
MD	Missile Defense
MDAPS	Major Defense Acquistion Programs
MDR	Medium Data Rate
MED	Medical
MEECN	Minimum Essential Emergency Communications Network
MELP	Mixed Excitation Linear Prediction
MG	Multinational Group
MHP	Mobile Host Protocol
MHSS	Military Health Services System
MHz	Megahertz
MI	Motion Imagery
MIB	Management Information Base
MIDS	Multi-functional Information Distribution System
MIL-HDBK	Military Handbook
MILSATCOM	Military Satellite Communications
MIL-STD	Military Standard
MIME	Multipurpose Internet Mail Extensions

MISB	Motion Imagery Standards Board
MISP	Motion Imagery Standards Profile
MISSI	Multilevel Information Systems Security Initiative
MIST	Miniature Interoperable Surface Terminal
MLPP	Multi-Level Precedence and Preemption
MMF	Multimedia Formats Interface
MMPM	MEECN Message-Processing Mode
MNG	Multiple-Image Network Graphics
MOF	Meta-Object Facility
MPEG	Motion Pictures Expert Group
MPOA	Multiprotocol over ATM
MS	Missile Systems
MSMP	Modeling and Simulation Master Plan
MSI	Multispectral Imagery
MSP	Message Security Protocol
MTA	Message Transfer Agent
MTI	Moving Target Indicator
MUS	Munition Systems
NAFAG	NATO Air Force Armaments Group
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NAVWAR	Navigation Warfare
NAWCADLKE	Naval Air Warfare Center Aircraft Division-Lakehurst
NBC	Nuclear, Biological, Chemical
NC3TA	North Atlantic Treaty Organization (NATO) Consultation, Command and Control (C3) Technical Architecture (TA)
NCC	Nuclear Command and Control
NCPDP	National Council for Prescription Drug Program
NCSC	National Computer Security Center
NEMA	National Electrical Manufacturers Association
NET	Network Protocols Interface
NIMA	National Imagery and Mapping Agency
NIST	National Institute of Standards and Technology
NITF	National Imagery Transmission Format
NITFS	National Imagery Transmission Format Standard
NMD	National Missile Defense
NP	Network Protocol
NRO	National Reconnaissance Office
NSA	National Security Agency

NSIF	NATO Secondary Imagery Format
NSM	Network and Systems Management
NTIS	National Technical Information Service
NTM	National Technical Means
NTP	Network Time Protocol
NTSC	National Television Standards Committee
NTSDS	National Target/Threat Signature Data System
OA	Operational Architecture
ODBC	Open Database Connectivity
ODMG	Object Data Management Group
OE	Operating Environment
OJCS	Office of the Joint Chiefs of Staff
OLE	Object Linking and Embedding
OMA	Object Management Architecture
OMG	Object Management Group
OMT	Object Model Template
OOTW	Operations Other Than War
ORD	Operational Requirements Document
OS	Operating System
OSD	Office of the Secretary of Defense
OSE	Open Systems Environment
OUSD(AT&L)	Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics)
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OSJTF	Open Systems Joint Task Force
OSPF	Open Shortest Path First
PASV	Passive
PCI	Peripheral Computer Interface
PCIMG	PCI Industrial Computer Manufacturer's Group
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Services
PHY	Physical Layer
PIAE	Profile for Imagery Access Extensions
PICS	Protocol Implementation Conformance Statement
PKI	Public-Key Infrastructure
PLDs	Programmable Logic Devices
PMNV/RSTA	Program Management Office for Night Vision/Reconnaissance and Target Acquistion
PNG	Portable Network Graphics

PNNI	Private Network-Network Interface
POSIX	Portable Operating System Interface for Computer Environments
PP	Protection Profile
PPP	Point-to-Point Protocol
PPS	Precise Positioning Service
PRI	Primary Rate Interface
PRO	Product Data Association
PSK	Phase Shift Keying
PSTN	Public Switched Telephone Networks
QoS	Quality of Service
R&D	Research and Development
RAs	Registration Authorities
RADIUS	Remote Authentication Dial In User Service
RCS	Records Control Schedule
RDA	Remote Database Access
RDBMS	Relational Database Management System
RDF	Resource Description Framework
RF	Radio Frequency
RFC	Request for Comments
RFI	Receiver Fixture Interface Alliance
RFP	Request for Proposals
RFX	Receiver/Fixture Interface
RMA	Records Management Application
RMON	Remote Monitoring
RPF	Raster Product Format
RSVP	Resource Reservation Protocol
RTI	Runtime Infrastructure
RTP	Real-Time Protocol
RTS	Runtime Services Interface
RTT	Radio Transmission Technologies
SA	Systems Architecture
SAASM	Selective Availability Anti-Spoofing Module
SAE	Society of Automotive Engineers
SAR	Synthetic Aperture Radar
SAR SDE	Synthetic Aperture Radar Support Data Extension
SATCOM	Satellite Communications
SBU	Sensitive, But Unclassified

SCC	Standards Coordinating Committee
SCPS	Space Communications Protocol Standards
SCSI-2	Small Computer Systems Interface-2
SDE	Support Data Extensions
SDF	Simulation Data Format
SDK	Software Development Kit
SDN	Secure Data Network
SDNS	Secure Data Network System
SEDRIS	Synthetic Environment Data Representation and Interchange Specification
SFP	Switch Function and Parametric Data Interface
SGML	Standard Generalized Markup Language
SHF	Super High Frequency
SIF	Standard Simulator Database Interchange Format
SIGINT	Signals Intelligence
SILS	Standard for Interoperable LAN Security
SIPE	Soldier Integrated Protective Ensemble
SIPRNET	Secure Internet Protocol Router Network
SIS	Signal-in-Space
SLP	Sensor Link Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMPTE	Society of Motion Picture and Television Engineers
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOM	Simulation Object Model
SONET	Synchronous Optical Network
SOO	Statement Of Objective
SOW	Statement of Work
SP	Security Protocol
SPDs	Special-Purpose Devices
SPIA	Standards Profile for Imagery Access
SPS	Standard Positioning Service
SQL	Structured Query Language
SR	Bellcore Special Report
SRM	Spatial Reference Model
SRS	Software Requirement Specification
SS	Soldier Systems
SSDB	Standard Simulator Data Base
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target

STANAG	Standardization Agreement [NATO]
STD	Standard
STEP	Standard for the Exchange of Product Model Data
STOU	Store Unique
SUS	Single UNIX Specification
SWM	Switch Matrix Interface
TA	Technical Architecture
TACO2	Tactical Communications Protocol 2
TADIL	Tactical Digital Information Link
TAFIM	Technical Architecture Framework for Information Management
TASG	Technical Architecture Steering Group
TC	Technical Committee
TCP	Transmission Control Protocol
TCSEC	Trusted Computer Security Evaluation Criteria
TDD	Time Division Duplex
TDL	Tactical Data Link
TDMA	Time Division Multiple Access
TED	TriTeal Enterprise Desktop
TEISS	The Enhanced Integrated Soldier System
TELNET	Telecommunications Network
TFTP	Trivial File Transfer Protocol
TGWG	Time and Geospatial Working Group
TIA	Telecommunications Industry Association
TIDP	Technical Interface Design Plan
TIS	Technical Interface Specification
TLS	Transport Layer Security
TMD	Theater Missile Defense
TMN	Telecommunications Management Network
TOG	The Open Group
TOS	Type-of-Service; Test Program to Operating System Interface (ATS Subdomain)
TP	Transport Protocol
TP0	Transport Protocol Class 0
TPD	Test Program Documentation Interface
TPS	Test Program Set
TR	Technical Report
TRIM	Test Resource Information Model
TRM	Technical Reference Model
TRSL	Test Requirements Specification Language
TSIG	Trusted Systems Interoperability Group

TSIX(RE)	Trusted Security Information Exchange for Restricted Environments
TSR	Test Strategy Report
U	Unclassified
UCA	Unified Cryptologic Architecture
UCA-TA	UCA-Technical Architecture
UCS	Universal Multiple-Octet Coded Character Set
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UML	Unified Modeling Language
UMS	Unattended MASINT Sensor
UN	United Nations
UNI	User-Network Interface
UPN	Universal Product Number
URL	Uniform Resource Locator
USA	United States Army
USACOM TMD	United States Atlantic Command Theater Missile Defense
USAF	United States Air Force
USCG	United States Coast Guard
USCS	United States Cryptologic System
USD(A&T)	Under Secretary of Defense (Acquisition and Technology)
USD(AT&L)	Under Secretary of Defense (Acquisition, Technology, and Logistics)
USIGS	United States Imagery and Geospatial Information Service
USIS	United States Imagery System
USMC	United States Marine Corps
USMTF	United States Message Text Format
USN	United States Navy
USNO	United States Naval Observatory
USSTRATCOM	United States Strategic Command
UTC	Coordinated Universal Time
UTC (USNO)	UTC as maintained at the U.S. Naval Observatory
UTR	Unit Under Test Requirements Interface
UUT	Unit Under Test
UVMap	Urban Vector Smart Map
VHDL	VHSIC Hardware Description Language
VHF	Very High Frequency
VHS	Vertical Helical Scan
VHSIC	Very High Speed Integrated Circuit
VISA	Virtual Instrument Standard Architecture

VISP	Video Imagery Standards Profile
VITC	Vertical Interval Time Code
VITD	VPF Interim Terrain Data
VLF	Very Low Frequency
VMap	Vector Map
VME	Versa Modulo Europa
VMF	Variable Message Format
VoIP	Voice Over Internet Protocol
VPF	Vector Product Format
VPN	Virtual Private Network
VPP	VXI*plug&play*
VRML	Virtual Reality Modeling Language
VSM	Video Systems Matrix
VTC	Video Teleconferencing
VTU	Video Teleconferencing Unit
VXI	VME Extensions for Instrumentation
W3C	World Wide Web Consortium
WGS	World Geodetic System
WMO	World Meteorological Organization
WS	Weapon Systems
WSHCI	Weapon Systems Human-Computer Interface
WSTAWG	Weapons Systems Technical Architecture Working Group
WVS*PLUS*	World Vector Shoreline Plus
WWW	World Wide Web
XHTML	Extensible HyperText Markup Language
XMI	XML Metadata Interchange
XML	Extensible Markup Language
XPATH	XML Path Language
XSL	XML Stylesheet Language
XSLT	XML Stylesheet Language Transformations

Appendix B: DoD JTA List of Mandated and Emerging Standards

For a list of the mandated and emerging standards in the DoD Joint Technical Architecture, go to DoD Joint Technical Architecture List of Mandated and Emerging Standards at <http://www-jta.itsi.disa.mil>.

Page intentionally left blank.

Appendix C: Document Sources

Organization	Source Location	URL
ACP	Allied Communications Publication	http://www-library.itsi.disa.mil/
AICC	Aviation Industry CBT Committee	http://www.aicc.org/
AMPEX	Ampex Corporation 500 Broadway, M.S. 1101 Redwood City, CA 94063	http://www.ampex.com
ANSI	American National Standards Institute, Attention Customer Service, 11 West 42nd St., New York, NY 10036	http://www.ansi.org
ASTM	American Society for Testing and Materials 100 Barr Harbor Drive West Conshohocken, PA 19428	http://www.astm.org
ATM FORUM	The ATM Forum 2570 West El Camino Real, Suite 304 Mountain View, CA 94040	http://www.atmforum.com
ATSC	Advanced Television Systems Committee 1750 K Street NW Suite 1200 Washington, DC 20006	http://www.atsc.org/
BELLCORE	Bellcore is now called Telcordia	http://www.telcordia.com/
BMDO	Ballistic Missile Defense Organization	http://www.acq.osd.mil/bmdo/bmdolink/html/organ.html
C2CDM	Command and Control Core Data Model (C2CDM) Information may be obtained from the referenced URL.	http://www-datadmn.itsi.disa.mil/
CCITT	International Telegraph and Telephone Consultative Committee (CCITT) is now known as International Telecommunications Union - Telecommunications Standardization Sector (ITU-T). See the ITU-T entry for source location information.	http://www.itu.int
COMPU SERVE INC.	CompuServe Incorporated	http://www.compuserve.com/gateway/default.asp

Organization	Source Location	URL
CORBA	Information about the Common Object Request Broker Architecture (CORBA) can be obtained from the Object Management Group (OMG). See the OMG entry for source location information.	http://www.omg.org http://www-corba.itsi.disa.mil/
DDM	DoD Defense Data Model (DDM) Information may be obtained from the referenced URL.	http://www-datadmn.itsi.disa.mil/
DDDS	Access to the Defense Data Dictionary System (DDDS) can be obtained on-line or through a PC Access Tool (PCAT). Developers should use both versions for full DDDS coverage. Information about the DDDS is available from: DISA JIEO, Center for Standards 701 South. Courthouse Road Arlington, VA 22204 USA. Tel: +1 703 735 3027	http://www-datadmn.itsi.disa.mil/ Take path: DoD Government Documents Data Administration (DATADMN)
DGI	DGI Working Group Digital Geographic Information Exchange Standard National Imagery and Mapping Agency ST/SOS Mail Stop P-24 12310 Sunrise Valley Drive Reston, VA 20191	http://www.digest.org/
DICOM	Digital Imaging and Communications in Medicine	n/a
DISA	DCA Circulars (DCAC) and DISA Circulars (DISAC) may be obtained from the Defense Information Systems Agency (DISA) Publications Office by written request on company letterhead and citing contract number. Defense Information Systems Agency Publications Office 701 South Courthouse Road Arlington VA 22204 USA Tel: +1 703 607 6548 Fax: +1 703 607 4661.	http://www.itsi.disa.mil/
DMSO	Defense Modeling and Simulation Office	http://www.dmso.mil/
DoD	Department of Defense OASD (PA)/DPC 1400 Defense Pentagon, Room 1E757 Washington, DC 20301	http://www.defenselink.mil/

Organization	Source Location	URL
DoD-HDBK	See MIL STD	http://astimage.daps.dla.mil/online/
DoD-STD	See MIL STD	http://astimage.daps.dla.mil/online/
DoD TRM	DoD TRM Version 1.0, 5 November 1999, The DoD Technical Reference Model (TRM) may be obtained from the DISA Center for Information Technology Standards web page.	http://www-trm.itsi.disa.mil
DOT	Department of Transportation	http://www.dot.gov/
EDISMC	The DoD EDI Standards Management Committee (EDISMC) coordinates EDI standardization activities with DoD. DoD-approved implementation conventions may be viewed on the World Wide Web at the referenced URL.	http://www-edi.itsi.disa.mil/
EIA	Electronic Industry Alliance (EIA) documents may be obtained from: Global Engineering Documents, An IHS Company 15 Inverness Way East Englewood, CO 80112 USA Tel: +1 800 854 7179	http://www.global.ihs.com
FESMCC	The Federal Electronic Data Interchange (EDI) Standards Management Coordinating Committee (FESMCC) harmonizes the development of EDI transaction sets and message standards among Federal agencies. The final Architecture document (Streamlining Procurement Through Electronic Commerce) from the Federal Electronic Commerce Acquisition Program Management Office (ECAPMO) is now available.	http://ec.fed.gov/edi.htm
FIPS	Federal Information Processing Standards (FIPS) are available to DoD Organizations (See MIL STD); others must request copies of FIPS from: National Technical Information Service (NTIS) 5285 Port Royal Road Springfield, VA 22161-2171 USA. Tel: +1 800 553 6847	http://www.ntis.gov/search.htm
FTR	Federal Telecommunications Recommendation Defense Information Systems Agency (DISA) Joint Information Engineering Organization (JIEO) code JEBBC Fort Monmouth, NJ 07703 USA	http://disa.dtic.mil/disnvtc/standards.htm

Organization	Source Location	URL
HIBCC	Health Industry Business Communications Council 2525 East Arizona Biltmore Circle-Suite 127 Phoenix, AZ 85016 Tel: +1 602 381 1091	http://www.hibcc.org/
HL7	Health Level Seven, Inc. 3300 Washtenaw Avenue, Suite 227 Ann Arbor, MI 48104 Tel: +1 734 677 7777	http://www.hl7.org/
IAB	Internet Architecture Board (IAB) documents are available from Internet Engineering Task Force (IETF). See the IETF entry for source location information.	http://www.iab.org/ http://www.ietf.org
ICAO	International Civil Aviation Organization	http://www.icao.org/
IEEE	Secretary, IEEE Standards Board Institute of Electrical and Electronics Engineers, Inc P.O. Box 1331, 445 Hoes Lane Piscataway, NJ 08855-1331, USA Tel: +1 800 678 4333	http://www.standards.ieee.org
IETF	Internet Engineering Task Force SRI International, Room EJ291 Network Information Systems Center 333 Ravenswood Avenue Menlo Park, CA 94025, USA Email: mailserv@ds.internic.net (Include the phrase "Send rfcxxxx.txt" in the body of the message to obtain a copy of the corresponding RFC standard via email.)	http://www.ietf.org
INTEL	INTEL	http://www.intel.com
ISO	International Organization for Standardization (ISO) Standards can be obtained from: American National Standards Institute (ANSI) Attention Customer Service 11 West 42nd St., New York, NY 10036 USA Tel: +1 212 642 4900	http://www.ansi.org

Organization	Source Location	URL
ITSG	The Information Technology Standards Guidance (ITSG) may be obtained from the DISA Center for Standards (CFS) web page.	http://www.itsi.disa.mil/ Take path: Info Tech Stnds Guidance (ITSG) Ver 3.1 http://www-itsg.itsi.disa.mil/
ITU-T	International Telecommunications Union -Telecommunications Standardization Sector (ITU-T) standards may be obtained from: National Technical Information Service 5285 Port Royal Road Springfield, VA 22161 USA Tel: +1 800 553 6847	http://www.itu.int/
JTA	Information about the Joint Technical Architecture document can be obtained from the JTA web site.	http://www-jta.itsi.disa.mil/
MICROSOFT PRESS	Microsoft	http://www.microsoft.com/
MIL-HDBK	See MIL STD	http://astimage.daps.dla.mil/online/
MIL-PRF	See MIL STD	http://astimage.daps.dla.mil/online/
MIL-STD	Copies of military standards (MIL STD, DoD STD), and handbooks (MIL HDBK, DOD HDBK) are available from: DoDSSP Building 4 / Section D 700 Robins Avenue Philadelphia, PA 19111-5098 USA Tel: +1 215 697 2667/2179 (M-F, 7:30 AM-4:00 PM)	http://astimage.daps.dla.mil/online/
MISSI	Multilevel Information Systems Security Initiative (MISSI) product information (FORTEZZA, etc.) may be obtained by calling the MISSI Help Desk at: Tel: +1 800 466 4774 (1-800-GO-MISSI)	http://www.nsa.gov:8080/isso/index.html
NAWCADLKE	Copies of Naval Air Warfare Center Aircraft Division, NAWCADLKE-MISC-05-PD-003, Navy Standard Digital “Simulation Data Format (SDF)” can be obtained from: Naval Air Warfare Center ATE Software Center, Code 4.8.3.2, Bldg. 551-1, Lakehurst, NJ 08733 USA.	http://www.nawcad.navy.mil/index.cfm

Organization	Source Location	URL
NCSC	The Rainbow Series of documents from the National Computer Security Center (NCSC) may be obtained from: NSA-V21 9800 Savage Rd. Fort Meade, MD 20755 USA. Tel: +1 410 859 6091	http://www.radium.ncsc.mil/tpep/library/rainbow/index.html
NETSCAPE	Netscape	http://www.netscape.com/
NIST	National Institute of Standards and Technology (NIST) documents may be obtained from: National Technical Information Service (NTIS) 5285 Port Royal Road Springfield, VA 22161-2171 USA Tel: +1 800 553-6847	http://www.nist.gov/ http://www.ntis.gov/search.htm
NITF	National Imagery Transmission Format	http://164.214.2.51/ntb/baseline/format.htm
NSA	National Security Agency Central Security Service 9800 Savage Road Fort George G. Meade, MD 20755	http://www.nsa.gov:8080/
NTSDS	The National Target/Threat Signatures Data System [NTSDS] is a DOD migration system.	http://www.defenselink.mil/
OMG	Information about the Object Management Group (OMG) is available from the OMG Web site.	http://www.omg.org
OSF	Open Systems Foundation (OSF), X/Open, and Open Group documents may be obtained from: Open Group, Apex Plaza Forbury Road Reading, RG1 1AX England Tel: +44 118 9 508311 Fax: +44 118 9 500110	http://www.opengroup.org/publications/catalog
OPENGL	OpenGL	http://www.opengl.org/ http://www.sgi.com/software/opengl/manual.html

Organization	Source Location	URL
POSIX	Portable Operating System Interface is now Knowledge Software LTD	http://www.knosof.co.uk/posix.html http://www.knosof.co.uk/index.html
RCTA	RTCA, Inc. 1140 Connecticut Ave., NW, Suite 1020 Washington, DC 20036 Tel: +1 202 833 9339	http://www.rtca.org
RFC	See IETF	http://www.ietf.org
RSA	RSA Security Corporate Headquarters 20 Crosby Drive, Bedford, MA 01730 Tel: +1 877 RSA 4900	http://www.rsasecurity.com
SAE	Society of Automotive Engineers Tel: +1 877 606 7323	http://www.sae.org/
SMPTE	Society of Motion Picture and Television Engineers 595 West Hartsdale Avenue White Plains, NY 10607	http://www.smpte.org/
SR	Bellcore Special Report Tel: +1 800 521 2673	http://www.telcordia.com/
STANAG	STANAGs and other NATO standardization agreements may be obtained by DoD, Federal agencies, and their contractors from: Central U.S. Registry 3072 Army Pentagon Washington, D.C. 20301-3072 USA. Tel: +1 703 697 5943/6432 Fax: +1 703 693 0585 Contractor requests for documents should be forwarded through their COR (contracting officer representative) or other Government sponsor to establish need-to-know.	NA
TAFIM	Technical Architecture Framework for Information Management (TAFIM) information may be obtained from the DISA Technical Standards Website referenced URL.	http://www.its.disa.mil
TELCORDIA	(Formerly Bellcore)	http://www.telcordia.com/

Organization	Source Location	URL
TIA	Telecommunications Industry Association (TIA) Standards can be obtained from: Global Engineering Documents 7730 Carondelet Ave,. Suite 407 Clayton, MO 63105 USA Tel: +1800 854 7179	http://global.ihs.com/
TIDP	Technical Interface Design Plans (TIDPs) may be obtained via the service POCs to the Joint Multi-TADIL CCB from: DISA/JIEO Center for Standards (CFS) TADIL Division, code JEBCA Tel: +1 703 735 3524	http://www.itsi.disa.mil
UML	Information about Unified Modeling Language (UML) can be obtained at the Object Management Group (OMG) web site.	http://www.omg.org
USA	United States Army	http://www.army.mil/
USAF	United States Air Force	http://www.af.mil/
USIGS	The United States Imagery and Geospatial Information Service (USIGS) is an umbrella term for the suites of systems formerly called the United States Imagery System (USIS) and the Global Geospatial Information and Services (GGIS). Information related to standards can be found on: the NIMA Standards and Interoperability web page, or contact NIMA: Tel: 703-755-5663 E-Mail: wesdockj@nima.mil	http://www.nima.mil/sandi
USIS	See USIGS	http://www.nima.mil/sandi
USN	United States Navy	http://www.navy.mil/
VXI	(VXI plug&play) System Alliance 6504 Bridge Point Parkway Austin, TX 78730	http://www.vxipnp.org/

Organization	Source Location	URL
W3C	World Wide Web Consortium (W3C) W3C Host general contact information W3C at MIT/LCS general contact information Massachusetts Institute of Technology Laboratory for Computer Science 545 Technology Square Cambridge, MA 02139	http://www.w3.org/
WMO	World Meteorological Organization (WMO) documents may be obtained from: American Meteorological Society Attention: WMO Publications Center 45 Beacon Street, Boston, MA 02108 USA	http://www.wmo.ch/
X/OPEN	See OSF Open Software Foundation	http://www.opengroup.org/publications/catalog

Page intentionally left blank.

Appendix D: References

- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01A: Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems, 30 June 1995.
- Joint Chiefs of Staff. Joint Vision 2010. Chairman of the Joint Chiefs of Staff, 5126 Joint Staff, Pentagon, Washington, D.C., 20318-5126, June 1997.
- Defense Management Report Decision (DMRD) 918: Defense Information Infrastructure, September 15, 1992.
- Defense Standardization Program (DSP) 4120.3-M: Policies and Procedures. Office of the Assistant Secretary of Defense, Production and Logistics, July 1993.
- Department of Defense Directive 4630.5: Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems. November 12, 1992.
- Department of Defense Regulation (DoDR) 5000.2-R: Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, March 15, 1996.
- Department of Defense Directive (DoDD) 5000.59: DoD Modeling and Simulation (M&S) Management, January 4, 1994.
- Department of Defense 5000.59-P: DoD Modeling and Simulation (M&S) Master Plan (MSMP), October 1995.
- Department of Defense Directive (DoDD) 8320.1: Data Administration, September 26, 1991.
- Department of Defense Technical Reference Model (DoD TRM), Version 1.0, 5 November 1999.
- IEEE 610.12A-1990: IEEE Standard Glossary of Software Engineering Terminology.
- IEEE P1029.3:19xx, Test Requirements Specification Language (TRSL).
- IEEE 1226.11:19xx, ABBET Test Resource Information Model (TRIM).
- IEEE 1232, Artificial Intelligence Exchange and Services Tie to All Test Environments (AI-ESTATE).
- IEEE 1232.1:1997, Artificial Intelligence Exchange and Services Tie to All Test Environments (AI-ESTATE): Data and Knowledge Specification.
- IEEE 1232.2, Artificial Intelligence Exchange and Services Tie to All Test Environments (AI-ESTATE)
- Electronic Industry Association: Electronic Design Interchange Format (EDIF), 19xx.
- Information Technology Management Reform Act (ITMRA) (also known as Clinger-Cohen Act of 1996 (Public Law 104-106).
- Memorandum: Executive Agent for DoD Information Standards, 24 March 1993.
- Memorandum: Paul A. Strassman: Open Systems Implementation, May 23, 1991.
- Memorandum: Secretary of Defense: Specifications and Standards – A new Way of Doing Business, June 1994.
- Office of Management and Budget Circular No. A-119: Federal Participation in the Development and Use of Voluntary Standards, October 20, 1993.

- Public Law 104-106: Clinger-Cohen Act of 1996, February 10, 1996 (formerly the Information Technology Management Reform Act of 1996).
- Public Law 104-113: National Technology Transfer and Advancement Act of 1995. 104th Congress, March 7, 1996.

Appendix E: JTA Relationship to DoD Standards Reform

DOD (Specifications and) Standards Reform Background

The DoD Standards Reform was begun in June 1994 when the Secretary of Defense issued his memorandum entitled "Specifications and Standards - A New Way of Doing Business." The Secretary of Defense directed that performance-based specifications and standards or nationally-recognized private sector standards be used in future acquisitions. The intent of this initiative is to eliminate non-value added requirements, and thus to reduce the cost of weapon systems and materiel; remove impediments to getting commercial state-of-the-art technology into our weapon systems; and integrate the commercial and military industrial bases to the greatest extent possible. The Defense Standards Improvement Council (DSIC) directs implementation of the Reform. The DSIC has interpreted and extended the Reform policy through a series of numbered OSD policy memos. These policy memos and other DSIC decisions, newsletters and other standardization related information are posted on the Defense Standardization Program (DSP) World Wide Web home page at: <http://www.dsp.dla.mil/>.

The JTA and the DoD Standards Reform

The standards and specifications and other standardization documents identified in the Joint Technical Architecture (JTA) can be cited in solicitations without conflicting with the DoD Standards Reform. All JTA standards have been granted Department-wide exemption from the waiver requirement by the Defense Standards Improvement Council. Mandatory application of JTA standards to acquisition solicitations is authorized. Contrary to interpretations that have been made in the recent past by some DoD organizations, the DoD Standards Reform is not eliminating military standards and specifications nor precluding their use. What the Reform is trying to eliminate is the automatic development and imposition of military-unique standards and specifications as the cultural norm. The JTA calls out non-Government standards in every case where it makes sense and where it will lead to the use of commercial products and practices that meet the DoD's needs. The JTA only calls out Military and Federal standards and specifications in those instances where no non-Government standard exists that is cost effective and meets the requirement or where the use of the non-Government standard must be clarified to enable interoperability of DoD systems.

Reform Waiver Policy

Policy Memo 95-1 establishes procedures for waivers for use of specifications and standards cited as requirements in solicitations. These waiver procedures apply to the types of standards that fall under the province of the Defense Standardization Program and are indexed in the DoD Index of Standards and Specifications (DoDISS). Specifically of relevance to the JTA, Policy Memo 95-1 states that non-Government standards, Interface Standards, Federal Information Processing Standards (FIPS), and Performance Specifications do not require waivers. Also, Policy Memo 95-9 provides that international standardization agreements such as NATO STANAGs (and ACPs) do not require waivers. Federal Telecommunications Standards (FED-STD) do not require a waiver when they qualify as interface standards. All of the above waiver-free document types encompass most of the standards cited in the JTA. The DSP Home Page provides lists of waiver-free standards and in the near future the DoDISS will indicate those standards that can be used without a waiver.

Non-DoDISS Standards Not Subject to the Reform Waiver Policy

There are a small number of JTA standards that are not among the types of Government standards that are indexed in the DoDISS and are therefore not subject to the Reform waiver policy. Therefore, they also do not require a waiver to be cited in a solicitation. However, the citation of these non-DoDISS

standards in solicitations must comply with Service/Agency requirements for preparation and approval of performance-based program unique specifications. A system specification used to procure a C4I system or a weapon system is a program unique specification. Procedures for preparing performance specifications are provided in MIL-STD-961D, Defense Specifications, Change 1, 22 August 1995 and in the DSP Performance Specification Guide, SD-15, dated 29 June 1995. MIL-STD-961D defines a performance specification as follows: "A specification that states requirements in terms of the required results with criteria for verifying compliance, but without stating the methods for achieving the required results. A performance specification defines the functional requirements for the item, the environment in which it must operate, and interface and interchangeability characteristics." By this definition, standards that define "interface" characteristics can be properly cited in a performance specification. Therefore, JTA non-DoDISS standards that are used to define interface characteristics are not in conflict with service/agency requirements for preparation and approval of performance-based program unique specifications.

Interface Standards Are Waiver-Free

Most JTA standards qualify as Interface Standards. Policy Memo 95-6 defines the five types of DoD-prepared standards as: interface standards, standard practices, test method standards, manufacturing process standards, and design criteria standards. Policy Memo 95-1 states that of these types, interface standards and standard practices do not require a waiver when cited in a solicitation. MIL-STD-962C (a standard practice) provides definitions, format, and content direction for military standards. It defines an interface standard as follows: "A standard that specifies the physical, functional, or military operational environment interface characteristics of systems, subsystems, equipment, assemblies, components, items or parts to permit interchangeability, interconnection, interoperability, compatibility, or communications." The use of military and Federal interface standards in solicitations is fully compliant with the DoD Standards Reform.

Non-Government Standards Vs. Military/Federal Standardization Documents

One of DoD's key acquisition reform goals is to reduce acquisition costs and remove impediments to commercial-military integration by emulating commercial buying practices wherever possible. Thus, for any processes, practices, or methods that are described by a non-Government standard used by Commercial firms and which meet DoD's needs, DoD activities should also be using a non-Government standard instead of applying, developing, or revising a military or Federal Standard. The standards selected for the JTA are predominantly non-Government standards. Military or Federal standards have been selected for the JTA only in those instances where non-Government standards failed to satisfy the DoD needs. In most of those instances, in fact, the military or Federal standard is a profile of one or more non-Government standards. The military or Federal profile identifies the chosen classes, subsets, options, and parameters of one or more base standards necessary for achieving interoperability (or other function). In some instances, the profile specifies unique interface requirements not satisfied by the non-Government standard. Therefore the JTA complies fully with this key acquisition reform goal.

Appendix F: Glossary

Note: Where two textual variants of the same term, e.g., “real time” and “real-time” occur in the document, both are shown.

Access Control

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

Accreditation

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

Activity Model (IDEF0)

A graphic description of a system or subject that is developed for a specific purpose and from a selected viewpoint. A set of one or more IDEF0 diagrams that depict the functions of a system or subject area with graphics, text and glossary. (FIPS Pub 183, Integration Definition For Function Modeling (IDEF0), December 1993)

Aggregate-Level Simulation Protocol (ALSP)

A family of simulation interface protocols and supporting infrastructure software that permit the integration of distinct simulations and war games. Combined, the interface protocols and software enable large-scale, distributed simulations and war games of different domains to interact at the combat object and event level. The most widely known example of an ALSP confederation is the Joint/Service Training Confederation (CBS, AWSIM, JECEWSI, RESA, MTWS, TACSIM, CSSTSS) that has provided the backbone to many large, distributed, simulation-supported exercises. Other examples of ALSP confederations include confederations of analytical models that have been formed to support U.S. Air Force, U.S. Army, and U.S. TRANSCOM studies. (DoD 5000.59-P, “Modeling and Simulation Master Plan,” October 1995, authorized by DoD Directive 5000.59, January 4, 1994)

American National Standards Institute (ANSI)

The principal standards coordination body in the U.S. ANSI is a member of the ISO.

Application Platform

- The collection of hardware and software components that provide the services used by support and mission-specific software applications. (DoD TRM, Version 1.0, 5 November 1999)
- 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, Version 1.0, 5 November 1999)

Application Platform *Entity*

The term ‘application platform *entity*’ is used when referencing the DoD TRM, as opposed to referencing an actual hardware platform (physical implementation). (DoD TRM, Version 1.0, 5 November 1999)

Application Program Interface (API)

- The interface, or set of functions, between the application software and the application platform. (NIST Special Publication 500-230; DoD TRM, Version 1.0, 5 November 1999)
- The means by which an application designer enters and retrieves information. (DoD TRM, Version 1.0, 5 November 1999)

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 applications 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, Version 1.0, 5 November 1999)

Architecture

Architecture has various meanings, depending upon its contextual usage. (1) The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time. (2) Organizational structure of a system or component. (IEEE STD 610.12-1990; DoD TRM, Version 1.0, 5 November 1999) or;

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. (OSJTF)

Authentication

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

CBR

Circuit (voice and telephony) traffic over ATM.

Character-Based Interface

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

Combatant Command

A unified or specified command with a broad continuing mission under a single commander [Commander-in-Chief, CINC] established and so designated by the President, through the Secretary of Defense with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic [e.g., Middle East, Central Command] or functional [e.g., military equipment and personnel transport, Transportation Command] responsibilities. [Source—Joint Pub 1-02, 10 June 1998]

Unless otherwise directed by the President or Secretary of Defense, the authority, direction, and control of the Commander of a Unified or Specified Combatant Command with respect to all the commands and forces assigned to that command [including Headquarters, Service, and Agency Components] include the command functions of giving authoritative direction to subordinate commands and forces necessary to carry out missions assigned to the command... [Source: DoD Directive 5100.1, "Functions of the Department of Defense and Its Major Commands," September 25, 1987].

Command and Control

The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (Joint Pub 1-02)

Command, Control, Communications, and Computer Systems

Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations. (Joint Pub 1-02)

Commercial Item

- Any item customarily used by the general public for other than governmental purposes, that has been sold, leased, or licensed to the general public, or that has been offered for sale, lease, or license to the general public.
- Any item that evolved from an item described above through advances in technology or performance that is not yet available in the commercial market, but will be available in time to meet the delivery requirements of the solicitation.
- 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 above.
- Any combination of items meeting the requirements above or below that are of a type customarily combined and sold in combination to the general public.
- Installation services, maintenance services, repair services, training services, and other services if such services are procured for support of any item referred to above, if the sources of such services:
  - offers such services to the general public and DoD simultaneously and under similar terms and conditions and
  - offers to use the same work force for providing DoD with such services as the source used for providing such services to the general public.
- Services offered and sold competitively, in substantial quantities, in the commercial marketplace based on established catalog prices of specific tasks performed and under standard commercial terms and conditions.
- Any item, combination of items, or service referred to above notwithstanding the fact that the item or service is transferred between or among separate divisions, subsidiaries, or affiliates of a contractor.
- A nondevelopmental item developed exclusively at private expense and sold in substantial quantities, on a competitive basis, to State and local governments.

(Standardization Document [SD-2], Buying Commercial and Nondevelopmental Items: A Handbook. Office of the Under Secretary of Defense for Acquisition and Technology, April 1996.)

Commercial off-the-Shelf (COTS)

- See the definition of Commercial Item found above. (OSJTF 1995).
- Refers to an item of hardware or software that has been produced by a contractor and is available for general purchase. Such items are at the unit level or higher. Such items must have been sold and delivered to government or commercial customers, must have passed customer's acceptance testing, be operating under customer's control, and within the user environment. Further, such items must have meaningful reliability, maintainability, and logistics historical data. (DoD TRM, Version 1.0, 5 November 1999)

Compliance

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

Conceptual Model of the Mission Space (CMMS)

One of the three components of the DoD Common Technical Framework (CTF). They are first abstractions of the real world and serve as a frame of reference for simulation development by capturing the basic information about important entities involved in any mission and their key actions and interactions. They are simulation-neutral views of those entities, actions, and interactions occurring in the real world. (DoD 5000.59-P, "Modeling and Simulation Master Plan," October 1995, authorized by DoD Directive 5000.59, January 4, 1994)

Confidentiality

- The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (Source: RFC 2828, Internet Security Glossary, May 2000)
- Assurance that information is not disclosed to unauthorized entities or processes. (Source: National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009)

Configuration Management

A discipline applying technical and administrative direction and surveillance to: (1) identify and document the functional and physical characteristics of a configuration item, (2) control changes to those characteristics, and (3) record and report changes to processing and implementation status. (DoD TRM, Version 1.0, 5 November 1999)

Coordinated Universal Time (UTC)

Time scale, based on the second (SI), as defined and recommended by the CCIR and maintained by the Bureau International des Poids et Mésures (BIPM).

Data Dictionary

A specialized type of database containing metadata that is managed by a data dictionary system; a repository of information describing the characteristics of data used to design, monitor, document, protect, and control data in information systems and databases; an application of a data dictionary system. (DoD 8320.1-M-1, "Data Element Standardization Procedures," January 15, 1993, authorized by DoD Directive 8320.1, September 26, 1991)

Data Integrity

- 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.
- The property that data has not been exposed to accidental or malicious alteration or destruction.

Data Model

In a database, the user's logical view of the data in contrast to the physically stored data, or storage structure. A description of the organization of data in a manner that reflects the information structure of an enterprise. (DoD 8320.1-M-1, "Data Element Standardization Procedures," January 15, 1993, authorized by DoD Directive 8320.1, September 26, 1991)

Designated Approving Authority (DAA)

The official with the authority to formally assume responsibility for operating an Automated Information System (AIS) or network at an acceptable level of risk. (NSTISSI No. 4009)

Digital Signature

The digital signature allows a message originator to sign (cover) data (e.g. the Hash value). This provides the recipient with the means to verify the identity of the originator (user authentication and non-repudiation).

Distributed Interactive Simulation (DIS)

Program to electronically link organizations operating in the four domains: advanced concepts and requirements; military operations; research, development, and acquisition; and training. A synthetic environment within which humans may interact through simulation(s) at multiple sites networked using compliant architecture, modeling, protocols, standards, and databases. (DoD 5000.59-P, "Modeling and Simulation Master Plan," October 1995, authorized by DoD Directive 5000.59, January 4, 1994)

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.

Element

A service area, interface, or standard within the JTA document. The definitions below are abbreviated versions of those appearing elsewhere in the JTA Glossary.

- Service Area – a set of system capabilities grouped by functional areas. Both the DoD Technical Reference Model and the JTA define set(s) of service areas common to every system.
- Interface – a boundary between two functional areas in a reference model.
- Standard – a document that establishes uniform engineering and technical requirements. The mandated standards in the JTA are grouped by their applicable service areas.

Electronic Business/Electronic Commerce

The interchange and processing of information via electronic techniques for accomplishing transactions based upon the application of commercial standards and practices. An integral part of implementing EB/EC is the application of business process improvement or reengineering to streamline business processes prior to the incorporation of technologies facilitating the electronic exchange of business information.

External Environment Interface (EEI)

The interface that supports information transfer between the application platform and the external environment. (NIST Special Publication 500-230; DoD TRM, Version 1.0, 5 November 1999)

Federate

A member of an HLA Federation. All applications participating in a Federation are called Federates. In reality, this may include Federate Managers, data collectors, live entity surrogates, simulations, or passive viewers. See HLA Glossary: <http://www.dmso.mil/projects/hla/docslib/hlagloss.html>.

Federation

A named set of interacting federates, a common federation object model, and supporting RTI, that are used as a whole to achieve some specific objective. See HLA Glossary: <http://www.dmso.mil>.

Federation Object Model (FOM)

An identification of the essential classes of objects, object attributes, and object interactions that are supported by an HLA federation. In addition, optional classes of additional information may also be specified to achieve a more complete description of the federation structure and/or behavior. See HLA Glossary: <http://www.dmso.mil>.

Government off-the-shelf (GOTS)

Software applications, modules, or objects developed for Government departments or agencies and subsequently made available to other Government entities. GOTS software often will be found in reuse repositories maintained to facilitate and encourage its distribution and use.

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.).

Hash

The Hash function provides a check for data integrity.

High-Level Architecture (HLA)

Major functional elements, interfaces, and design rules, pertaining as feasible to all DoD simulation applications, and providing a common framework within which specific system architectures can be defined. See HLA Glossary at <http://www.dmso.mil>.

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 tool kit components from more than one user interface style.

Imagery

Collectively, the representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. (JCS)

Information Technology (IT)

- The term "information technology," with respect to an executive agency means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.
- The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
- Notwithstanding the subparagraphs above the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (Information Technology Management Reform Act of 1996. See: <http://www.c3i.osd.mil>.

Institute of Electrical and Electronics Engineers (IEEE)

An accredited standards body that has produced standards such as the network-oriented 802 protocols and POSIX. Members represent an international cross-section of users, vendors, and engineering professionals. (DoD TRM, Version 1.0, 5 November 1999)

Intelligence

- The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.
- Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (Joint Pub 1-02)

Interactive Model

A model that requires human participation. Syn: human-in-the-loop. ("A Glossary of Modeling and Simulation Terms for Distributed Interactive Simulation (DIS)," August, 1995)

Interconnections

The manual, electrical, electronic, or optical communications paths/linkages between the systems. Includes the circuits, networks, relay platforms, switches, etc., necessary for effective communications.

Interface

A shared boundary between two functional units. A functional unit is referred to as a entity when discussing the classification of items related to application portability.

International Electrotechnical Commission (IEC)

An international standards body similar to ISO, but limited by its charter to standards in the electrical and electrotechnical areas. In 1987, the ISO and IEC merged ISO Technical Committee 97 and IEC Technical Committees 47B and 83 to form ISO/IEC Joint Technical Committee (JTC) 1, which is the only internationally recognized committee dealing exclusively with information technology standards.

International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from some 100 countries, one from each country. ISO is a non-governmental organization, established to promote the development of standardization and related activities in the

world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity. ISO's work results in international agreements, which are published as International Standards.

International Telecommunications Union - Telecommunications Standardization Sector (ITU-T)

ITU-T, formerly called the Comité Consultatif International de Télégraphique et Téléphonique (CCITT), is part of the International Telecommunications Union, a United Nations treaty organization. Membership and participation in ITU-T is open to private companies; scientific and trade associations; and postal, telephone, and telegraph administrations. Scientific and industrial organizations can participate as observers. The U.S. representative to ITU-T is provided by the Department of State. Since ITU-T does not have the authority of a standards body nor the authority to prescribe implementation of the documents it produces, its documents are called recommendations rather than standards.

Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security). The IETF is a subdivision of the Internet Architecture Board (IAB) responsible for the development of protocols, their implementations, and standardization.

Interoperability

- The ability of two or more systems or components to exchange data and use information. (IEEE STD 610.12)
- The ability of two or more systems to exchange information and to mutually use the information that has been exchanged. (Army Science Board)

Interworking

The exchange of meaningful information between computing elements (semantic integration), as opposed to interoperability, which provides syntactic integration among computing elements.

Joint Task Force

A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. Also called JTF. [Source—Joint Pub 1-02, 10 June 1998] [The JTF includes a Headquarters element and all of the Service Expeditionary Forces that support the Joint Task Force mission.]

Joint Technical Committee (JTC) 1

JTC1 was formed in 1987 by merger of ISO Technical Committee 97 and IEC Technical Committees 47B and 83 to avoid development of possibly incompatible information technology standards by ISO and IEC. ANSI represents the U.S. government in ISO and JTC1.

Key Exchange

The key is securely transmitted to the recipient by a secure Key Exchange. The Key Exchange process wraps (similar to encrypt) the key necessary to implement the encryption algorithm.

Legacy Environments

Legacy environments could be called legacy architectures or infrastructures and as a minimum consist of a hardware platform and an operating system. Legacy environments are identified for phase-out, upgrade, or replacement. All data and applications software that operate in a legacy environment must be categorized for phase-out, upgrade, or replacement. (DoD TRM, Version 1.0, 5 November 1999)

Legacy Standard

A JTA standard that is a candidate for phase-out, upgrade, or replacement. A legacy standard may be an obsolete standard without an upgrade path, or an older version of a currently mandated JTA standard. A legacy standard is generally associated with an existing or "legacy system," although it may be necessary in a new or upgraded system when an interface to a legacy system is required. (JTADG)

Legacy Systems

Systems that are candidates for phase-out, upgrade, or replacement. Generally legacy systems are in this category because they do not comply with data standards or other standards. Legacy system workloads must be converted, transitioned, or phased out (eliminated). Such systems may or may not operate in a legacy environment. (DoD TRM, Version 1.0, 5 November 1999)

Live, Virtual, and Constructive Simulation

The categorization of simulation into live, virtual, and constructive is problematic because there is no clear division between these categories. The degree of human participation in the simulation is infinitely variable, as is the degree of equipment realism. This categorization of simulations also suffers by excluding a category for simulated people working real equipment (e.g., smart vehicles). (DoD 5000.59-P, "Modeling and Simulation Master Plan," October 1995, authorized by DoD Directive 5000.59, January 4, 1994)

- **Live Simulation**. A simulation involving real people operating real systems.
- **Virtual Simulation**. A simulation involving real people operating simulated systems. Virtual simulations inject human-in-the-loop (HITL) in a central role by exercising motor control skills (e.g., flying an airplane), decision skills (e.g., committing fire control resources to action), or communication skills (e.g., as members of a C4I team)
- **Constructive Model or Simulation**. Models and simulations that involve simulated people operating simulated systems. Real people stimulate (make inputs) to such simulations, but are not involved in determining the outcomes.

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. (SD-2, April 1996)

Metadata

Information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings. (DoD 8320.1-M-1, Data Standardization Procedures, August 1997)

Model

A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. ("A Glossary of Modeling and Simulation Terms for Distributed Interactive Simulation (DIS)," August, (DoD Directive 5000.59, "DoD Modeling and Simulation (M&S) Management,"

January 4, 1994); (DoD 5000.59-P, "Modeling and Simulation Master Plan," October 1995, authorized by DoD Directive 5000.59, January 4, 1994).

Modeling and Simulation (M&S)

The use of models, including emulators, prototypes, simulators, and stimulators, either statically or over time, to develop data as a basis for making managerial or technical decisions. The terms "modeling" and "simulation" are often used interchangeably. ("M&S Educational Training Tool (MSETT), Navy Air Weapons Center Training Systems Division Glossary," April 28, 1994)

Motif

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

Multimedia

The presentation of information on a medium using any combination of video, sound, graphics, animation, and text; using various input and output devices.

National Institute of Standards and Technology (NIST)

The division of the U.S. Department of Commerce that ensures standardization within Government agencies. NIST was formerly known as the National Bureau of Standards. NIST develops and maintains Federal Information Processing Standards (FIPS) PUBS, the standards the Federal Government uses in its procurement efforts. Federal agencies, including DoD, must use these standards where applicable.

National Security System

- The term "national security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which: (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) subject to subsection (b), is critical to the direct fulfillment of military or intelligence missions.
- LIMITATION.-Subsection (a)(5) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). Information Technology Management Reform Act of 1996. See: <http://www.c3i.osd.mil>.

Nondevelopmental Item (NDI)

- Any previously developed item used exclusively for governmental purposes by a U.S. Federal, State or Local government agency or a foreign government with which the U.S. has a mutual defense cooperation agreement.
- Any item . . . that requires only minor modification in order to meet the requirements of the procuring agency.
- Any item currently being produced that does not meet the requirement of . . . solely because the item is not yet in use.

Object Model

A specification of the objects intrinsic to a given system, including a description of the object characteristics (attributes) and a description of the static and dynamic relationships (associations) that exist between objects. See HLA Glossary: <http://www.dmso.mil>.

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
- Use of standards which are developed/adopted by industrially recognized standards bodies
- Definition of all aspects of system interfaces to facilitate new or additional systems capabilities for a wide range of applications
- 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, body of data, or user can be transferred from one hardware or software environment to another. (DoD TRM, Version 1.0, 5 November 1999)

Practice

A recommended implementation or process that further clarifies the implementation of a standard or a profile of a standard. (VISP [Video Imagery Standards Profile])

Profile of a Standard

An extension to an existing, approved standard that further defines the implementation of that standard in order to ensure interoperability. A profile is generally more restrictive than the base standard it was extracted from. (VISP)

Protocol Data Unit (PDU)

DIS terminology for a unit of data that is passed on a network between simulation applications. (DoD 5000.59-P, "Modeling and Simulation Master Plan," October 1995, authorized by DoD Directive 5000.59, January 4, 1994)

Real Time, also 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)
- Absence of delay, except for the time required for transmission. (DoD HCI Style Guide)

Real-Time Control System

Systems capable of responding to external events with negligible delays. (DoD HCI Style Guide)

Real-Time Systems

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

Reconnaissance

A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (Joint Pub1-02)

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 models provide a mechanism for identifying key issues associated with portability, scalability, and interoperability. Most importantly, reference models will aid in the evaluation and analysis of domain-specific architectures. (TRI-SERVICE Open Systems Architecture Working Group)

Runtime Infrastructure (RTI)

The general-purpose distributed operating system software that provides the common interface services during the runtime of an HLA federation. See HLA Glossary: <http://hla.dmso.mil/hla/general/hlagloss.html>.

Scalability, Scaleability

- The capability to adapt hardware or software to accommodate changing work loads. (OSJTF)
- The ability to use the same application software on many different classes of hardware/software platforms from personal computers to super computers (extends the portability concept). The ability to grow to accommodate increased work loads.

Secondary Imagery Dissemination (SID)

The process for the post-collection electronic transmission or receipt of C3I-exploited non-original imagery and imagery-products in other than real- or near-real-time.

Security

- The combination of confidentiality, integrity, and availability.
- 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.

Service Area

A set of capabilities grouped into categories by function. The JTA defines a set of services common to DoD information systems.

Simulation Object Model (SOM)

A specification of the intrinsic capabilities that an individual simulation offers to federations. The standard format in which SOMs are expressed provides a means for federation developers to quickly determine the suitability of simulation systems to assume specific roles within a federation. See HLA Glossary: <http://www.dmso.mil>.

Specification

A document prepared to support acquisition that describes the essential technical requirements for purchased materiel and the criteria for determining whether those requirements are met. (DoD 4120.3-M)

Standard

A document that establishes uniform engineering or technical criteria, methods, processes, and practices. (DoD 4120.24-M)

Standards-Based Architecture

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 weapon system, and whose purpose is to ensure that a conformant system satisfies a specified set of requirements. (OSJTF)

Standards Profile

A set of one or more base standards and, where applicable, the identification of those classes, subsets, options, and parameters of those base standards necessary for accomplishing a particular function. (DoD TRM, Version 1.0, 5 November 1999)

Standard Simulator Database Interchange Format (SIF)

A DoD data exchange standard (MIL-STD-1821) adopted as an input/output vehicle for sharing externally created simulator databases among the operational system training and mission rehearsal communities.

Surveillance

The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. (Joint Pub1-02)

Synthetic Environment Data Representation and Interchange Specification (SEDRIS)

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.

Synthetic Environments (SE)

Interneted simulations that represent activities at a high level of realism from simulations of theaters of war to factories and manufacturing processes. These environments may be created within a single computer or a vast distributed network connected by local and wide area networks and augmented by super-realistic special effects and accurate behavioral models. They allow visualization of and immersion into the environment being simulated. (DoD 5000.59-P, "Modeling and Simulation Master Plan," October 1995, authorized by DoD Directive 5000.59, January 4, 1994); (CJCSI 8510.01, Chairman of the Joint Chiefs of Staff Instruction 8510.01, "Joint Modeling and Simulation Management," February 17, 1995)

System

- People, machines, and methods organized to accomplish a set of specific functions. (FIPS 11-3)
- An integrated composite of people, products, and processes that provides a capability or satisfies a stated need or objective. (DoD 5000.2)

Systems Architecture (SA)

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.

Technical Architecture (TA)

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.

Technical Reference Model (TRM)

A conceptual framework that provides the following:

- A consistent set of service and interface categories and relationships used to address interoperability and open system issues.
- Conceptual entities that establish a common vocabulary to better describe, compare, and contrast systems and components.
- A basis (an aid) for the identification, comparison, and selection of existing and emerging standards and their relationships.
- The framework is not an architecture, is not a set of standards, and does not contain standards.

Video

Electro-Optical imaging sensors and systems that generate sequential or continuous streaming imagery at specified rates. Video standards are developed by recognized bodies such as ISO, ITU, SMPTE, EBU, etc. (VISP)

Weapon Systems

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) See also National Security Systems.

Page intentionally left blank.