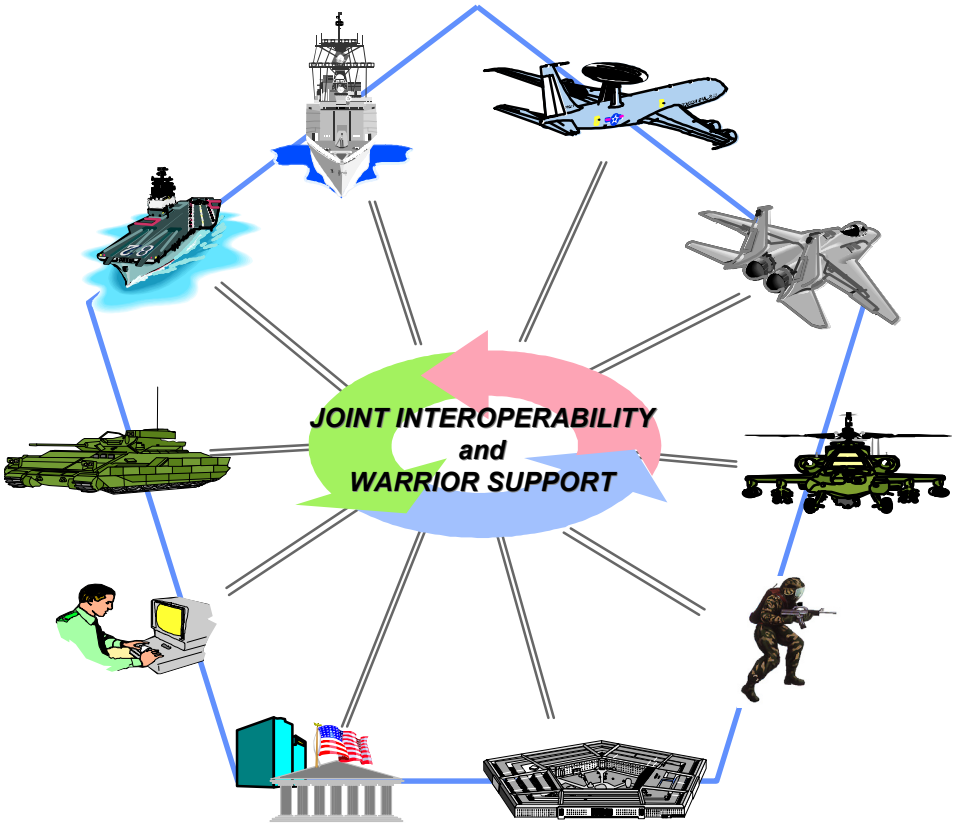
Department of Defense
Joint Technical Architecture



Version 5.1
12 September 2003

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 2020 (JV 2020) builds upon and extends the conceptual template established by Joint Vision 2010. JV 2020 guides the continuing transformation of America's Armed Forces and recognizes the importance of technical and intellectual innovation to the U.S. Military and its operations. The DoD Joint Technical Architecture (JTA) is crucial to achieving JV 2020.

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 3 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 subdomains 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; Common Operating Environment (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.

Page intentionally left blank.

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
1.2 Purpose 1
1.3 Scope (Applicability) 2
1.4 Background 2
1.5 Architectures Defined 3
1.5.1 Operational Architecture View 4
1.5.2 Technical Architecture View 4
1.5.3 Systems Architecture View 5
1.6 Relationships between the C4ISR Architecture Framework 2.0 and the DoD JTA 5
1.7 Document Organization 5
1.7.1 General Organization 5
1.7.2 Information Technology Standards 6
1.7.3 Domains and Subdomains 6
1.7.4 Appendices (Appendix A, B, C, D) 8
1.8 DoD Technical Reference Model 9
1.9 Key Considerations in Using the JTA 11
1.10 JTA Relationship to the Defense Standardization Program (DSP) 11
1.11 Standards Selection Criteria 11
1.12 Configuration Management 12

Section 2: Information Processing Standards 15
2.1 Introduction 15
2.2 Purpose 15
2.3 Scope (Applicability) 15
2.4 Background 15
2.5 Information Processing Services 15
2.5.1 Software Engineering Services 15
2.5.1.1 Common Operating Environment 15
2.5.1.1(a) Mandated 16
2.5.2 User Interface Services 16
2.5.2.1 User Interface Service — POSIX 16
2.5.2.1(a) Mandated 16
2.5.2.2 User Interface Service — Win32 16
2.5.2.2(a) Mandated 16
2.5.3 Data Management Services 16
2.5.3(a) Mandated 16
2.5.3(b) Emerging 17
2.5.4 Data Interchange Services 18
2.5.4.1 Document Interchange 18
2.5.4.1(a) Mandated 18
2.5.4.1(b) Emerging 19
2.5.4.2 Common Document Interchange Formats 21
2.5.4.2(a) Mandated 22
2.5.4.3 Graphics Data Interchange 23
2.5.4.3(a) Mandated 24
2.5.4.3(b) Emerging 24

2.5.4.4 Environmental Data Interchange . . . 24
2.5.4.4(a) Mandated. . . . 24
2.5.4.4(b) Emerging. . . . 24
2.5.4.4.1 Geospatial Data Interchange . . . 25
2.5.4.4.1(a) Mandated. . . . 25
2.5.4.4.2 Atmospheric and Oceanographic Data Interchange . . . 26
2.5.4.4.2(a) Mandated. . . . 26
2.5.4.4.2(b) Emerging. . . . 26
2.5.4.5 Still Imagery Data Interchange. . . . 27
2.5.4.5(a) Mandated. . . . 27
2.5.4.5(b) Emerging. . . . 28
2.5.4.6 Motion Imagery Data Interchange . . . 28
2.5.4.6.1 Motion Imagery Systems . . . 29
2.5.4.6.1(a) Mandated. . . . 29
2.5.4.6.2 Video Teleconference Systems . . . 29
2.5.4.6.3 Video Support Services . . . 29
2.5.4.6.3(a) Mandated. . . . 29
2.5.4.7 Audio Data Interchange . . . 30
2.5.4.7(a) Mandated. . . . 30
2.5.4.7.1 Audio Associated with Motion Imagery . . . 30
2.5.4.7.1.1 Audio for Motion Imagery Systems . . . 31
2.5.4.7.1.1(a) Mandated. . . . 31
2.5.4.7.1.2 Audio for Video Support Systems . . . 31
2.5.4.7.1.2(a) Mandated. . . . 31
2.5.4.7.2 Voice Encoder . . . 31
2.5.4.7.2(a) Mandated. . . . 31
2.5.4.7.2(b) Emerging. . . . 32
2.5.4.8 Data Interchange Storage Media . . . 32
2.5.4.8(a) Mandated. . . . 32
2.5.4.9 Time-of-Day Data Interchange. . . . 32
2.5.4.9(a) Mandated. . . . 32
2.5.4.10 Multimedia Data Interchange . . . 33
2.5.4.10(a) Mandated. . . . 33
2.5.4.10(b) Emerging. . . . 33
2.5.4.11 Calendaring and Scheduling . . . 33
2.5.4.11(a) Mandated. . . . 33
2.5.4.11(b) Emerging. . . . 33
2.5.5 Graphics Services . . . 33
2.5.5(a) Mandated. . . . 33
2.5.5(b) Emerging. . . . 33
2.5.6 Platform Communications Services . . . 33
2.5.7 Operating System Services . . . 33
2.5.7(a) Mandated. . . . 34
2.5.7(b) Emerging. . . . 35
2.5.8 Internationalization Services . . . 35
2.5.8(a) Mandated. . . . 35
2.5.9 Security Services . . . 36
2.5.10 System Management Services . . . 36
2.5.10(a) Mandated. . . . 36
2.5.10(b) Emerging. . . . 36
2.5.11 Distributed Computing Services . . . 36
2.5.11.1 Distributed-Object Computing . . . 36
2.5.11.1(a) Mandated. . . . 37
2.5.12 Environment Management . . . 37
2.5.12.1 Electronic Records Management . . . 37
2.5.12.1(a) Mandated. . . . 37
2.5.12.1(b) Emerging. . . . 37
2.5.12.2 Learning Technology . . . 37
2.5.12.2(a) Mandated. . . . 37

2.5.12.2(b) Emerging. . . . 38
2.5.12.3 Biometric Technology Services. . . . 38
2.5.12.3(a) Mandated. . . . 38

Section 3: Information Transfer Standards . . . 39
3.1 Introduction . . . 39
3.2 Purpose and Scope. . . . 39
3.3 Background . . . 39
3.4 End Systems Standards . . . 39
3.4.1 Host Standards . . . 40
3.4.1(a) Mandated. . . . 40
3.4.1.1 Electronic Mail . . . 40
3.4.1.1(a) Mandated. . . . 40
3.4.1.1(b) Emerging. . . . 40
3.4.1.2 Directory Services . . . 41
3.4.1.2.1 X.500 Directory Services. . . . 41
3.4.1.2.1(a) Mandated. . . . 41
3.4.1.2.1(b) Emerging. . . . 41
3.4.1.2.2 Lightweight Directory Access Protocol . . . 41
3.4.1.2.2(a) Mandated. . . . 41
3.4.1.2.2(b) Emerging. . . . 41
3.4.1.2.3 Domain Name System . . . 41
3.4.1.2.3(a) Mandated. . . . 42
3.4.1.2.3(b) Emerging. . . . 42
3.4.1.3 File Transfer . . . 42
3.4.1.3(a) Mandated. . . . 42
3.4.1.4 Remote Terminal . . . 42
3.4.1.4(a) Mandated. . . . 42
3.4.1.5 Network Time Synchronization. . . . 42
3.4.1.5(a) Mandated. . . . 42
3.4.1.6 Bootstrap Protocol . . . 43
3.4.1.6(a) Mandated. . . . 43
3.4.1.7 Configuration Information Transfer. . . . 43
3.4.1.7(a) Mandated. . . . 43
3.4.1.7(b) Emerging. . . . 43
3.4.1.8 Web Services . . . 43
3.4.1.8.1 Hypertext Transfer Protocol . . . 43
3.4.1.8.1(a) Mandated. . . . 43
3.4.1.8.2 Uniform Resource Locator . . . 43
3.4.1.8.2(a) Mandated. . . . 43
3.4.1.8.2(b) Emerging. . . . 44
3.4.1.9 Connectionless Data Transfer . . . 44
3.4.1.9(a) Mandated. . . . 44
3.4.1.10 Transport Services . . . 44
3.4.1.10.1 Transmission Control Protocol . . . 44
3.4.1.10.1(a) Mandated. . . . 44
3.4.1.10.2 User Datagram Protocol . . . 44
3.4.1.10.2(a) Mandated. . . . 44
3.4.1.10.3 Open Systems Interconnection Transport Over IP-Based Networks . . . 44
3.4.1.10.3(a) Mandated. . . . 44
3.4.1.10.3(b) Emerging. . . . 44
3.4.1.11 Network Services . . . 45
3.4.1.11(a) Mandated. . . . 45
3.4.1.11(b) Emerging. . . . 45
3.4.1.12 Quality of Service . . . 46
3.4.1.12(a) Mandated. . . . 46
3.4.1.12(b) Emerging. . . . 46
3.4.1.13 Voice Over IP . . . 46
3.4.1.13(a) Mandated. . . . 46

3.4.1.13(b) Emerging. . . . 46
3.4.1.14 Communication Protocols for High-Stress, Resource-Constrained Environments . . . 46
3.4.1.14(a) Mandated. . . . 46
3.4.1.14(b) Emerging. . . . 47
3.4.2 Video Teleconferencing Standards . . . 47
3.4.2(a) Mandated. . . . 47
3.4.2(b) Emerging. . . . 49
3.4.3 Facsimile Standards . . . 49
3.4.3.1 Analog Facsimile Standards . . . 50
3.4.3.1(a) Mandated. . . . 50
3.4.3.2 Digital Facsimile Standards . . . 50
3.4.3.2(a) Mandated. . . . 50
3.4.4 Imagery Dissemination Communications Standards. . . . 50
3.4.4(a) Mandated. . . . 50
3.4.5 Global Positioning System . . . 50
3.4.5(a) Mandated. . . . 50
3.4.5(b) Emerging. . . . 51
3.4.6 Identification Friend or Foe . . . 51
3.4.6(a) Mandated. . . . 51
3.4.6(b) Emerging. . . . 52
3.5 Network Standards . . . 52
3.5.1 Internetworking (Router) Standards . . . 52
3.5.1(a) Mandated. . . . 52
3.5.1(b) Emerging. . . . 52
3.5.2 Internet Protocol . . . 53
3.5.2(a) Mandated. . . . 53
3.5.2(b) Emerging. . . . 53
3.5.3 Internet Protocol Routing . . . 54
3.5.3.1 Interior Routers . . . 54
3.5.3.1(a) Mandated. . . . 54
3.5.3.2 Exterior Routers . . . 54
3.5.3.2(a) Mandated. . . . 54
3.5.4 Network Quality of Service Standards . . . 54
3.5.4.1 General Quality of Service Standards . . . 54
3.5.4.1(a) Mandated. . . . 54
3.5.4.1(b) Emerging. . . . 54
3.5.4.2 Voice Quality of Service Standards . . . 55
3.5.4.2(a) Mandated. . . . 55
3.6 Subnetworks. . . . 55
3.6.1 Local Area Network Access . . . 55
3.6.1(a) Mandated. . . . 55
3.6.1(b) Emerging. . . . 56
3.6.2 Point-to-Point Standards . . . 56
3.6.2(a) Mandated. . . . 56
3.6.2(b) Emerging. . . . 57
3.6.3 Combat Net Radio Networking . . . 57
3.6.3(a) Mandated. . . . 57
3.6.4 Integrated Services Digital Network . . . 57
3.6.4(a) Mandated. . . . 57
3.6.5 Asynchronous Transfer Mode . . . 58
3.6.5(a) Mandated. . . . 59
3.6.5(b) Emerging. . . . 60
3.6.6 Gigabit Ethernet . . . 61
3.6.6(a) Mandated. . . . 61
3.6.7 Mobile Cellular . . . 61
3.6.7(a) Mandated. . . . 61
3.6.7(b) Emerging. . . . 61
3.7 Transmission Media . . . 62
3.7.1 Military Satellite Communications . . . 62

3.7.1.1 Ultra High Frequency Satellite Terminal Standards . . . 62
3.7.1.1(a) Mandated. . . . 62
3.7.1.1(b) Emerging. . . . 63
3.7.1.2 Super High Frequency Satellite Terminal Standards . . . 63
3.7.1.2(a) Mandated. . . . 63
3.7.1.2(b) Emerging. . . . 64
3.7.1.3 Extremely High Frequency Satellite Payload and Terminal Standards. . . . 64
3.7.1.3(a) Mandated. . . . 64
3.7.2 Satellite State-of-Health Communication Standards . . . 64
3.7.2(a) Mandated. . . . 64
3.7.2(b) Emerging. . . . 65
3.7.3 Radio Communications . . . 66
3.7.3(a) Mandated. . . . 66
3.7.3(b) Emerging. . . . 67
3.7.3.1 Tactical Data Link Transmission Standards . . . 67
3.7.3.1(a) Mandated. . . . 67
3.7.4 Synchronous Optical Network Transmission Facilities . . . 67
3.7.4(a) Mandated. . . . 67
3.8 Network and Systems Management . . . 67
3.8.1 Data Communications Management . . . 68
3.8.1(a) Mandated. . . . 68
3.8.1(b) Emerging. . . . 68
3.9 Telecommunications Management . . . 69
3.9(a) Mandated. . . . 69

Section 4: Information Modeling, Metadata, and Information Exchange Standards . . . 71
4.1 Introduction . . . 71
4.2 Purpose. . . . 71
4.3 Scope (Applicability) . . . 71
4.4 Background . . . 71
4.5 Information Modeling. . . . 72
4.5.1 Activity Model. . . . 72
4.5.1(a) Mandated. . . . 72
4.5.2 Data Model . . . 72
4.5.2(a) Mandated. . . . 72
4.5.2(b) Emerging. . . . 73
4.5.3 Object Modeling . . . 73
4.5.3(a) Mandated. . . . 73
4.5.3(b) Emerging. . . . 73
4.6 DoD Data Architecture Implementation. . . . 73
4.6(a) Mandated. . . . 74
4.7 Data Definitions . . . 74
4.7(a) Mandated. . . . 74
4.7(b) Emerging. . . . 74
4.8 Information Exchange Standards . . . 74
4.8.1 Tactical Information Exchange Standards . . . 75
4.8.1.1 Bit-Oriented Formatted Messages . . . 75
4.8.1.1(a) Mandated. . . . 75
4.8.1.1(b) Emerging. . . . 76
4.8.1.2 Character-Based Formatted Messages . . . 76
4.8.1.2(a) Mandated. . . . 76
4.8.1.3 Binary Floating-Point Data Interchange . . . 76
4.8.1.3(a) Mandated. . . . 77
4.8.2 XML-based Information Exchange . . . 77

Section 5: Human-Computer Interface Standards . . . 79
5.1 Introduction . . . 79
5.2 Purpose. . . . 79
5.3 Scope (Applicability) . . . 79

5.4 Background . . . 79
5.5 General User Interface Design . . . 79
5.5.1 Graphical User Interface . . . 79
5.5.2 Character-Based Interfaces . . . 80
5.5.2(a) Mandated. . . . 80
5.6 Style Guides . . . 80
5.6.1 Commercial Style Guides . . . 80
5.6.1.1 X-Window Style Guides . . . 80
5.6.1.1(a) Mandated. . . . 80
5.6.1.2 Windows Style Guide . . . 80
5.6.1.2(a) Mandated. . . . 81
5.6.2 Domain-Level Style Guides . . . 81
5.6.2(a) Mandated. . . . 81
5.6.3 System-Level Style Guides . . . 81
5.7 Symbology . . . 82
5.7(a) Mandated. . . . 82

Section 6: Information Security Standards . . . 83
6.1 Introduction. . . . 83
6.2 Purpose . . . 83
6.3 Scope . . . 83
6.4 Computing Environment . . . 83
6.4.1 Applications . . . 83
6.4.1.1 Secure Web Browsing . . . 83
6.4.1.1(a) Mandated. . . . 83
6.4.1.2 Secure Messaging . . . 84
6.4.1.2(a) Mandated. . . . 84
6.4.1.3 Access Control. . . . 85
6.4.1.3.1 Identification and Authentication (I&A) Control: Passwords . . . 85
6.4.1.3.1(a) Mandated. . . . 85
6.4.1.3.1(b) Emerging. . . . 85
6.4.1.3.2 Authentication Servers . . . 85
6.4.1.3.2(a) Mandated. . . . 85
6.4.1.4 Data Labeling. . . . 85
6.4.1.5 Secure Session . . . 86
6.4.1.5(a) Mandated. . . . 86
6.4.1.5(b) Emerging. . . . 86
6.4.1.6 Secure File Transfer . . . 86
6.4.1.6(a) Mandated. . . . 86
6.4.1.6(b) Emerging. . . . 86
6.4.1.7 Secure Distributed Computing . . . 86
6.4.1.7(a) Mandated. . . . 86
6.4.1.7(b) Emerging. . . . 87
6.4.1.8 Operating System Security . . . 87
6.4.1.8(a) Mandated. . . . 87
6.4.1.8(b) Emerging. . . . 87
6.4.2 Cryptographic Security Services . . . 87
6.4.2.1 Encryption Algorithms . . . 87
6.4.2.1(a) Mandated. . . . 87
6.4.2.1(b) Emerging. . . . 87
6.4.2.2 Hash Algorithms . . . 88
6.4.2.2(a) Mandated. . . . 88
6.4.2.3 Signature Algorithms . . . 88
6.4.2.3(a) Mandated. . . . 88
6.4.2.4 Cryptographic Tokens . . . 88
6.4.2.5 Cryptographic APIs . . . 88
6.4.2.5(a) Mandated. . . . 88
6.4.2.5(b) Emerging. . . . 88
6.4.2.6 Cryptographic Key Algorithms . . . 89

6.4.2.6(a) Mandated. . . . 89
6.4.2.7 Cryptographic Modules. . . . 89
6.4.2.7(a) Mandated. . . . 89
6.5 Enclave Boundary . . . 89
6.5.1 Firewall . . . 89
6.5.1(a) Mandated. . . . 89
6.5.1(b) Emerging. . . . 90
6.5.2 Guards . . . 90
6.5.3 Remote Access . . . 90
6.5.4 Malicious Code . . . 90
6.6 Network and Infrastructure . . . 90
6.6.1 Network Layer . . . 90
6.6.1(a) Mandated. . . . 90
6.6.1(b) Emerging. . . . 91
6.6.2 Link Layer . . . 91
6.6.2(a) Mandated. . . . 91
6.6.2(b) Emerging. . . . 91
6.6.3 Physical Layer . . . 91
6.6.3(a) Mandated. . . . 91
6.6.3(b) Emerging. . . . 91
6.6.4 Naming Service . . . 92
6.6.4(a) Mandated. . . . 92
6.6.4(b) Emerging. . . . 92
6.6.5 Directory Service . . . 92
6.7 Supporting Infrastructures. . . . 92
6.7.1 Public-Key Infrastructure (PKI) . . . 92
6.7.1.1 PKI Certificates. . . . 93
6.7.1.1(a) Mandated. . . . 93
6.7.1.1(b) Emerging. . . . 93
6.7.1.2 PKI Operational Protocol and Exchange Formats . . . 93
6.7.1.2(a) Mandated. . . . 93
6.7.1.2(b) Emerging. . . . 94
6.7.1.3 PKI Management Protocols . . . 94
6.7.1.3(a) Mandated. . . . 94
6.7.1.3(b) Emerging. . . . 94
6.7.1.4 PKI API. . . . 94
6.7.1.4(a) Mandated. . . . 94
6.7.1.4(b) Emerging. . . . 95
6.7.1.5 PKI Cryptography . . . 95
6.7.1.5(a) Mandated. . . . 95
6.7.1.5(b) Emerging. . . . 95
6.7.2 Key Management Infrastructure . . . 95
6.7.2(a) Mandated. . . . 95
6.7.3 Intrusion Detection Systems (IDS). . . . 95
6.7.3.1 Intrusion Detection Devices . . . 95
6.7.3.1(a) Mandated. . . . 95
6.7.3.1(b) Emerging. . . . 95
6.7.3.2 Intrusion Detection Communications Protocol . . . 96
6.7.3.2(a) Mandated. . . . 96
6.7.3.2(b) Emerging. . . . 96
6.7.3.3 Intrusion Detection Message Exchange Format. . . . 96
6.7.3.3(a) Mandated. . . . 96
6.7.3.3(b) Emerging. . . . 96
6.8 Evaluation Criteria. . . . 96
6.8.1 Common Criteria . . . 96
6.8.1(a) Mandated. . . . 97

C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Domain . . . 99
C4ISR.1 Domain Description . . . 99
C4ISR.2 Purpose and Scope . . . 99
C4ISR.3 Applicability . . . 99
C4ISR.4 Information Processing Standards . . . 99
C4ISR.4.1 Common Ground Moving Target Indicator Data Format . . . 100
C4ISR.4.1(a) Mandated. . . . 100
C4ISR.4.1(b) Emerging. . . . 100
C4ISR.5 Information Transfer Standards . . . 100
C4ISR.5.1 Transmission Media . . . 100
C4ISR.5.1.1 Radio Communications . . . 100
C4ISR.5.1.1.1 Unattended MASINT Sensor Communication Standards . . . 100
C4ISR.5.1.1.1(a) Mandated. . . . 100
C4ISR.5.1.2 Network Standards . . . 100
C4ISR.5.1.2(a) Mandated. . . . 100
C4ISR.5.1.2(b) Emerging. . . . 101
C4ISR.5.1.3 Platform to Ground Station Direct Data Transfer Interface . . . 101
C4ISR.5.1.3(a) Mandated. . . . 101
C4ISR.5.1.3(b) Emerging. . . . 101
C4ISR.5.2 Payload-Platform Interface . . . 101
C4ISR.5.2.1 Internal Communications . . . 101
C4ISR.5.2.1.1 Fibre Channel . . . 102
C4ISR.5.2.1.1(a) Mandated. . . . 102
C4ISR.5.2.1.2 FireWire . . . 102
C4ISR.5.2.1.2(a) Mandated. . . . 102
C4ISR.5.2.2 Vehicle/Sensor Telemetry . . . 102
C4ISR.5.2.2(a) Mandated. . . . 102
C4ISR.5.3 Nuclear Command and Control Information Transfer. . . . 102
C4ISR.5.3(a) Mandated. . . . 103
C4ISR.6 Information Modeling, Metadata, and Information Exchange Standards . . . 103
C4ISR.6.1 Information Exchange Standards . . . 103
C4ISR.6.1.1 Target/Threat Data Interchange Standards . . . 103
C4ISR.6.1.1(a) Mandated. . . . 103
C4ISR.6.1.2 Nuclear Command and Control Information Exchange. . . . 103
C4ISR.6.1.2(a) Mandated. . . . 103
C4ISR.6.2 Sensor Link Protocol (SLP) Message Set . . . 104
C4ISR.6.2(a) Mandated. . . . 104
C4ISR.6.2(b) Emerging. . . . 104
C4ISR.7 Human-Computer Interface Standards . . . 104
C4ISR.7.1 Nuclear Command and Control HCI . . . 104
C4ISR.7.1(a) Mandated. . . . 104
C4ISR.7.1(b) Emerging. . . . 104
C4ISR.8 Information Security Standards . . . 104

C4ISR.CRY: Cryptologic Subdomain . . . 105
C4ISR.CRY.1 Subdomain Description . . . 105
C4ISR.CRY.2 Purpose and Scope . . . 105
C4ISR.CRY.3 Applicability . . . 105
C4ISR.CRY.4 Background . . . 105
C4ISR.CRY.5 Subdomain-Specific Services and Interfaces . . . 106
C4ISR.CRY.5.1 Small-Scale Special Purpose Devices . . . 106
C4ISR.CRY.5.1(a) Mandated. . . . 106
C4ISR.CRY.5.1(b) Emerging. . . . 106
C4ISR.CRY.5.2 Collaborative Data Sharing . . . 106
C4ISR.CRY.5.2(a) Mandated. . . . 107
C4ISR.CRY.5.2(b) Emerging. . . . 107

C4ISR.SR: Space Reconnaissance Subdomain . . . 109
C4ISR.SR.1 Subdomain Introduction . . . 109
C4ISR.SR.2 Information Processing Standards . . . 109
C4ISR.SR.2.1 Hardware Product Data Interchange . . . 109
C4ISR.SR.2.1(a) Mandated. . . . 109
C4ISR.SR.2.2 Object-Oriented Database Management . . . 111
C4ISR.SR.2.2(a) Mandated. . . . 111
C4ISR.SR.3 Information Transfer Standards . . . 111
C4ISR.SR.3.1 Synchronous Optical Network Transmission Facilities . . . 111
C4ISR.SR.3.1(a) Mandated. . . . 111
C4ISR.SR.4 Information Modeling, Metadata, and Information Exchange Standards . . . 111
C4ISR.SR.4(a) Mandated. . . . 111

CS: Combat Support Domain . . . 113
CS.1 Domain Description . . . 113
CS.2 Purpose and Scope . . . 113
CS.3 Applicability . . . 113
CS.4 Background . . . 113
CS.5 Core-Related Information Technology Categories . . . 113
CS.5.1 Document Interchange . . . 113
CS.5.1(a) Mandated. . . . 114
CS.5.2 Graphics Data Interchange . . . 114
CS.5.2(a) Mandated. . . . 114
CS.5.3 Product Data Interchange . . . 114
CS.5.3(a) Mandated. . . . 114
CS.5.3(b) Emerging. . . . 116
CS.5.4 Electronic Data Interchange . . . 117
CS.5.4(a) Mandated. . . . 117
CS.5.4(b) Emerging. . . . 117
CS.5.5 Information Modeling, Metadata, and Information Exchange Standards . . . 118
CS.5.5.1 Electronic Fingerprint Information Exchange Standards . . . 118
CS.5.5.1(a) Mandated. . . . 118
CS.5.6 Information Security Standards . . . 118
CS.6 Domain-Specific Standards . . . 118
CS.6.1 Electronic Business/Electronic Commerce . . . 118
CS.6.1.1 Smart Card Technology Standards . . . 118
CS.6.1.1(a) Mandated. . . . 119
CS.6.1.1(b) Emerging. . . . 119

CS.ATS: Automatic Test Systems Subdomain . . . 121
CS.ATS.1 Subdomain Description . . . 121
CS.ATS.2 Purpose . . . 121
CS.ATS.3 Applicability . . . 121
CS.ATS.4 Background . . . 122
CS.ATS.5 Core-Related Information Technology Categories . . . 123
CS.ATS.5.1 Data Interchange Services . . . 123
CS.ATS.5.1.1 Instrument Driver API Standards . . . 123
CS.ATS.5.1.1(a) Mandated. . . . 124
CS.ATS.5.1.2 Digital Test Data Formats . . . 124
CS.ATS.5.1.2(a) Mandated. . . . 124
CS.ATS.5.1.3 Resource Adapter Interface . . . 124
CS.ATS.5.1.3(a) Mandated. . . . 124
CS.ATS.5.1.3(b) Emerging. . . . 124
CS.ATS.5.1.4 Diagnostic Processing Standards . . . 125
CS.ATS.5.1.4(a) Mandated. . . . 125
CS.ATS.5.1.4(b) Emerging. . . . 125
CS.ATS.5.1.5 Test Requirements Data Standards . . . 125
CS.ATS.5.1.5(a) Mandated. . . . 125
CS.ATS.5.1.5(b) Emerging. . . . 125

CS.ATS.6 Information Transfer Standards . . . 125
CS.ATS.6.1 Instrument Communication Manager Standards . . . 125
CS.ATS.6.1(a) Mandated. . . . 126
CS.ATS.6.1(b) Emerging. . . . 126
CS.ATS.6.2 Maintenance Test Data and Services . . . 126
CS.ATS.6.2(a) Mandated. . . . 126
CS.ATS.6.2(b) Emerging. . . . 126
CS.ATS.6.3 Product Design Data . . . 126
CS.ATS.6.3(a) Mandated. . . . 126
CS.ATS.6.3(b) Emerging. . . . 127
CS.ATS.6.4 Built-In Test Data . . . 127
CS.ATS.6.4(a) Mandated. . . . 127
CS.ATS.6.4(b) Emerging. . . . 127
CS.ATS.7 Subdomain-Specific Service Areas . . . 127
CS.ATS.7.1 Platform/Environment Services . . . 127
CS.ATS.7.1.1 System Framework Standards . . . 127
CS.ATS.7.1.1(a) Mandated. . . . 128
CS.ATS.7.1.1(b) Emerging. . . . 128
CS.ATS.7.1.2 Receiver/Fixture Interface . . . 128
CS.ATS.7.1.2(a) Mandated. . . . 128
CS.ATS.7.1.2(b) Emerging. . . . 128
CS.ATS.7.1.3 Switching Matrix Interface . . . 128
CS.ATS.7.1.3(a) Mandated. . . . 128
CS.ATS.7.1.3(b) Emerging. . . . 128
CS.ATS.7.1.4 Other Interfaces . . . 128
CS.ATS.7.1.4.1 Computer Asset Controller Interface . . . 129
CS.ATS.7.1.4.2 Host Computer Interface . . . 129
CS.ATS.7.1.4.3 Instrument Control Bus Interface . . . 129
CS.ATS.7.1.4.4 Instrument Command Language . . . 129
CS.ATS.7.2 Application Development Environments . . . 129

CS.DTS: Defense Transportation System Subdomain . . . 131
CS.DTS.1 Subdomain Description . . . 131
CS.DTS.2 Purpose and Scope. . . . 131
CS.DTS.3 Applicability . . . 131
CS.DTS.4 Background . . . 131
CS.DTS.5 Core-Related Information Technology Categories . . . 131
CS.DTS.5.1 Product Data Interchange . . . 131
CS.DTS.5.1(a) Mandated. . . . 132
CS.DTS.5.2 Information Security Standards . . . 132
CS.DTS.5.2(a) Mandated. . . . 132
CS.DTS.5.2(b) Emerging. . . . 132

CS.HR: Human Resources Subdomain . . . 133
CS.HR.1 Subdomain Description . . . 133
CS.HR.2 Purpose and Scope. . . . 133
CS.HR.3 Applicability . . . 134
CS.HR.4 Background . . . 134
CS.HR.5 Core-Related Information Technology Categories . . . 134
CS.HR.5.1 Information Processing . . . 134
CS.HR.5.1.1 Document Interchange . . . 134
CS.HR.5.1.1(a) Mandated. . . . 134
CS.HR.5.1.1(b) Emerging. . . . 134

CS.MED: Medical Subdomain . . . 135
CS.MED.1 Subdomain Description . . . 135
CS.MED.2 Purpose and Scope . . . 135
CS.MED.3 Applicability . . . 135
CS.MED.4 Background . . . 135
CS.MED.5 Core-Related Information Technology Categories . . . 136
CS.MED.5.1 Medical Electronic Data Interchange . . . 136
CS.MED.5.1.1 Clinical Transactions . . . 136
CS.MED.5.1.1(a) Mandated . . . 136
CS.MED.5.1.2 Healthcare Administrative Transactions . . . 136
CS.MED.5.1.2(a) Mandated . . . 136
CS.MED.5.1.3 Retail Pharmacy Transactions . . . 137
CS.MED.5.1.3(a) Mandated . . . 137
CS.MED.5.2 Medical Still Imagery Data Interchange . . . 137
CS.MED.5.2(a) Mandated . . . 137
CS.MED.5.3 Medical Information Exchange Standards . . . 138
CS.MED.5.3(a) Mandated . . . 138
CS.MED.5.3(b) Emerging . . . 138
CS.MED.5.4 Information Security Standards . . . 138

M&S: Modeling and Simulation Domain . . . 139
M&S.1 Domain Description . . . 139
M&S.2 Purpose . . . 139
M&S.3 Scope and Applicability . . . 139
M&S.4 Background . . . 140
M&S.5 Core-Related Information Technology Categories . . . 140
M&S.5.1 Information Processing Standards . . . 141
M&S.5.1(a) Mandated . . . 141
M&S.5.1(b) Emerging . . . 141
M&S.5.2 Information Modeling, Metadata, and Information Exchange Standards . . . 142
M&S.5.2(a) Mandated . . . 142
M&S.5.2(b) Emerging . . . 142

WS: Weapon Systems Domain . . . 143
WS.1 Domain Description . . . 143
WS.2 Purpose and Scope . . . 143
WS.3 Background . . . 144
WS.3.1 Technical Reference Model . . . 144
WS.4 JTA Core-Related Information Technology Categories . . . 145
WS.4.1 Information Modeling, Metadata, and Information Exchange Standards . . . 145
WS.4.1(a) Mandated . . . 145
WS.4.1(b) Emerging . . . 145
WS.4.2 Human-Computer Interface Standards . . . 146
WS.4.2(a) Mandated . . . 146
WS.4.2(b) Emerging . . . 146
WS.4.3 Symbology . . . 146
WS.4.3(a) Mandated . . . 146
WS.5 Domain-Specific Services and Interfaces . . . 146
WS.5.1 Systems Services Layer Interfaces . . . 147
WS.5.1.1 Operating Environment Interface . . . 147
WS.5.1.1(a) Mandated . . . 147
WS.5.1.1(b) Emerging . . . 147
WS.5.2 Physical Resources Layer Interfaces . . . 147
WS.5.2.1 Parallel Buses . . . 147
WS.5.2.1.1 Single Board Computers (SBCs) Expansion Buses . . . 147
WS.5.2.1.1(a) Mandated . . . 147
WS.5.2.1.1(b) Emerging . . . 148

WS.AV: Aviation Subdomain . . . 149
WS.AV.1 Aviation Subdomain Overview . . . 149
WS.AV.1.1 Purpose . . . 149
WS.AV.1.2 Background . . . 149
WS.AV.1.3 Scope and Applicability . . . 149
WS.AV.1.4 Subdomain Organization . . . 149
WS.AV.1.5 Preferred Standards Selection Process . . . 149
WS.AV.1.5.1 Best Fit Ground Rules . . . 150
WS.AV.1.5.1.1 Forward Looking . . . 150
WS.AV.1.5.1.2 Open . . . 150
WS.AV.1.5.1.2.1 Widely Used . . . 151
WS.AV.1.5.1.2.2 International . . . 151
WS.AV.1.5.1.2.3 Consensus Based . . . 151
WS.AV.1.5.1.2.4 Public Domain . . . 151
WS.AV.1.5.1.2.5 Well Defined (Verifiable) . . . 151
WS.AV.2 Aviation Subdomain Preferred Interoperability Standards . . . 151
WS.AV.2.1 Communications . . . 151
WS.AV.2.1.1 Military Satellite Communications . . . 151
WS.AV.2.1.2 Radio Communications . . . 152
WS.AV.2.1.2.1 High Frequency . . . 152
WS.AV.2.1.2.2 Very High Frequency . . . 152
WS.AV.2.1.2.3 Ultra High Frequency . . . 153
WS.AV.2.1.2.4 Combat Net Radio . . . 153
WS.AV.2.1.2.5 Global Air Traffic Management – Communications . . . 153
WS.AV.2.1.2.5.1 Traffic Information . . . 154
WS.AV.2.1.2.5.2 Area Navigation . . . 154
WS.AV.2.2 Data Links . . . 154
WS.AV.2.2.1 Link 4A . . . 154
WS.AV.2.2.2 Link 11 . . . 155
WS.AV.2.2.3 Link 16 . . . 155
WS.AV.2.3 Navigation/Landing Aids . . . 155
WS.AV.2.3.1 Global Positioning . . . 155
WS.AV.2.3.1.1 Global Air Traffic Management – Navigation . . . 155
WS.AV.2.3.2 Tactical Area Navigation . . . 156
WS.AV.2.3.3 Airborne Radio Marker . . . 156
WS.AV.2.3.4 Landing Aids . . . 156
WS.AV.2.3.4.1 Instrument Landing Aids . . . 156
WS.AV.2.3.4.2 Microwave Landing Aids . . . 156
WS.AV.2.3.4.3 GPS Landing Aids . . . 157
WS.AV.2.3.4.4 Multimode Landing Aids . . . 157
WS.AV.2.4 Identification Aids . . . 157
WS.AV.2.4.1 Identification Friend or Foe . . . 157
WS.AV.2.4.2 Traffic Alert and Collision Avoidance . . . 158
WS.AV.2.4.3 Automatic Dependent Surveillance - Broadcast . . . 158
WS.AV.3 Aviation Subdomain “Other JTA” Standards . . . 158
WS.AV.4 Aviation Subdomain Terms, Definitions and Acronyms . . . 158
WS.AV.4.1 Performance-Based Business Environment (PBBE) . . . 158
WS.AV.4.2 Verifiable . . . 158

WS.GV: Ground Vehicle Subdomain . . . 161
WS.GV.1 Subdomain Description . . . 161
WS.GV.2 Purpose and Scope . . . 161
WS.GV.3 Background . . . 161
WS.GV.4 Subdomain-Specific Services and Interfaces . . . 161
WS.GV.4.1 Application Software Layer Interfaces . . . 161
WS.GV.4.1(a) Mandated . . . 161
WS.GV.4.1(b) Emerging . . . 161
WS.GV.4.2 System Services Layer Interfaces . . . 161
WS.GV.4.2.1 Operating Environment Interface . . . 162

WS.GV.4.2.1(a) Mandated. . . . 162
WS.GV.4.3 Physical Resources Layer Interfaces. . . . 162
WS.GV.4.3.1 Serial Buses . . . 162
WS.GV.4.3.1(a) Mandated. . . . 162
WS.GV.4.3.1(b) Emerging. . . . 162
WS.GV.4.3.2 Parallel Buses. . . . 163
WS.GV.4.3.2.1 Backplane Buses. . . . 163
WS.GV.4.3.2.1(a) Mandated. . . . 163
WS.GV.4.3.2.2 I/O Buses. . . . 164
WS.GV.4.3.2.2(a) Mandated. . . . 164
WS.GV.4.3.2.3 Single Board Computers (SBCs) Expansion Buses . . . 164
WS.GV.4.3.2.3(a) Mandated. . . . 164

WS.MD: Missile Defense Subdomain . . . 165
WS.MD.1 Subdomain Description . . . 165
WS.MD.2 Purpose and Scope . . . 165
WS.MD.3 JTA Core-Related Information Technology Categories . . . 165
WS.MD.3.1 Navigation . . . 165
WS.MD.3.1(a) Mandated. . . . 165
WS.MD.3.2 Time Synchronization . . . 166
WS.MD.3.2(a) Mandated. . . . 166
WS.MD.3.3 Information Transfer Standards. . . . 166
WS.MD.3.3(a) Mandated. . . . 166
WS.MD.3.3(b) Emerging. . . . 166
WS.MD.3.4 Bit-Oriented Formatted Messages . . . 166
WS.MD.3.4(a) Mandated. . . . 166
WS.MD.3.5 Missile Defense Data Element Descriptions . . . 166
WS.MD.3.5(a) Mandated. . . . 167
WS.MD.3.5(b) Emerging. . . . 167

WS.MS: Missile Systems Subdomain . . . 169
WS.MS.1 Subdomain Description. . . . 169
WS.MS.2 Purpose and Scope . . . 169
WS.MS.3 Background. . . . 169
WS.MS.4 JTA Core-Related Information Technology Categories. . . . 169
WS.MS.4.1 Information Processing Standards. . . . 169
WS.MS.4.1.1 Geospatial Data Interchange . . . 170
WS.MS.4.1.1(a) Mandated. . . . 170
WS.MS.4.1.1(b) Emerging. . . . 170
WS.MS.4.2 Information Transfer Standards . . . 170
WS.MS.4.2(a) Mandated. . . . 170
WS.MS.4.2(b) Emerging. . . . 170
WS.MS.5 Subdomain-Specific Services and Interfaces . . . 170
WS.MS.5.1 Physical Resources Layer Interfaces . . . 170
WS.MS.5.1.1 Serial Buses. . . . 171
WS.MS.5.1.1(a) Mandated. . . . 171
WS.MS.5.1.1(b) Emerging. . . . 171
WS.MS.5.1.2 Parallel Buses . . . 171
WS.MS.5.1.2.1 Backplane Buses . . . 171
WS.MS.5.1.2.1(a) Mandated. . . . 171
WS.MS.5.1.2.1(b) Emerging. . . . 171
WS.MS.5.1.2.2 I/O Buses . . . 171
WS.MS.5.1.2.2(a) Mandated. . . . 171
WS.MS.5.1.2.2(b) Emerging. . . . 172
WS.MS.5.1.2.3 Single Board Computers (SBCs) Expansion Buses . . . 172
WS.MS.5.1.2.3(a) Mandated. . . . 172
WS.MS.5.1.2.3(b) Emerging. . . . 172

WS.MUS: Munition Systems Subdomain 173
WS.MUS.1 Subdomain Description 173
WS.MUS.2 Purpose and Scope 173
WS.MUS.3 Background 173
WS.MUS.4 Subdomain-Specific Services and Interfaces 173
WS.MUS.4.1 Application Software Layer Interfaces 174
WS.MUS.4.1(a) Mandated. 174
WS.MUS.4.1(b) Emerging. 174
WS.MUS.4.2 Physical Resources Layer Interfaces 174
WS.MUS.4.2.1 Parallel Buses 174
WS.MUS.4.2.1.1 I/O Buses 174
WS.MUS.4.2.1.1(a) Mandated. 174
WS.MUS.4.2.1.2 Single Board Computers (SBCs) Expansion Buses 175
WS.MUS.4.2.1.2(a) Mandated. 175

WS.SS: Soldier Systems Subdomain 177
WS.SS.1 Subdomain Description. 177
WS.SS.2 Purpose and Scope 177
WS.SS.3 Background. 177
WS.SS.4 Subdomain-Specific Services and Interfaces 177
WS.SS.4.1 Application Software Layer Interfaces 178
WS.SS.4.1(a) Mandated.. 178
WS.SS.4.1(b) Emerging. 178
WS.SS.4.2 Physical Resources Layer Interfaces 178
WS.SS.4.2.1 Serial Buses 178
WS.SS.4.2.1(a) Mandated. 178
WS.SS.4.2.1(b) Emerging. 178

Appendix A: Abbreviations and Acronyms 181

Appendix B: Document Sources 199

Appendix C: References 209

Appendix D: Glossary. 211

Page intentionally left blank.

List of Figures

Figure 1-1: Architecture Views Relationships 4

Figure 1-2: JTA Hierarchy Model 7

Figure 1-3: DoD Technical Reference Model (TRM) 10

Figure 5-1: HCI Development Guidance 81

Figure CS.ATS-1: Generic ATS Architecture. 121

Figure WS.AV-1: JTA Aviation Subdomain Preferred Standards Selection Process 150

Page intentionally left blank.

List of Tables

Table 1-1: Interface Translation Table 10

Table 1-2: JTA Development Group (JTADG) Voting Membership 13

Table 2-1: Common Document Interchange Formats 22

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.

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.

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.
- Effective means to protect the information.

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

1.2 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.

1.3 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/Combatant Command Area of Responsibility (AOR).
- Across Combatant Command 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 achievement 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.

1.4 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

(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. 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 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.

1.5 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 1-1 shows the relationship among the three views. The definitions are provided here to ensure a common understanding of the three views.[1]

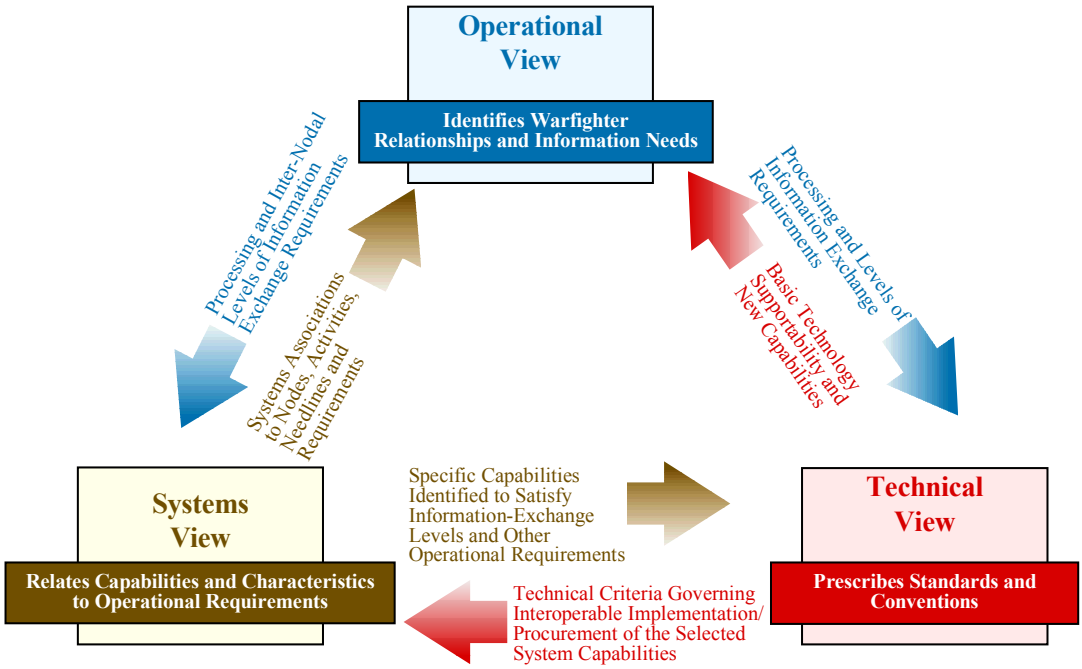


Figure 1-1: Architecture Views Relationships

1.5.1 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 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.

1.5.2 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,

[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.

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.

1.5.3 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.

1.6 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.

1.7 Document Organization

The JTA is organized into a main body, followed by domains, subdomains, and a set of appendices.

1.7.1 General Organization

The main body identifies the “Core” set of JTA elements consisting of service areas, interfaces, and standards. 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. 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.

1.7.2 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.

- **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.

1.7.3 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 1-2.

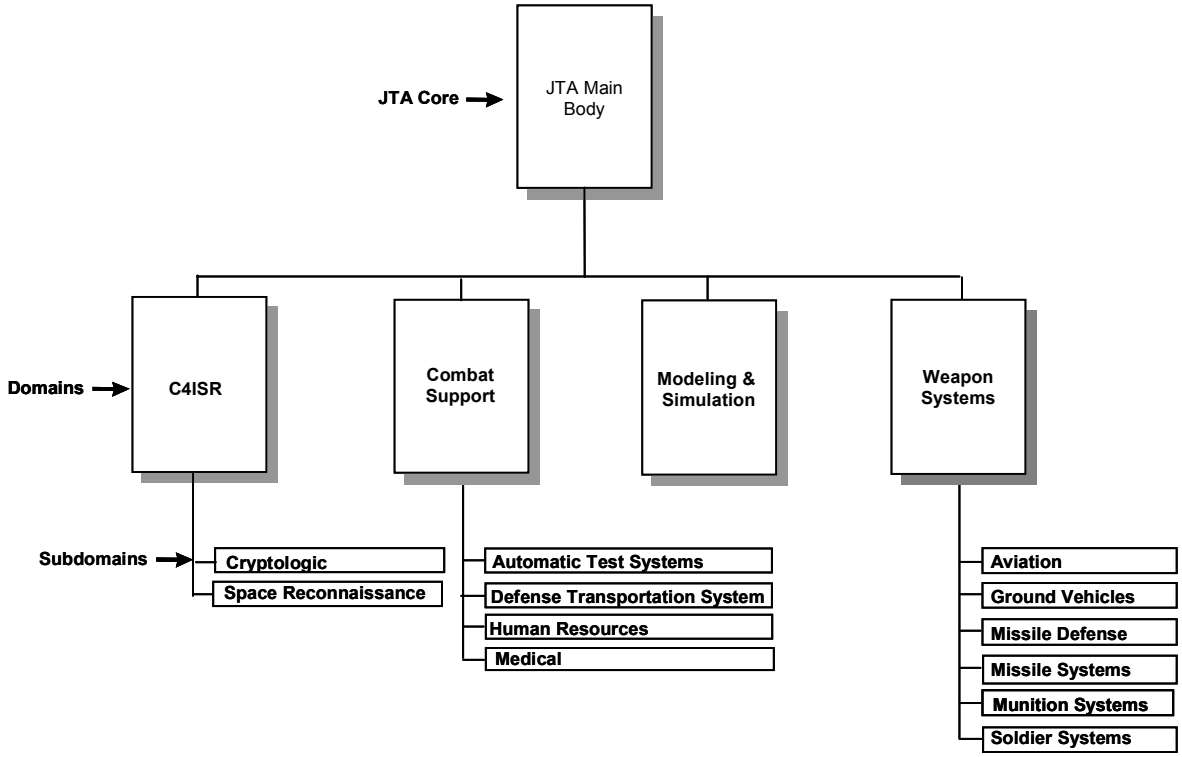


Figure 1-2: JTA Hierarchy Model

The current domains and subdomains are listed as follows:

- Domains
  - Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR)
  - Combat Support (CS)
  - Modeling and Simulation (M&S)
  - Weapon Systems (WS)
- Subdomains
  - Automatic Test Systems (ATS)

- Aviation (AV)
- Cryptologic (CRY)
- Defense Transportation System (DTS)
- Ground Vehicles (GV)
- Human Resources (HR)
- Medical (MED)
- Missile Defense (MD)
- Missile Systems (MS)
- Munition Systems (MUS)
- 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.

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 (TRM) defined in 1.8, but may also use a different, tailored, or expanded model.

1.7.4 Appendices (Appendix A, B, C, D)

The appendices provide supporting information and links to standards organizations' Web sites.

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

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

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

The DoD Joint Technical Architecture List of Mandated and Emerging Standards (LMES), now a stand-alone document on the JTA Web site, contains "currently mandated," "currently preferred," and "emerging" standards for each JTA service area.

1.8 DoD Technical Reference Model

The DoD Technical Reference Model (TRM), Version 2.0, 9 April 2001, 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 1-3, the model is partitioned into the following: an Application Software entity that includes both User Applications 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; 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	Security Services
User Interface Services	System Management Services
Data Management Services	Distributed Computing Services
Data Interchange Services	Internationalization Services
Graphics Services	Operating System Services
Platform Communications Services	Physical Environment 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, Data Management, Data Interchange, Graphics, Operating System, Internationalization, System Management, Distributed Computing and Environment Management service areas. This section also references, but does not specify, any standards for the Software Engineering, Communications (e.g., Platform, Applications, External Environment), and Security service areas.

Section 3 Information Transfer Standards specifies standards for the Communications and Network and System Management 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.

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

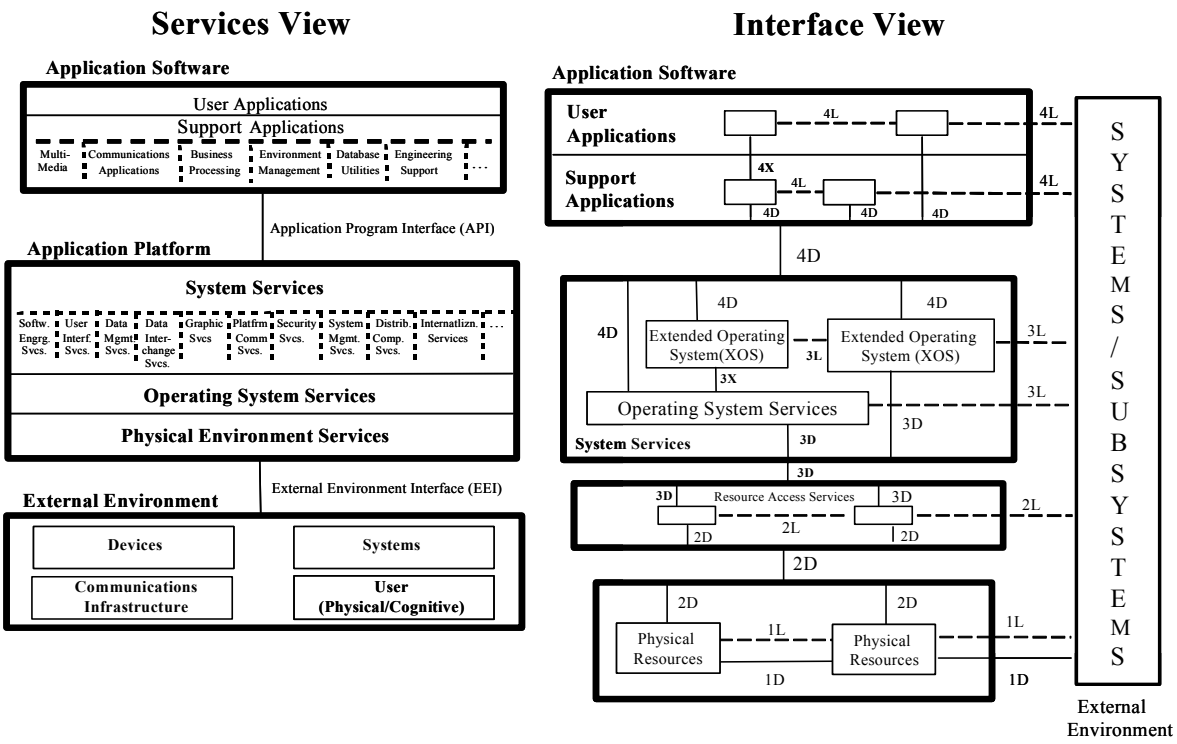


Figure 1-3: DoD Technical Reference Model (TRM)

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

Table 1-1 provides the interface relationships for Figure 1-3.

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)

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

1.9 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 JTA service/interface. 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/interface 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 the minimal set 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.

1.10 JTA Relationship to the Defense Standardization Program (DSP)

The DSP provides the policy framework and technical infrastructure for developing DoD specifications and standards and for participating in the development and adoption of commercial non-government standards and standards promulgated by other federal agencies and multinational treaty organizations. These standards provide a foundation for the JTA, which serves as a tool for the selection and application of standards developed or adopted under the DSP that are essential for achieving joint information interoperability. While the JTA provides technical direction in the selection of standards, such selection is based on standards application policies prescribed by DoD 4120.24-M, "Defense Standardization Program (DSP) Policies and Procedures." Consistent with these policies, the JTA mandates the minimum standards necessary to achieve joint interoperability and implements 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 since all mandatory standards in the JTA are of the types that have been identified by DoD standards reform as waiver-free or for which an exemption has already been obtained.

1.11 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.

1.12 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.

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) Interoperability Directorate (IN) JTA Web site at http://jta.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 change requests for submission as official DoD Component-sponsored change requests.

Where a standard is highlighted and underscored, it is hyperlinked to a Web site with information about the standard.

To submit a change request, register as a user at http://jtaonline.disa.mil.

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

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
Missile Defense Agency (MDA)
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)

Page intentionally left blank.

Section 2: Information Processing Standards

2.1 Introduction

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

2.2 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.

2.3 Scope (Applicability)

This section applies to user applications, support applications, 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).

2.4 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.

2.5 Information Processing Services

The information processing standards in this section apply to support applications, system services and operating system services that are contained in the Application Software and Application Platform Entities of the DoD TRM (see 1.8).

2.5.1 Software Engineering Services

The software engineering services provide system developers with the tools that are appropriate to the development and maintenance of applications. Language services provide the basic syntax and semantic definition for developers to encode the desired software functions. DoD programs should design and develop software based on the application of systems and software engineering best practices. Programming language selections should be made in the context of the system and software engineering factors to minimize overall life-cycle costs and risks and to maximize potential interoperability. 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.

2.5.1.1 Common Operating Environment

The Common Operating Environment (COE) concept and levels of compliance are described in the Integration and Runtime Specification (I&RTS). The 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 Application Program Interfaces (APIs). The COE may be adapted and tailored to meet the specific requirements of a domain. COE implementations provide standard, modular software services consistent with service areas identified in

the TRM. Application programmers then have access to these software services through standardized APIs.

2.5.1.1(a) Mandated. For systems having a requirement to implement the COE, the following standard is mandated:

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

2.5.2 User Interface Services

User Interface Services implement the Human-Computer Interface (HCI) style and control how users interact with the system by providing consistent access to application programs, operating system functions and system utilities.

2.5.2.1 User Interface Service — POSIX

For POSIX-based systems, the Common Desktop Environment (CDE)/Motif provides a common set of desktop applications and management capabilities. CDE/Motif uses the underlying X-Windows system.

2.5.2.1(a) Mandated. The following standards are mandated for use with POSIX-based systems:

- C903, X Window System (X11R6): Protocol, The Open Group, July 1999.
- C904, X Window System (X11R6): C-Language Library (Xlib), Open Group Technical Standard, December 1999.
- C905, X Window System (X11R6): Toolkit, Open Group Technical Standard, December 1999.
- C510, Window Management (X11R5): File Formats and Application Conventions, Open Group Technical Standard, ISBN 1-85912-090-3, May 1995.

2.5.2.2 User Interface Service — Win32

For Microsoft Windows-based systems, the Win32 API set provides user interface services. Documentation for the Win32 APIs is found within the Microsoft Platform Software Development Kit (SDK).

2.5.2.2(a) Mandated. The following standard is mandated for use with Microsoft Windows-based systems:

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

2.5.3 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.

2.5.3(a) Mandated. 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.

Referred to as SQL Object Language Bindings (SQL/OLB), this standard defines extensions to the syntax and semantics for SQL to support embedding of SQL statements into programs written in Java. It specifies the syntax and semantics of that embedding, as well as mechanisms to ensure binary portability of resulting SQL-J applications. The following standard is mandated:

- ANSI X3.135.10-1998: Information technology – Database languages – SQL – Part 10: Object Language Bindings (SQL/OLB).

2.5.3(b) Emerging. 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 9075-5:1999, 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 following standard is emerging:

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

2.5.4 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, time-of-day data, and multimedia data.

2.5.4.1 Document Interchange

The document interchange service specifies the supported data structures to be used for storage of electronic information and its transmission between information systems. Document formats are not restricted to physical byte layout for a file but also include the languages used to instruct information systems on how to display the document information.

2.5.4.1(a) Mandated. 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, 24 December 1999.

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.

The XML Schema Part 0: Primer provides an easily approachable description of the XML Schema definition language, and should be used alongside the formal descriptions of the language contained in Parts 1 and 2 of the XML Schema specification. The intended audience of this document includes application developers whose programs read and write schema documents, and schema authors who need to know about the features of the language, especially features that provide functionality above and beyond what is provided by DTDs. The text assumes that you have a basic understanding of XML 1.0 and XML namespaces. This document can be found at http://www.w3.org/TR/xmlschema-0/.

XML Schema Part 1: Structures specifies the XML Schema definition language, which offers facilities for describing the structure and constraining the contents of XML 1.0 documents, including those which exploit the XML Namespace facility. The schema language, which is itself represented in XML 1.0 and uses namespaces, substantially reconstructs and considerably extends the capabilities found in XML 1.0 document type definitions (DTDs). This specification depends on XML Schema Part 2: Datatypes. For defining XML schemas, when DTDs are not used, the following standard is mandated:

- XML Schema Part 1: Structures, W3C Recommendation, 2 May 2001.

The XML Schema Part 2: Datatypes specifies facilities for defining datatypes to be used in XML schemas as well as other XML specifications. The following standard is mandated:

- XML Schema Part 2: Datatypes, W3C Recommendation, 2 May 2001.

The XML namespaces standard provides a simple method for qualifying element and attribute names used in Extensible Markup Language documents by associating them with namespaces identified by URL references. The following standard is mandated:

- Namespaces in XML, W3C Recommendation, 14 January 1999.

2.5.4.1(b) Emerging. XHTML (Extensible HyperText Markup Language) is the next-generation follow-on to HTML. XHTML reformulates HTML as an XML 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, Second Edition, A Reformulation of HTML 4 in XML 1.0, W3C Recommendation, 26 January 2000, revised 1 August 2002.

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, W3C Working Draft, 12 November 2002.

– XForms Requirements, W3C Working Draft, 4 April 2001.

Resource Description Framework (RDF) describes a foundation for processing web-based metadata; it supports interoperability between different applications that may need to exchange machine-understandable information on the World Wide Web. RDF uses 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 1.0, W3C Candidate Recommendation, 27 March 2000, CR-rdf-schema-20000327.

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 Recommendation, 15 October 2001.

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 Working Draft, 24 August 2001.

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 Recommendation, 16 November 1999.

For applying an XML-encoded digital signature within an XML document, rather than as separate data, the following standard is emerging:

– XML-Signature Syntax and Processing, W3C Recommendation, 12 February 2002.

Xquery provides flexible query facilities to extract data from collections of XML documents as well as non-XML data viewed as XML via a mapping mechanism. The following standard is emerging:

– XQuery 1.0, An XML Query Language, W3C Working Draft, 15 November 2002.

Web Services Description Language defines the XML grammar needed for network services for distributed systems and provides the methods for automating the details involved in applications communication. The following standard is emerging:

– Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001.

Simple Object Access Protocol (SOAP) is a lightweight XML protocol used for exchanging information in a decentralized, distributed environment. It provides a simple method of enveloping and transferring an XML document using HTTP transfer protocol, and addressing the recipient using Uniform Resource Identifiers (URI). The following standard is emerging:

– Simple Object Access Protocol (SOAP) 1.1, W3C Note, 08 May 2000.

For publishing and discovery of web services, the following standard is emerging. Note that there are significant security issues that need to be considered before using this standard:

– UDDI Version 3.0 Published Specification, 19 July 2002.

Cascading Style Sheets (CSS) provides a simple approach for formatting documents. CSS lacks XSL/XSLT's ability to reorder information, but CSS can incrementally format documents and can handle HTML. For simple formatting of HTML and XML documents (where XSL's capabilities are not needed), the following is emerging:

– Cascading Style Sheets (CSS) Level 1 (CSS1), W3C Recommendation, 17 December 1996.

There are different approaches for accessing XML data, e.g., the Simple API for XML (SAX) approach is used for sequential access and the Java Document Object Model (JDOM) approach is used for a Java-specific binding of Document Object Model (DOM). For read/write random access to XML documents, the following standard is emerging:

– Document Object Model (DOM) Level 1 Specification, Version 1.0, W3C Recommendation, 1 October 1998.

2.5.4.2 Common Document Interchange Formats

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 HTML 4.01 Format MS Word® 7.0 Format Rich Text Format WordPerfect® 5.2 Format	.pdf .htm .doc .rtf .wp5	Vendor W3C Vendor Vendor Vendor
Briefing – Graphic Presentation	MS PowerPoint® 4.0 Format	.ppt	Vendor
Spreadsheet	MS Excel® 5.0 Format	.xls	Vendor
Database	dBASE IV® Format	.dbf	Vendor
Compression	GZIP® File Format WinZip File Format	.gz .zip	RFC 1952 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. 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.

2.5.4.2(a) Mandated. An organization is in compliance with the mandate to implement "backoff support" of a standard (1) when the organization can display and print all of the mandated formats and (2) when all of its applications of the appropriate document type can generate at least one of the formats of the appropriate document type. Note that special fonts, formatting, or features may not convert accurately.

Organizations that exchange plain text are mandated to implement backoff support for the following format standard:

- ISO/IEC 646:1991, Information technology – ISO 7-bit coded character set for information interchange.

Organizations that exchange data interchange of compound documents are mandated to implement backoff support for the following format standards:

- Adobe® PDF 1.3 2nd Edition Format.
- HTML 4.01 Specification, W3C Recommendation, 24 December 1999.
- Microsoft Word 7.0 Format.
- Rich Text Format (RTF) Specification, Version 1.6.
- Corel WordPerfect® 5.2 Format.

Organizations that exchange briefings and graphic presentations are mandated to implement backoff support for the following format standard:

- Microsoft PowerPoint® 4.0.

Organizations that exchange spreadsheets are mandated to implement backoff support for the following format standard:

- Microsoft Excel® 5.0 format.

Organizations that exchange databases data are mandated to implement backoff support for the following format standard:

- Ashton Tate dBase IV® format.

Organizations that exchange for file compression are mandated to implement backoff support for the following format standards:

- IETF RFC 1952, GZIP file format specification, Version 4.3, May 1996.
- WinZip file format.

Organizations that exchange computer automated design documents are mandated to implement backoff support for the following format standard:

- Autodesk AutoCAD® 14 format.

2.5.4.3 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 truecolor images are supported, plus an optional alpha channel for transparency.

2.5.4.3(a) Mandated. For the interchange of very large still-raster images that have no geospatial context and where lossy compression is acceptable, the following standard is mandated:

- 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 following standard is mandated:

- IETF RFC 2083, Portable Network Graphics (PNG) Specification, Version 1.0, March 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 following standard is mandated:

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

2.5.4.3(b) Emerging. 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 (VRML) – Part 1: Functional specification and UTF-8 encoding.

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

– Multiple-image Network Graphics (MNG) Format, Version 1.0, 31 January 2001.

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).

2.5.4.4 Environmental Data Interchange

Most environmental data is available from producers in specific product formats. As information systems become more capable, the need to integrate products and fuse data from multiple sources is increasing. A product-independent data interchange format allows product-specific formats to be decomposed into foundation data for potential integration, update, and fusion, potentially to be recomposed into the original product format.

2.5.4.4(a) Mandated. There are no mandated standards in this section.

2.5.4.4(b) Emerging. Synthetic Environment Data Representation and Interchange Specification (SEDRIS) facilitates interoperability among heterogeneous information technology applications by providing complete and unambiguous interchange of environment data. SEDRIS provides a standard interface for Geographic Information System (GIS) systems, which are key components in the generation of complex integrated environmental databases. 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. ISO/IEC 18023 provides a

standard methodology and format for representing environmental information and for its transmittal and exchange between information systems. ISO/IEC 18025 provides a standard coding system for environmental information used in multiple systems, including those used by environmental data collectors and producers. ISO/IEC 18026 provides a set of spatial reference models, both earth-centric and non-earth-centric (for application to celestial bodies other than the planet earth), and related coordinate transformation algorithms for use in standardizing the coordinate systems used for collecting and displaying environmental information within the requirements of MIL-STD-2401 and other international geospatial coordinate standards. For product independent environmental data interchange, the following standards are emerging:

- ISO/IEC 18023, Information technology – Computer graphics and image processing – Synthetic Environment Data Representation and Interchange Specification (SEDRIS), 5 December 2001.
- ISO/IEC 18025: Information technology – Computer graphics and image processing – Environmental Data Coding Specification (EDCS), 26 December 2002.
- ISO/IEC 18026: Information technology – Computer graphics and image processing – Spatial Reference Model (SRM), 14 January 2002.

2.5.4.4.1 Geospatial Data Interchange

Geospatial services are also referred to as mapping, charting, and geodesy (MC&G) services.

2.5.4.4.1(a) Mandated. 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, and Notice of Change, Notice 2, 16 August 2001.

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 (WVSPLUS). For vector-based products, the following standard is mandated:

- MIL-STD-2407, Interface Standard for Vector Product Format (VPF), 28 June 1996, with Notice of Change, Notice 1, 26 October 1999.

World Geodetic System (WGS 84), a Conventional Terrestrial Reference System (CTRS), is mandated for representation of a reference frame, reference ellipsoid, fundamental constants, and an Earth Gravitational Model with related geoid. Included in the Reference System are parameters for transferring to/from other geodetic datums. The National Imagery and Mapping Agency (NIMA) Technical Report (TR) 8350.2, DoD World Geodetic 1984, Its Definition and Relationships with Local Geodetic Systems, Third Edition, 4 July 1997, with Amendment 1, 3 January 2000, 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 Standard Practice, World Geodetic System (WGS), 11 January 1994, as implemented by NIMA TR 8350.2, Department of Defense World Geodetic System 1984: Its Definitions and Relationships with Local Geodetic Systems, Third Edition, 4 July 1997, as modified by Amendment 1, 3 January 2000.

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 as modified by Change Notice No. 1, 1 December 1998; Change Notice 2, 1 March 1999; Change Notice No. 3, 1 May 1999; Change Notice No. 4, 25 February 2000; Change Notice No. 5, 10 August 2000; Change Notice No. 6, 28 January 2001, and Change Notice No. 7, 10 January 2002.

2.5.4.4.2 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.

2.5.4.4.2(a) Mandated. 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.

2.5.4.4.2(b) Emerging. Hierarchical Data Format (HDF) was developed by the National Center for Supercomputing Applications (NCSA) to facilitate interchange of scientific data. It is used in many fields including environmental science, oceanography, and atmospheric modeling. It emphasizes

storage and I/O efficiency for use in the storage, archiving and transmission of large datasets like images, multidimensional arrays, structures and tables. HDF organizes data as a digraph, with Groups and Datasets as primary objects. Secondary and tertiary objects can be created for subsetting and assigning parameters to data, and each object may have more than one path to it. HDF provides a set of APIs which can be used to access the data or subsets without knowledge of the actual format.

For large or complex data sets that are interchanged between environmental data processing systems, the following standard is emerging:

– Hierarchical Data Format (HDF), Version 5, Release 1.4.2, National Center for Super Computing Applications, 4 October 2001.

2.5.4.5 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, NITFS 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, National Imagery Transmission Format Standard (NITFS), 12 October 1994.

The NITFS allows for Support Data Extensions (SDEs), which are a collection of data fields that provide space within the NITFS 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. These SDEs are described in the Compendium of Controlled Extensions (CE).

2.5.4.5(a) Mandated. 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, and Notice 2, 1 March 2001.
- 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 8632-1:1999, Information technology – Computer graphics – Metafile for the storage and transmission of picture description information – Part 1: Functional specification, as profiled by MIL-STD-2301A, Computer Graphics Metafile (CGM) Implementation Standard for the National Imagery Transmission Format Standard, 5 June 1998 with Notice 1, 1 March 2001.
- ISO/IEC 8632-3:1999, Information technology – Computer graphics – Metafile for the storage and transmission of picture description information – Part 3: Binary encoding, as profiled by MIL-STD-2301A, Computer Graphics Metafile (CGM) Implementation Standard for the National Imagery Transmission Format Standard, 5 June 1998 with Notice 1, 1 March 2001.

- ISO/IEC 8632-4:1999, Information technology – Computer graphics – Metafile for the storage and transmission of picture description information – Part 4: Clear text encoding, as profiled by MIL-STD-2301A, Computer Graphics Metafile (CGM) Implementation Standard for the National Imagery Transmission Format Standard, 5 June 1998 with Notice 1, 1 March 2001.
- ISO/IEC 15444-1:2001, Information technology – JPEG 2000 image coding system – Part 1: Core coding system, 20 December 2001, with Amendments 1 and 2, 29 January 2002. (Note that this standard is not compatible with ISO/IEC 10918-1:1994, JPEG.)
- The Compendium of Controlled Extensions (CE) for the National Imagery Transmission Format (NITF), Version 2.1, 16 November 2000.

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 3.4.4.

2.5.4.5(b) Emerging. 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, Information technology – Computer graphics and image processing – Image Processing and Interchange (IPI) Functional specification – Part 5: Basic Image Interchange Format (BIIF), 1 December 1998, with Technical Corrigendum 1:2001.

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. Part I of JPEG 2000 contains mandatory features. Part II of JPEG 2000 is a Final Draft International Standard (FDIS) that contains optional features beyond those in Part I including advanced region-of-interest capability, expanded file format, multispectral compression, low complexity implementation, and trellis quantized compression. Only those features that are needed for specific applications need be implemented. The following standard is emerging:

– ISO/IEC 15444-2:2001, JPEG 2000 image coding system, July 2001.

2.5.4.6 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.

For the purposes of the JTA, Motion Imagery Data Interchange Standards are divided into four categories:

- Motion Imagery Systems, which create, transmit, edit, store, archive, or disseminate digital motion imagery 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 motion imagery, the standards in the Motion Imagery section apply.
- Video Telemedicine Systems, which provide real-time visual interchange between remote locations in biomedical applications including fiber-optic and video teleconferencing. Though

there are no Video Telemedicine standards specifically mandated in this section of the JTA, when any Video Telemedicine System is used for the purpose of motion imagery data dissemination, the standards mandated in this section of the JTA apply.

- Video Support Services, which enable end-user applications associated with motion imagery (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 motion imagery systems are noted in the following sections:

2.5.4.6.1 Motion Imagery Systems

Department of Defense Directive Number 5105.60, 11 October 1996, established the National Imagery and Mapping Agency (NIMA). NIMA, through the National System for Geospatial Intelligence (NSGI), has the mission to "prescribe and mandate standards and end-to-end technical architectures related to imagery, imagery intelligence, and geospatial information for the DoD Components and for the non-DoD elements of the Intelligence Community" to include:

- Standards for end-to-end architectures related to imagery, imagery intelligence, and geospatial information.
- Technical guidance and direction to all the DoD Components and the non-DoD members of the Intelligence Community regarding standardization and interoperability of systems requiring geospatial information or imagery support and for exploitation and dissemination of imagery and imagery intelligence products and geospatial information.

2.5.4.6.1(a) Mandated. The Motion Imagery Standards Profile (MISP) is a collection of standards and practices on how component systems based on commercial standards can interconnect and provide interoperable service to DoD/IC/NSGI users. For the acquisition of systems that produce, use, or exchange motion imagery information, the following standards profile is mandated:

- Motion Imagery Standards Profile, Version 2.0, 29 November 2001.

2.5.4.6.2 Video Teleconference Systems

Video Teleconferencing (VTC) standards are specified in 3.4.2.

2.5.4.6.3 Video Support Services

Video support services specifies the structure and data formats for the production, exchange, transmission or use of digital video data.

2.5.4.6.3(a) Mandated. 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 1:1996, and Technical Corrigendum 2:1999.
- 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 13818-1:2000, Information technology – Generic coding of moving pictures and associated audio information – Part 1: Systems (MPEG-2).
- ISO/IEC 13818-2:2000, Information technology – Generic coding of moving pictures and associated audio information – Part 2: Video (MPEG-2).

2.5.4.7 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.

2.5.4.7(a) Mandated. 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 1:1996, and Technical Corrigendum 2:1999.
- ISO/IEC 11172-3:1993, Information technology – Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s – Part 3 (Audio Layer-3 only); with Technical Corrigendum 1:1996.

2.5.4.7.1 Audio Associated with Motion Imagery

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

- ☐ Audio for Motion 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. Video Teleconferencing (VTC) standards are specified in 3.4.2.

- 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.

2.5.4.7.1.1 Audio for Motion Imagery Systems

Audio for motion imagery systems specifies data formats for the exchange of the digital sound track associated with video in compressed and non-compressed formats.

2.5.4.7.1.1(a) Mandated. For audio systems associated with Video Imagery applications, the audio subsections of the Motion Imagery Standards Profile (MISP), Version 2.0, 29 November 2001, apply. The following standards are mandated:

- ANSI S4.40-1992/AES3:1992, AES (Audio Engineering Society) Recommended Practice for Digital Audio Engineering – Serial transmission format for two-channel linearly represented digital audio data, 1992 (reaffirmed and amended 1997).
- ISO/IEC 13818-3:1998, Information technology – Generic coding of moving pictures and associated audio information, Part 3: Audio:1998.

2.5.4.7.1.2 Audio for Video Support Systems

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.

2.5.4.7.1.2(a) Mandated. 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 – Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s – Part 3 (Audio Layer-3 only); with Technical Corrigendum 1:1996.

2.5.4.7.2 Voice Encoder

This section provides standards for audio for voice encoder.

2.5.4.7.2(a) Mandated. The 2.4 Kbps Mixed Excitation Linear Prediction (MELP) algorithm specified in MIL-STD-3005 is intended to provide seamless interoperability and enable end-to-end security across the domains of strategic and tactical satellite communications, including those using 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.

2.5.4.7.2(b) Emerging. 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).

2.5.4.8 Data Interchange Storage Media

This section provides standards for Data Interchange Storage Media.

2.5.4.8(a) Mandated. 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.

MIL-HDBK-9660B, 1 September 1997, provides additional guidance in the use of Compact Disc-Read Only Memory (CD-ROM) technology. Standards used for the exchange of multimedia data can be found in 3.4.2.

2.5.4.9 Time-of-Day Data Interchange

This section provides standards for time-of-day data interchange.

2.5.4.9(a) Mandated. Coordinated Universal Time (UTC), traceable to UTC U.S. Naval Observatory (USNO) maintained by the 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.

The Global Positioning System (GPS) provides two broadcast time products: (1) UTC USNO time-of-day information and (2) GPS System Time. Leap seconds are inserted or deleted when necessary in UTC USNO to keep the time-of-day system synchronized with the earth's rotation. GPS

System Time does not adjust for leap seconds and is optimized for short-term stability and uniform global distribution. See 3.4.5 for a GPS discussion, required standards, and guidelines.

2.5.4.10 Multimedia Data Interchange

This section provides standards for Multimedia Data Interchange.

2.5.4.10(a) Mandated. There are no mandated standards at this time.

2.5.4.10(b) Emerging. For on-demand or real-time video and audio streaming, the following standard is emerging:

– ISMA Specification 1.0:2001, Internet Streaming Media Alliance.

2.5.4.11 Calendaring and Scheduling

This section identifies standards for interoperability among calendaring and scheduling systems used by Surveillance and Reconnaissance (SR) IT and other DoD Intelligence systems.

2.5.4.11(a) Mandated. For date format standards, captured in FIPS 4-2, Representation of Calendar Date for Information Exchange 15 November 1998, the following standard is mandated:

- ANSI X3.30-1997: Representation of Date for Information Interchange.

2.5.4.11(b) Emerging. The following standard is emerging:

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

2.5.5 Graphics Services

These services support the creation and manipulation of graphics.

2.5.5(a) Mandated. 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 dialogues with graphics devices.
- OpenGL Graphics System: A Specification (Version 1.2.1), 1 April 1999.

2.5.5(b) Emerging. For three-dimensional graphics development, the following standard is emerging:

– OpenGL Graphics System: A Specification (Version 1.3), 14 Aug 2001.

2.5.6 Platform 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.

2.5.7 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), the Linux Standard Base, or the Win32 APIs.

When requiring real-time operating systems, ISO/IEC ISP 15287-2:2000, Information technology – Standardized Application Environment Profile – Part 2: POSIX Realtime Application Support (AEP) 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. These are Minimal Realtime System Profile (PSE51), Realtime Controller System Profile (PSE52), Dedicated Realtime System Profile (PSE53), and Multi-Purpose Realtime System Profile (PSE54).

2.5.7(a) Mandated. Not all operating system services are required to be implemented, but those that are used shall comply with the standards listed below. The operating system (OS) services mandates in this section currently do not apply to commercially-acquired handheld computing devices. When choosing an OS for hand-held computing devices, developers should consider the need to integrate these devices with existing desktop and server-based systems, and whether application code from these systems can be reused on the hand-held devices. These services shall be accessed by applications through either the standard POSIX, the Linux Standard Base, or the Win32 APIs.

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.
- IEEE 1003.2d:1994, IEEE Standard for Information Technology – Portable Operating System Interface (POSIX) – Part 2: Shell and Utilities – Amendment 1: Batch Environment.
- ISO/IEC 14519:1999, Information technology – POSIX Ada Language Interfaces – Binding for System Application Program Interface (API) – Realtime Extensions.

The Linux Standard Base (LSB) specification consists of a single common specification and architecture-specific specifications. The complete specification for a platform consists of the common specification plus one of the architecture specifications. The following standard is mandated for use in all systems running (or intended to run) Linux-based applications:

- Linux Standard Base Specification 1.2, Free Standards Group, 2002.

The following additional standards are mandated for use in systems running (or intended to run) Linux-based applications on the platforms specified:

- Linux Standard Base Specification for the IA32 Architecture 1.2, Free Standards Group, 2002.
- Linux Standard Base Specification for the PPC32 Architecture 1.2, Free Standards Group, 2002.

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.

2.5.7(b) Emerging. The following POSIX standards are emerging:

- ISO/IEC 15287-2:2000, Information technology – Standardized Application Environment Profile – Part 2: Posix Realtime Application Support (AEP).
- 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].
- 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].
- P1003.1q, 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.
- P1003.21, 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.

The Open Group (TOG), IEEE, and ISO consolidated the standards that make up ISO/IEC 9945-1:1996, ISO/IEC 9945-2:1993, IEEE STD 1003.1, IEEE STD 1003.2 and the appropriate parts of the Single UNIX Specification (SUS). These will be technically equivalent in all respects. The new set of specifications will form the core of the SUS, Version 3. The following standard is emerging:

- The Single UNIX Specification, Version 3 (SUS v3), The Open Group.

2.5.8 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.

2.5.8(a) Mandated. 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 more than 8-bit textual information respectively:

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

2.5.9 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).

2.5.10 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 3.8.

2.5.10(a) Mandated. There are no mandated standards for System Management Services.

2.5.10(b) Emerging. The Distributed Management Task Force (DMTF) Common Information Model (CIM) is an approach to the management of systems and networks through the interchange of management information between management systems and applications. For Windows based systems, the following standards are emerging:

- Common Information Model (CIM) Version 2.2, Distributed Management Task Force, Inc., 14 June 1999.
- Common Information Model (CIM) Schema Version 2.5, Distributed Management Task Force, Inc., 12 June 2001.
- Desktop Management Interface V2.0s Specification, Distributed Management Task Force, Inc., 24 June 1998.
- Specification for the Representation of CIM in XML Version 2.0, Distributed Management Task Force, Inc., 20 July 1999.
- IETF RFC 3060, Policy Core Information Model 6 Version 1 Specification, Internet Engineering Task Force, February 2000.
- Specification for CIM Operations over HTTP Version 1.0, Distributed Management Task Force, Inc., 11 August 1999.

2.5.11 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.

2.5.11.1 Distributed-Object Computing

Currently there are a number of competing middleware technologies which enable distributed objects to interoperate. In recognizing that each of these distributed-object computing technologies has strengths that differentiate it from the others, the JTA does not mandate the use of any single one. However, in order to ensure interoperability among application objects in heterogeneous distributed environments or different object models, the JTA mandates a requirement for interworking with the Object Management Group (OMG) Object Management Architecture (OMA). The OMA is composed of the Common Object Request Broker Architecture (CORBA), CORBAservices, and CORBAfacilities. For COM, application-level interworking results in COM clients interacting with non-COM servers and non-COM clients interacting with COM servers.

2.5.11.1(a) Mandated. 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.

2.5.12 Environment Management

Environment management services integrate and manage the execution of platform services for particular applications and users. These services are invoked via an easy-to-use, high-level interface that enables users and applications to invoke platform services without having to know the details of the technical environment. The environment management service determines which platform service is used to satisfy the request and manages access to it through the API.

2.5.12.1 Electronic Records Management

This section provides standards for Electronic Records Management.

2.5.12.1(a) Mandated. There are no mandated standards for Electronic Records Management.

2.5.12.1(b) Emerging. 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. The following standard is emerging:

– DoD-5015.2-STD, Design Criteria Standard for Electronic Records Management Software Applications, 19 June 2002 (Sections 2.2.1–2.2.1.1 only).

2.5.12.2 Learning Technology

Learning Technology standards provide for an integrated environment for education, training, and decision support. A growing number of technical standards for this field are in varying stages of development.

2.5.12.2(a) Mandated. There are no mandated standards for Learning Technology.

2.5.12.2(b) Emerging. The following standards are being tracked as Learning Technology emerging standards:

- IEEE 1484.1, Standard for Information Technology – Education and Training Systems Architecture and Reference Model, LTSA Draft 9, 2001-11-30.
- IEEE P1484.2, Standard for Information Technology – Learning Systems – Learner Model, PAPI Learner, Draft 7, 2000-11-29.
- IEEE 1484.11.1, Draft Standard for Learning Technology – Data Model for Content to LMS Communications, 2001-03-15.
- IEEE 1484.12.1, Draft Standard for Learning Object Metadata, 2002-03-04.

2.5.12.3 Biometric Technology Services

Biometric technologies are intended to overlay or replace password systems so that positive access control can be achieved. The Biometric API (BioAPI) Specification allows software applications to communicate with a broad range of biometric technologies by providing a high-level generic biometric authentication model that is suited for any form of biometric technology. It covers the basic functions of Enrollment, Verification, and Identification, and includes a database interface to allow a biometric service provider (BSP) to manage the Identification population.

The Common Biometric Exchange File Format (CBEFF) defines a common set of data elements necessary to support multiple biometric technologies and promote interoperability and utilization of biometric data. CBEFF describes the set of required and optional data fields, and also allows for new formats to be created.

2.5.12.3(a) Mandated. The following standards are mandated:

- ANSI INCITS 358-2002, BioAPI Specification, Version 1.1, Feb 13, 2002.
- NIST, NISTIR 6529, Common Biometric Exchange File Format (CBEFF), January 3, 2001.

Section 3: Information Transfer Standards

3.1 Introduction

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

3.2 Purpose and 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), secondary imagery dissemination, and Identification Friend or Foe (IFF). Networking and internetworking standards are identified. Transmission media standards for Military Satellite Communications (MILSATCOM), Synchronous Optical Network (SONET), and radio links as well as network and systems management standards for data communications and telecommunications are identified. In addition, several communication services include emerging technologies and standards that should be monitored for future extension of information transfer capabilities.This section includes the Communications Services depicted in Figure 1-3, DoD Technical Reference Model. Security standards are addressed in Section 6.

3.3 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).

This section contains two versions of the Internet Protocol (IP), IP Version 4 (IPv4) and IP Version 6 (IPv6), and identifies the services that will operate for each IP version. For IPv6 there are some services that may require the use of emerging standards.

Within this section, system components are categorized as end-systems, networks, subnetworks, and transmission media. Each component is addressed in subsequent paragraphs. End-systems (e.g., host computers, and terminals) (3.4) generally execute applications on behalf of users and share information with other end-systems via networks. Networks (3.5) 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. Subnetworks (3.6) are interconnected via routers which 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 (3.7).

This section also addresses the standards used to manage system components (3.8). Network and systems management includes the set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the status and resources of components.

3.4 End Systems Standards

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

3.4.1 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 also adds additional discussion and guidance for implementers. 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.

3.4.1(a) Mandated. For IPv4, the following standard is mandated:

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

3.4.1.1 Electronic Mail

The standard for official organizational-messaging traffic between DoD organizations is the Defense Message System's (DMS) X.400-based suite of military messaging standards defined in Allied 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 3.4.1.10.3 for operation over Internet Protocol (IP)-based networks.

3.4.1.1(a) Mandated. Current implementations of ACP 123 will need to be modified to accommodate interfaces for IPv6. For IPv4 and IPv6, 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, 26 June 2001.

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 IPv4 and IPv6, the following SMTP standards are mandated:

- IETF RFC 1870, Simple Mail Transfer Protocol Services Extension for Message Size Declaration, November 1995.
- IETF RFC 2821, Simple Mail Transfer Protocol, April 2001.
- IETF RFC 2822, Internet Message Format, April 2001.
- IETF RFCs 2045-2049, Multipurpose Internet Mail Extensions (MIME) Parts 1-5, November 1996.

3.4.1.1(b) Emerging. For IPv4 and IPv6, the following SMTP standards are emerging:

- IETF RFC 2231, MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations, November 1997.
- IETF RFC 2646, The Text/Plain Format Parameter, August 1999.
- IETF RFC 3023, XML Media Types, January 2001.

3.4.1.2 Directory Services

Directory services are basically pointer systems, housed in databases that store information on how to locate, archive, administer, and use a large collection of data about users and resources in a networked environment.

3.4.1.2.1 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 3.4.1.11 for operation over IP-based networks.

3.4.1.2.1(a) Mandated. Current implementations of X.500 will need to be modified to accommodate interfaces for IPv6. For IPv4 and IPv6, the following standard is mandated:

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

3.4.1.2.1(b) Emerging. For IPv4 and IPv6, the following standard is emerging:

– ITU-T X.500, The Directory – Overview of Concepts, Models, and Services – Data Communication Networks Directory, February 2001.

3.4.1.2.2 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.

3.4.1.2.2(a) Mandated. For IPv4 and IPv6, the following standard is mandated:

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

3.4.1.2.2(b) Emerging. Lightweight Directory Access Protocol Version 3 (LDAPv3) 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. For IPv4 and IPv6, the following standard is emerging:

– IETF RFC 2251, Lightweight Directory Access Protocol Version 3, December 1997.

3.4.1.2.3 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.

3.4.1.2.3(a) Mandated. For IPv4 and IPv6, 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.

It should be noted that the two previous standards define various Recource Records (RRs) and DNS name mapping that are specific to IPv4.

For IPv6 RRs and IPv6 address to DNS name mapping, the following standards are mandated:

- IETF RFC 1886, DNS Extensions to Support IPv6, December 1995.
- IETF RFC 3152, Delegation of IP6.ARPA, August 2001.

3.4.1.2.3(b) Emerging. For IPv4 and IPv6, the following DNS related standards are emerging:

- IETF RFC 1995, Incremental Zone Transfer in DNS, August 1996.
- IETF RFC 1996, A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY), August 1996.

3.4.1.3 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.

3.4.1.3(a) Mandated. For IPv4 and IPv6, 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).

In addition for IPv6, the relevant sections of the following standard is mandated:

- IETF RFC 2428, FTP Extensions for IPv6 and Network Address Translators (NATs), September 1998.

3.4.1.4 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.

3.4.1.4(a) Mandated. For IPv4 and IPv6, the following standard is mandated:

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

3.4.1.5 Network Time Synchronization

Network Time Protocol (NTP) provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet.

3.4.1.5(a) Mandated. For IPv4, the following standard is mandated:

- IETF RFC 1305, Network Time Protocol (Version 3) Specification, Implementation, and Analysis, March 1992.

3.4.1.6 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.

3.4.1.6(a) Mandated. For IPv4, 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.

3.4.1.7 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.

3.4.1.7(a) Mandated. For IPv4, the following standard is mandated:

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

3.4.1.7(b) Emerging. For IPv6, the following standard is emerging:

– IETF RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), July 2003.

3.4.1.8 Web Services

Web services provide the server and client with Web access features for connections between browser and server.

3.4.1.8.1 Hypertext Transfer Protocol

Hypertext Transfer Protocol (HTTP) is used for search and retrieval within the Web. For securing HTTP, see Section 6.

3.4.1.8.1(a) Mandated. For IPv4 and IPv6, the following standard is mandated:

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

3.4.1.8.2 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:).

3.4.1.8.2(a) Mandated. For IPv4 and IPv6, the following standards for the syntax of URIs and URLs are mandated:

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

3.4.1.8.2(b) Emerging. For IPv6, the following standard for the syntax of URLs, is emerging:

– IETF RFC 2732, Format for Literal IPv6 Addresses in URLs, December 1999.

3.4.1.9 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.

3.4.1.9(a) Mandated. For IPv4, the following standard is mandated:

- MIL-STD-2045-47001C, Connectionless Data Transfer Application Layer Standard, 22 March 2002.

This standard is currently being updated to work in an IPv6 environment.

3.4.1.10 Transport Services

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

3.4.1.10.1 Transmission Control Protocol

Transmission Control Protocol (TCP) provides a reliable connection-oriented transport service.

3.4.1.10.1(a) Mandated. For IPv4 and IPv6, 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.
- IETF RFC 2581, TCP Congestion Control, April 1999.

3.4.1.10.2 User Datagram Protocol

User Datagram Protocol (UDP) provides an unacknowledged, connectionless datagram transport service.

3.4.1.10.2(a) Mandated. For IPv4 and IPv6, the following standard is mandated:

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

3.4.1.10.3 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.

3.4.1.10.3(a) Mandated. For IPv4, the following standard is mandated:

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

3.4.1.10.3(b) Emerging. For IPv4 and IPv6, the following standard is emerging:

– IETF RFC 2126, ISO Transport Service on Top of TCP (ITOT), March 1997.

3.4.1.11 Network Services

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. Currently, IP Version 4 (IPv4) is the mandated internetworking protocol for networks carrying operations traffic within DoD. IPv6 is the next generation network layer protocol of the Internet and DoD. IPv6 has been designed to provide better internetworking capabilities than are currently available within IPv4. IPv6 includes supports for the following: expanded addressing and routing capabilities, authentication and privacy, auto-configuration, and traffic class and flow label fields to facilitate implementation of quality of service capabilities.

3.4.1.11(a) Mandated. All implementations of IPv4 must pass the 8-bit Type-of-Service (TOS) byte transparently up and down through the transport layer as defined in IETF Standard 3, Requirements for Internet Hosts, Communication Layers, October 1989. For IPv4, 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, Requirements for Internet Hosts, Communications Layers, October 1989.
- 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 multiaddressed IP option field must be used. For IPv4, the following standard is mandated:

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

For IPv6, the following standards are mandated:

- 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.

3.4.1.11(b) Emerging. For IPv6, the following standards are emerging:

- IETF RFC 1981, Path MTU Discovery for IPv6, August 1996.
- IETF RFC 2473, Generic Packet Tunneling in IPv6 Specification, December 1998.
- IETF RFC 2710, Multicast Listener Discovery (MLD) for IPv6, October 1999.
- IETF RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture, April 2003.
- IETF RFC 3587, IPv6 Global Unicast Address Format, August 2003.

Mobile Host Protocol (MHP) 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. For IPv4, the following standards are emerging:

- IETF RFC 2794, Mobile IP Network Access Identification Extension for IPv4, March 2000.
- IETF RFC 3344, IP Mobility Support for IPv4, August 2002.

For IPv4 and IPv6, the following standard is emerging:

– IETF RFC 2507, IP Header Compression, February 1999.

3.4.1.12 Quality of Service

Quality of Service (QoS) is the ability of a network to ensure that the predetermined traffic and service requirements of a network element (e.g., end-system, router, application) can be satisfied.

3.4.1.12(a) Mandated. No additional standards are mandated for Quality of Service.

3.4.1.12(b) Emerging. 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 3.5.4 for emerging Network QoS standards. For IPv4 and IPv6, the following receiver-initiated QoS standard is emerging:

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

3.4.1.13 Voice Over IP

Voice Over IP (VoIP) 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.

3.4.1.13(a) Mandated. No additional standards are mandated for Voice over IP.

3.4.1.13(b) Emerging. The following VoIP standards are emerging:

– ITU-T Recommendation H.323, Packet-Based Multimedia Communications Systems (Version 2), February 1998.
– IETF RFC 3261, Session Initiation Protocol, June 2002.
– IETF RFC 3015, Megaco Protocol Version 1.0, November 2000.
– IETF RFC 1889, RTP: A Transport Protocol for Real-Time Applications, January 1996.

3.4.1.14 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.

3.4.1.14(a) Mandated. There are no mandated standards for Communication Protocols for High-Stress, Resource-Constrained Environments.

3.4.1.14(b) Emerging. 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 four protocols that operate at or above the network layer of the Open Systems Interconnect (OSI) model—File Protocol, Transport Protocol, Security Protocol, and Network Protocol.

For stressed communications environments (such as satellite links) where high bit error rates, long 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 – Protoco specification for space communications – Network protocol, 5 October 2000.
- CCSDS 713.5-B-1/ISO 15892:2000, Space data and information transfer systems – Protocol specification for space communications – Security protocol, 5 October 2000.
- CCSDS 714.0-B-1/ISO 15893:2000, Space data and information transfer systems – Protocol specification for space communications – Transport protocol, 5 October 2000.
- CCSDS 717.0-B-1/ISO 15894:2000, Space data and information transfer systems – Protocol specification for space communications – File protocol, 5 October 2000.

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

3.4.2 Video Teleconferencing Standards

The ASD(C3I) mandated Federal Telecommunications Recommendation (FTR) 1080B-2002 Video Teleconferencing Profile (VTCP) identifies ITU-T H.320 and H.323 as the key standards to provide interoperability between Video Teleconferencing (VTC) terminal equipment. ITU-T H.320, Narrow Band Visual Telephone Systems and Terminal Equipment, May 1999, is an umbrella standard of recommendations addressing audio, video, signaling and control for digital circuit switched networks operating at data rates of 56-1,920 kilobits per second (kbits/s) such as ISDN. ITU-T H.323, Packet-based Multimedia Communications Systems, February 1998, is an umbrella standard of recommendations addressing audio, video, signaling and control for packet-switched networks. Also in the FTR is ITU-T T.120, Data Protocols for Multimedia Conferencing, 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.

3.4.2(a) Mandated. For Video Teleconferencing Units (VTUs) and Multipoint Control Units (MCUs) the following standards, as they are profiled by FTR 1080B-2002, Appendix A, VTCP, August 2002, are mandated:

For VTU/MCU general, the following standards are mandated:

- ITU-T H.231, Multipoint Control Units for Audiovisual Systems Using Digital Channels up to 1920 kbit/s, July 1997.
- ITU-T H.243, Procedures for Establishing Communication Between Three or More Audiovisual Terminals Using Digital Channels up to 1920 kbit/s, February 2000.

For VTU/MCU audio, the following standard is mandated:

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

For VTU/MCU audio over circuit switched networks, the following standard is mandated:

- ITU-T G.728, Coding of Speech at 16 kbit/s Using Low-Delay Code Excited Linear Prediction, September 1992.

For MCU audio over circuit switched networks, the following standard is mandated:

- ITU-T G.722, 7 kHz Audio-Coding Within 64 kbit/s, November 1988.

For VTU/MCU video, the following standard is mandated:

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

For VTU/MCU multimedia, applications implementing the features of audiographic conferencing, facsimile, still image transfer, annotation, pointing, whiteboard, file transfer, audio visual control, and application sharing, operating at data rates of 9.6 to 1,920 kbit/s, 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, Data Protocols for Multimedia Conferencing, July 1996.
- ITU-T T.122, Multipoint Communications Service – Service Definition, February 1998.
- ITU-T T.123, Network – Specific Data Protocol Stacks for Multimedia Conferencing, May 1999.
- ITU-T T.124, Generic Conference Control, February 1998.
- ITU-T T.125, Multipoint Communications Service Protocol Specification, February 1998.
- ITU-T T.126, Multipoint Still Image and Annotation Protocol, July 1997.
- ITU-T T.127, Multipoint Binary File Transfer Protocol, August 1995.
- ITU-T T.128, Multipoint Application Sharing, February 1998.

For VTU/MCU circuit switched networks, the following standards are mandated:

- ITU-T H.221, Frame Structure for 64 to 1920 kbit/s Channel in Audiovisual Services, May 1999.
- ITU-T H.224, Real-time Control Protocol for Simplex Applications Using the H.221 LSD/HSD/MLP Channels, February 2000.
- ITU-T H.230, Frame-Synchronous Control and Indication Signals for Audiovisual Systems, May 1999.
- ITU-T H.242, System for Establishing Communication Between Audiovisual Terminals Using Digital Channels up to 2 Mbps, May 1999.
- ITU-T H.281, Far-End Camera Control Protocol for Video Conferences Using H.224, November 1994.

- ITU-T H.320, Narrow-band Visual Telephone Systems and Telephone Equipment, May 1999.

For VTU/MCU packet switched networks, the following standards are mandated:

- ITU-T H.225.0, Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communications Systems, February 1998.
- ITU-T H.245, Control Protocol for Multimedia Communications, February 1998.
- ITU-T H.323, Packet-based Multimedia Communications Systems, February 1998.

For all other VTC implementations, such as those used over wide area networks where bandwidth, quality of service, and scalability may not be sufficient for IP-based video conferencing, see emerging standards in 3.4.2(b).

For VTC terminals operating at low bit rates (9.6 to 28.8 kbit/s), the following standard is mandated:

- ITU-T H.324, Terminal for Low Bit Rate Multimedia Communications, March 2002.

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 kbit/s channels, July 1995.

For information on the ASD (C3I) VTC guidance and the FTR 1080B-2002 VTCP see http://www.ncs.gov/n2.

3.4.2(b) Emerging. For integrating packet and circuit switched networks for transmission of multimedia traffic, the following standards are emerging:

- ITU-T H.323, Packet-based Multimedia Communications Systems, November 2000. This standard has the most industry support for VTC over ATM.

The above standard provides for two modes of operation over ATM: 1) IP over ATM media stream for delivery of H.225.0 and H.245 messages and for the RTCP portion of the audio and video streams, and 2) Real-Time Protocol (RTP) on AAL5 for RTP audio and video streams. 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.

- ITU-T H.248, Gateway Control Protocol, June 2000.
- IETF RFC 3435, Media Gateway Control Protocol (MGCP) Version 1.0, January 2003.
- IETF RFC 3261, Session Initiation Protocol (SIP), June 2002.

For IP-based, broadcast-quality video rates of less than 1 Mbps, the ISO/IEC MPEG and the ITU-T Video Coding Expert Group (VCEG) have joined efforts in the development of the emerging H.26L standard which was initiated by the ITU-T committee. Upon ratification, the new standard will be designated as ITU-T H.264 and MPEG-4 Part 10. The following standard is emerging:

- ITU-T H.264/ISO/IEC FCD 14496-10, Advanced Video Coding, July 2002.

3.4.3 Facsimile Standards

The following facsimile standards are required for transmitting and receiving hardcopy in analog and digital forms. Facsimile is the process by which fixed graphic images, such as printed text and pictures,

are scanned, and the information converted into electrical signals that may be transmitted over a telecommunications system and used to create a copy or file of the original. Facsimile standards can be also employed for the transmission and reception of facsimile data to or from a computer without requiring a hard copy at either end. The following facsimile standards are required for transmitting and receiving copy in analog and digital modes.

3.4.3.1 Analog Facsimile Standards

Mandated facsimile (analog output) standards comply with the ITU-T Group 3 specifications.

3.4.3.1(a) Mandated. 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.

3.4.3.2 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.

3.4.3.2(a) Mandated. The following standard is mandated:

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

3.4.4 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 3.4.1.10 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 (TIS) to connect the TACO2 host to specific cryptographic equipment.

3.4.4(a) Mandated. 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.

3.4.5 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.

3.4.5(a) Mandated. 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 at http//gps.losangeles.af.mil.

3.4.5(b) Emerging. 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 emerging:

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

3.4.6 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.

3.4.6(a) Mandated. 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.

3.4.6(b) Emerging. The following standard defines the required characteristics of military IFF systems to support the new NATO Mode 5 capabilities:

– DoD AIMS 03-1000 Mark XIIA, Performance/Design and Qualification Requirements Technical Standard for the ATCRBS/IFF/MARK XIIA Electronic Identification System and Military Mode S.

3.5 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.

3.5.1 Internetworking (Router) Standards

Routers are used to interconnect various subnetworks and end-systems. Protocols necessary to provide this service are specified below. IETF RFC 1812 is an umbrella standard that references other documents and corrects errors in some of the referenced documents. In addition, some of the standards mandated for hosts in 3.4.1 also apply to routers. Security requirements are addressed in Section 6.

3.5.1(a) Mandated. For IPv4, the following standards are mandated:

- IETF RFC 1812, Requirements for IP Version 4 Routers, 22 June 1995.
- IETF RFC 951, Bootstrap Protocol, September 1985.
- IETF RFC 1542, Clarifications and Extensions for the Bootstrap Protocol, October 1993.
- IETF RFC 2131, Dynamic Host Configuration Protocol, March 1997.
- IETF RFC 2132, DHCP Options and BOOTP Vendor Extensions, March 1997.
- IETF Standard 33/RFC 1350, The TFTP Protocol (Revision 2), July 1992, to be used for initialization only.

For IPv4 and IPv6, the following standards are mandated:

- 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.

For IPv6, the following standards are mandated:

- IETF RFC 1886, DNS Extensions to Support IPv6, December 1995.
- IETF RFC 3152, Delegation of IP6.ARPA, August 2001.

3.5.1(b) Emerging. For IPv6, the following standard is emerging:

– IETF RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), July 2003.

3.5.2 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. Currently, IP Version 4 (IPv4) is the mandated internetworking protocol for networks carrying opertions traffic within DoD. IPv6 is the next generation network layer protocol of the Internet and DoD. IPv6 has been designed to provide better internetworking capabilities than are currently available within IPv4. IPv6 includes supports for the following: expanded addressing and routing capabilities, authentication and privacy, autoconfiguration, and traffic class and flow label fields to facilitate implementation of quality of service capabilities.

3.5.2(a) Mandated. For IPv4, 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 multiaddressed datagrams over CNR, the multiaddressed IP option field must be used. For IPv4, the following standard is mandated:

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

For IPv6, the following standards are mandated:

- 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.

3.5.2(b) Emerging. For IPv6, the following standards are emerging:

- IETF RFC 1981, path MTU Discovery for IPv6, August 1996.
- IETF RFC 2710, Multicast Listener Discovery (MLD) for IPv6, October 1999.
- IETF RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture, April 2003.
- IETF RFC 3587, IPv6 Global Unicast Address Format, August 2003.

Mobile Host Protocol (MHP) 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. For IPv4, the following standards are emerging:

- IETF RFC 2794, Mobile IP Network Access Identification Extension for IPv4, March 2000.
- IETF RFC 3344, IP Mobility Support for IPv4, August 2002.

For IPv4 and IPv6, the following standard is emerging:

- IETF RFC 2507, IP Header Compression, February 1999.

3.5.3 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.

3.5.3.1 Interior Routers

Routers within an autonomous system are considered local routers that are administered and advertised locally by means of an interior gateway protocol.

3.5.3.1(a) Mandated. For IPv4 unicast interior gateway routing, the following standard is mandated:

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

For IPv6 unicast interior gateway routing, the following standard is mandated:

- IETF RFC 2740, OSPF for IPv6, December 1999.

3.5.3.2 Exterior Routers

Exterior gateway protocols are used to specify routes between autonomous systems.

3.5.3.2(a) Mandated. For IPv4 and IPv6 exterior gateway routing, Border Gateway Protocol 4 (BGP-4) using 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.

For IPv6 exterior gateway routing, Border Gateway Protocol 4 (BGP-4) using TCP as a transport service, the following standards are mandated:

- IETF RFC 2545, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing, March 1999.
- IETF RFC 2858, Multiprotocol Extensions for BGP-4, June 2000.

3.5.4 Network Quality of Service Standards

Quality of Service (QoS) is the ability of a network to ensure that the predetermined traffic and service requirements of subnetwork elements satisfy the end to end interoperability requirements of the network.

3.5.4.1 General Quality of Service Standards

To ensure interoperability by providing acceptable quality of service within DoD networks.

3.5.4.1(a) Mandated. No additional standards are mandated for this section.

3.5.4.1(b) Emerging. 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 for IPv4 and IPv6:

- 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 2210, The Use of RSVP with IETF Integrated Services, September 1997.
- IETF RFC 2380, RSVP over ATM Implementation Requirements, August 1998.
- IETF RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.
- IETF RFC 3031, Multi-protocol Label Switching Architecture, January 2001.
- IETF RFC 3168, The Addition of Explicit Congestion Notification (ECN) to IP, September 2001.
- IETF RFC 3175, Aggregation of RSVP for IPv4 and IPv6 Reservations, September 2001.
- IEEE 802.1Q:1998, IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridge Local Area Networks.
- ISO/IEC 15802-3:1998, Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Common specifications – Part 3: Media Access Control (MAC) Bridges.

3.5.4.2 Voice Quality of Service Standards

To ensure interoperability by providing acceptable service quality between voice services within the Defense Switched Network (DSN).

3.5.4.2(a) Mandated. The following standards are mandated:

- ITU-T P.800, Methods for Subjective Determination of Transmission, August 1996.
- ITU-T P.862, Perceptual Evaluation of Speech Quality (PESQ), an Objective Method for End-to-End Speech Quality Assessment of Narrowband Telephone Networks and Speech Codecs, February 2002.

3.6 Subnetworks

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

3.6.1 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).

3.6.1(a) Mandated. The following standards are mandated as the minimum set for operation in a Joint Task Force for platforms physically connected to a Joint Task Force LAN.

- ISO/IEC 8802-3:2000 (IEEE Std. 802.3, 2000 Edition), Information technology, Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, Clauses 21-30 for 100BaseT and Clause 14 for 10BaseT.

For IPv4, the following standards are mandated:

- 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.

3.6.1(b) Emerging. 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 following standards are emerging:

- 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.

For using IPv6 over Joint Task Force ethernet LANs, the following standard is emerging:

- IETF RFC 2464, Transmission of IPv6 Packets over Ethernet Networks, December 1998.

3.6.2 Point-to-Point Standards

The point-to-point standards are designed for single links that transport packets between two peers. These links provide full-duplex simultaneous bi-directional operation, and are assumed to deliver packets in order.

3.6.2(a) Mandated. For full-duplex, synchronous or asynchronous, point-to-point communications, for IPv4, the following standard is mandated:

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

For full-duplex, synchronous or asynchronous, point-to-point communications, for IPv4 and IPv6, the following standards are mandated:

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

3.6.2(b) Emerging. 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. For IPv4, the following standards are emerging:

- IETF RFC 1990, The PPP Multilink Protocol, August 1996.
- IETF RFC 3241, Robust Header Compression (ROHC) over PPP, April 2002.

For IPv6, the following standards are emerging:

- IETF RFC 2472, IP Version 6 over PPP, December 1998.
- IETF RFC 3241, Robust Header Compression (ROHC) over PPP, April 2002.

3.6.3 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-188-220C.

3.6.3(a) Mandated. With the exception of High Frequency (HF) networks, MIL-STD-188-220C is mandated as the standard communications net access protocol for CNR networks. For IPv4, the following standard is mandated:

- MIL-STD-188-220C, Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, 22 May 2002.

This standard is currently being updated to work in an IPv6 environment.

3.6.4 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- 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.

3.6.4(a) Mandated. For BRI physical layer, the following standards are mandated:

- 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, the following standard is mandated:

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

For the data-link layer, the following standard is mandated:

- ANSI T1.602-1996 (R2000), ISDN Data Link Signaling Specification for Application at the User Network Interface, 1996 (Reaffirmed 2000).

For signaling at the user-network interface, the following standards are mandated:

- ANSI T1.607-2000, ISDN – Layer 3 Signaling Specification for Circuit Switched Bearer Service for Digital Subscriber Signaling System Number 1 (DSS1), 2000.
- ANSI T1.610-1998, DSS1 – Generic Procedures for the Control of ISDN Supplementary Services, 1998.
- ANSI T1.619-1992 (R1999), Multi-Level Precedence and Preemption (MLPP) Service, ISDN Supplementary Service Description, 1992 (Reaffirmed 1999).
- ANSI T1.619a-1994 (R1999), Supplement, 1994 (Reaffirmed 1999).

For signaling at node-to-node interface, the following standards are mandated:

- ANSI T1.111-2001, Signaling System No. 7, Message Transfer Part, 2001.
- ANSI T1.112-2001, Telecommunications – Signaling System Number 7 (SS7) – Signaling Connection Control Part (SCCP), 2001.
- ANSI T1.113-2000, Signaling System No. 7, ISDN User Part, 2000.
- ANSI T1.114-2000, Signaling System Number 7 (SS7) – Transaction Capabilities Application Part (TCAP), 2000.

For addressing, the following standards are mandated:

- 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, the following standard is mandated:

- 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, the following standard is mandated:

- IETF RFC 1618, PPP over ISDN, 13 May 1994.

3.6.5 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.

3.6.5(a) Mandated. For Physical Layer, the following standards are mandated:

- 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 V3.1, 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, the following standards are mandated:

- 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, the following standards are mandated:

- 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, the following standard is mandated:

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

For Circuit Emulation Functions, the following standard is mandated:

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

For AAL1 and AAL5 Functions, the following standards are mandated:

- 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, the following standards are mandated:

- 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, the following standards are mandated:

- 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, the following standard is mandated:

- DoD ATM Addressing Plan, 17 April 1998.

3.6.5(b) Emerging. 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.

- ATM Forum, af-aic-0178.000, ATM-Multiprotocol Label Switching (MPLS) Network Interworking Version 1.0, August 2001.
- 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.

3.6.6 Gigabit Ethernet

Gigabit Ethernet extends the speed of the Ethernet specification to 1 Gbps. Gigabit Ethernet is used for campus networks and building backbones.

3.6.6(a) Mandated. While no specific LAN/CAN technology is mandated, when using Gigabit Ethernet (1000 Mbps service) over fiber or Category 5 copper cabling, the following physical layer and framing standard is mandated:

- ISO/IEC 8802-3:2000 (IEEE Std. 802.3, 2000 Edition), Information technology, Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, Clauses 36, 37 and 38 for fiber and Clause 40 for Category 5 copper.

3.6.7 Mobile Cellular

Currently fielded Second Generation (2G) Personal Communications Service (PCS) wireless systems will eventually be replaced by Third Generation (3G) wireless/cellular systems, which are currently being developed in North America, Europe, and in various Asian countries. The umbrella standard for 3G is the ITU IMT-2000 family of standards. The complete set of 3G Radio interface specifications for both TDMA and CDMA is contained in Recommendation ITU-R M.1457-1 (also called IMT.RSPC). 3G systems need to meet the requirement of supporting data transmission at 144 kb/s for the vehicular user, 384 kb/s for the dismounted and outdoor to indoor user, and 2 Mb/s for the indoor office user. The major issues that are being resolved include support for legacy cellular systems and mutually agreed upon cellular standards that permit global roaming. The standards associated with the groups devoted to developing and updating 3G and the Recommendation ITU-R M.1457-1 are the following: (1) The 3rd Generation Partnership Project (3GPP), which is focused on 3G extensions of the European GSM system and interoperability of North American TDMA (IS-136) and the 3G follow-on, UWC-136, (known in ITU as TDMA Single-Carrier (SC)) with GSM and UMTS. The 3GPP standards encompass GSM and GSM-MAP based Wideband CDMA (WCDMA) (known in ITU as CDMA Direct Spread (DS)). It is also known as the Universal Mobile Telecommunications System (UMTS) and is a part of the ITU IMT-2000 concept. (2) The Third Generation Partnership Project 2 (3GPP2) is a collaborative third generation (3G) telecommunications standards-setting project comprised of North American and Asian interests developing global specifications for interface to ANSI/TIA/EIA-41. The 3GPP2 is focused on the 3G extension of the cdmaOne (North American) CDMA standard, and is one of the initiatives of the ITU IMT-2000 concept. 3GPP2 data standards (cdma2000, known in ITU as CDMA Multi-Carrier (MC)) are based upon IS-95B. IS-95B is the packet mode version of direct sequence CDMA standard IS-95A. 3GPP2 uses existing work in the Internet Engineering Task Force (IETF) on mobile IP to enhance network architecture. The web sites for these two projects are http://www.3gpp.org and http://www.3gpp2.org.

3.6.7(a) Mandated. No standards are mandated in this section.

3.6.7(b) Emerging. The following 3G Radio interface specification that contains both 3GPP and 3GPP2 developed standards is emerging:

– ITU-R M.1457-1, Detailed Specifications of the Radio Interfaces of IMT-2000, February 2001.

3.7 Transmission Media

Transmission media is used to transmit information from one location to another location. This section addresses the following types of transmission media: military satellite communications, radio communications, and synchronous optical network transmission.

3.7.1 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.

3.7.1.1 Ultra High Frequency Satellite Terminal Standards

The UHF SATCOM system operates on the high VHF and low UHF frequencies (Uplink 292 to 319 MHz; Downlink 243 to 270 Mhz). These relatively low frequency bands are used for supporting many long-haul tactical, contingency, and special military operations. This section includes the standards that define the interoperability and performance requirements for user terminals and access controllers that operate over the military UHF SATCOM system. UHF Satellite Terminal Standards define the waveforms and protocols to allow user communications over unprocessed transponders on Fleet SATCOM (FLTSAT) and UHF Follow-on (UFO) satellites.

3.7.1.1(a) Mandated. The following standards are mandated:

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, with Notice of Change 1, 16 October 2001.

For 5-kHz only Demand-Assigned Multiple Access (DAMA) service, supporting the transmission of data at 75 to 2400 bps and messaging and multi-hop, 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.

For 5- and 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 (Including 5-kHz and 25-kHz Slave Channels), 20 March 1998; with Notice of Change 1, 9 September 1998; and Notice of Change 2, 4 June 1999.

For data controllers operating over single-access 5-kHz and 25-kHz UHF SATCOM channels (a robust link protocol that can transfer error-free data efficiently and effectively over channels that have high error rates), the following standard 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.

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.

3.7.1.1(b) Emerging. The UHF SATCOM standards are undergoing a major revision and will be superseded by these emerging standards when they are approved. The emerging standards are being developed in a layered type structure following the ISO/OSI model. The new standards will eliminate the functional duplicity of the present standards and will make them easier and less expensive to implement. The following standards are emerging:

- MIL-STD-188-182B, Interoperability and Performance Standard for UHF SATCOM DAMA Orderwire Messages and Protocols.
- MIL-STD-188-183B, Interoperability and Performance Standard for Multiple Accessing 5-kHz and 25-kHz UHF SATCOM Channels.
- MIL-STD-188-184A, Interoperability and Performance Standard for the Data Control Waveform.

3.7.1.2 Super High Frequency Satellite Terminal Standards

The military SHF SATCOM system operates on the X-Band (7.25 to 8.4 GHz) of the SHF spectrum. In addition, the Department of Defense uses commercial SATCOM systems that operate on the C-Band (3.4 to 6.65 GHz) and Ku-Band (10.95 to 14.5 GHz) of the SHF spectrum. This section includes the standards that define the interoperability and performance requirements for user terminals and access controllers that will operate over military and commercial SHF SATCOM system.

3.7.1.2(a) Mandated. The following standards are mandated:

For minimum mandatory Radio Frequency (RF) and Intermediate Frequency (IF) requirements to ensure interoperability of SATCOM Earth terminals operating over C-band, X-band, Ku-band, military Ka-band, and commercial Ka-band SHF channels:

- MIL-STD-188-164A, Interoperability of SHF Satellite Communications Earth Terminals, 15 April 2002.

For minimum mandatory requirements to ensure interoperability of Phase-Shift Keying (PSK) modems operating in the Frequency Division Multiple Access (FDMA) mode with C-band, X-band, Ka-band, and Ku-band transponding SATCOM Earth Terminals:

- MIL-STD-188-165A, Interoperability of SHF Satellite Communications PSK Modems (FDMA Operation), 15 April 2002.

For the minimum mandatory requirements to ensure interoperability of SATCOM baseband equipment the following standard is mandated:

- MIL-STD-188-168, Interoperability Standard for SHF Satellite Communications Baseband Equipment, 3 October 2002.

MIL-STD-188-168 contains information concerning SHF multiplexing and de-multiplexing and does not currently address all baseband pertinent information.

3.7.1.2(b) Emerging. The following draft standards are emerging.

- 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.
- MIL-STD-188-170, Interoperability and Performance Standard for SHF Satellite Communications Anti-Jamming Modems (This modem uses spread spectrum techniques to protect SHF SATCOM user communications and control links against enemy jamming).

3.7.1.3 Extremely High Frequency Satellite Payload and Terminal Standards

This section covers standards that ensure interoperability between satellite communications systems providing jam-resistant, secure communications on the high SHF and low EHF frequencies (20 GHz and 44 GHz) for both Low and Medium Data Rates (LDR and MDR).

3.7.1.3(a) Mandated. The following standards are mandated:

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:

- 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.

For waveform, signal processing, and protocol requirements for acquisition, access control, and communications for Medium Data Rate (MDR) (4.8 kbit/s to 1.544 Mbps) EHF satellite data links:

- MIL-STD-188-136A, EHF MDR Uplinks and Downlinks, 8 June 1998; with Notice of Change 1, 1 July 1999, and Notice of Change 2, 30 October 2000.

3.7.2 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.

3.7.2(a) Mandated. The following standards are mandated:

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:

- 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:

- ISO 11754:1994, (CCSDS 101.0-B-4), Space Data and Information Transfer Systems – Telemetry Channel Coding.

For the data unit formats and functions implemented within the coding and physical layers of the satellite health and status communications:

- ISO 12171:1998, (CCSDS 201.0-B-2), Space Data and Information Transfer Systems – Telecommand – Channel Service – Architectural Specification.

For procedures and data unit formats implemented within the segmentation and transfer layers of the telecommand data routing service:

- ISO 12172:1998, (CCSDS 202.0-B-2), Space Data and Information Transfer Systems – Telecommand – Data Routing Service.

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

- ISO 12173:1998, (CCSDS 202.1-B-1), Space Data and Information Transfer Systems – 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:

- ISO 12174:1998, (CCSDS 203.0-B-1), Space Data and Information Transfer Systems – 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, (CCSDS 102.0-B-4), Space Data and Information Transfer Systems – Packet Telemetry.

3.7.2(b) Emerging. For transmission of telemetry, command, and control and status data over IP-based ground networks, the following standards are emerging:

- ISO 15396:1998 (CCSDS 910.4-B-1) Space Data and Information Transfer Systems – Cross Support Reference Model – Space Link Extension Services.
- CCSDS 910.5-R-2, Space Link Extension – Service Management Specification, September 2001.

- CCSDS 910.7-R-1, Space Link Extension – Service Management – Space Link Physical Layer Management Object Specification, October 2001.
- CCSDS 911.1-R-2, Space Link Extension – Return All Frames Service Specification, November 2000.
- CCSDS 911.2-R-1, Space Link Extension – Return Virtual Channel Frames Service Specification, November 1997.
- CCSDS 912.1-R-2, Space Link Extension – Forward CLTU Service Specification, May 2000.
- CCSDS 912.3-R-1, Space Link Extension – Forward Packet Service Specification, November 1997.

3.7.3 Radio Communications

The following services are required for the transmission and reception of radio signals.

3.7.3(a) Mandated. The following standards are mandated:

For radio subsystem requirements operating in the Low Frequency (LF)/Very Low Frequency (VLF) frequency bands:

- 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.

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

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

For anti-jamming capabilities for HF radio equipment:

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

For HF data modem interfaces.

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

For radio subsystem requirements operating in the Very High Frequency (VHF) frequency bands:

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

For radio subsystem requirements operating in the Ultra High Frequency (UHF) frequency bands:

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

For anti-jamming capabilities for UHF radio equipment:

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

For radio subsystem requirements operating in the Super High Frequency (SHF) frequency bands:

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

3.7.3(b) Emerging. For anti-jamming capabilities for VHF radio systems:

– MIL-STD-188-241, RF Interface Requirements for VHF Frequency Hopping Tactical Radio Systems.

3.7.3.1 Tactical Data Link Transmission Standards

Tactical data links consist of data elements, standard message formats, protocols for exchanging the messages, and the transmission waveform.

3.7.3.1(a) Mandated. Link 16 provides for exchange of air, space, surface, subsurface, and ground tracks using J-series messages and operating in the upper UHF spectrum, and for the identification, location, and status of friendly forces. For transmission of Link 16 with the Joint Tactical Information Distribution System (JTIDS)/Multi-Functional Information Distribution System (MIDS) radios, the following standard is mandated:

- (S) STANAG 4175, Edition 3, Technical Characteristics of the Multifunctional Information Distribution System (MIDS), 6 February 2001, (U).

3.7.4 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.

3.7.4(a) Mandated. 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.
- 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.

3.8 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.

3.8.1 Data Communications Management

Data communications management stations and management agents (in end-systems and networked elements) shall support the Simple Network Management Protocol (SNMP).

3.8.1(a) Mandated. 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 2790, Host Resources MIB, March 2000.
- IETF Standard 50/RFC 1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994.
- IETF Standard 59/RFC 2819, Remote Network Monitoring Management Information Base, May 2000.
- IETF RFC 1850, Open Shortest Path First (OSPF) Version 2 Management Information Base, November 1995.

3.8.1(b) Emerging. The SNMPv3 Management Framework is described in IETF-Proposed Standard RFCs 2571 through 2575. SNMPv3 builds on the mandate SNMPV1, IETF Standard 15, 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. The following standards are emerging:

- IETF RFC 2571, An Architecture for Describing SNMP Management Frameworks, April 1999.
- IETF RFC 2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), April 1999.
- IETF RFC 2573, SNMP Applications, April 1999.
- IETF RFC 2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), April 1999.
- IETF RFC 2575, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), April 1999.

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, using SMIv2, November 1996.
- IETF RFC 2012, SNMPv2 Management Information Base for the Transmission Control Protocol (TCP), using SMIv2, November 1996.
- IETF RFC 2013, SNMPv2 Management Information Base for the User Datagram Protocol (UDP) using SMIv2, November 1996.
- IETF RFC 2021, Remote Network Monitoring Management Information Base Version 2 using SMIv2, January 1997.
- IETF RFC 2788, Network Services Monitoring MIB, March 2000.
- IETF RFC 2789, Mail Monitoring MIB, March 2000.
- IETF RFC 2515, Definitions of Managed Objects for ATM Management, February 1999.
- IETF RFC 2605, Directory Server Monitoring MIB, June 1999.

3.9 Telecommunications Management

Telecommunications management systems for telecommunications switches will implement the Telecommunications Management Network (TMN) framework to perform the exchange of information within a telecommunications network.

3.9(a) Mandated. 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, May 1996.
- ITU-T M.3211.1, TMN management service: Fault and performance management of the ISDN access, May 1996.
- ITU-T M.3400, TMN Management Functions, February 2000.
- ISO/IEC 9595:1998, Information technology – Open Systems Interconnection – Common management information service (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.

Page intentionally left blank.

Section 4: Information Modeling, Metadata, and Information Exchange Standards

4.1 Introduction

This section of the Core specifies standards for information modeling (activity, data, and object models) and information exchange (bit-oriented and character-based formatted messages).

4.2 Purpose

This section specifies the minimum information modeling, metadata, and information exchange standards DoD will use to develop or upgrade integrated, interoperable systems.

4.3 Scope (Applicability)

The Information Modeling section applies to activity models, data models, object models and data definitions used to define physical databases. Information Exchange Standards refer to the exchange of information among mission-area applications within the same system or among different systems.

Information exchange standards include the Tactical Data Links (TDLs), bit-oriented and character-based formatted messages. Among them are the Tactical Digital Information Links (TADILs) and United States Message Text Format (USMTF). The goal of these formatted messages is to provide a timely, integrated, and coherent picture for joint commanders and their operational forces.

4.4 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 define entities, their data elements, and illustrate the interrelationships among the entities. A data model identifies 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. Object models show associations and dependencies between system interfaces and the essential business rules for exercising those relationships.

The DoD Data Architecture (DDA) is an enterprise view data model that provides the structure of the Department's data to the developers of all DoD systems. The DDA has replaced the Defense Data Model (DDM). The DDA portrays DoD data standards grouped in functional views, which are aligned by Functional Data Administrators rather than subject areas as was done in the DDM. Tactical systems must incorporate applicable C2 Core Data Model (C2CDM) elements. A subset of the DDA the C2CDM also represents the C3 Functional View.

In order to provide an authoritative source for DoD data definitions and other metadata 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 Architecture (DDA) and to document content and format for data elements. System developers use this repository as a primary source of data element standards.

Efficient execution of information exchange requirements (IERs) is key to evolving DoD toward the 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. 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.

4.5 Information Modeling

This section addresses standards for three basic types of models frequently created: activity, data, and object.

4.5.1 Activity Model

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.

4.5.1(a) Mandated. 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 following standard is mandated:

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

4.5.2 Data Model

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.

4.5.2(a) Mandated. IDEF1X is used to produce a graphical information model that 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. 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 following standard for data modeling is mandated:

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

4.5.2(b) Emerging. 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 PUB 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 data modeling standard is emerging:

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

4.5.3 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.

4.5.3(a) Mandated. The Unified Modeling Language (UML) is a language for specifying, visualizing, constructing, and documenting the artifacts of software systems and business modeling. The UML includes specifications for modeling elements, notation and modeling guidelines. The UML is independent of particular programming languages and development processes. The UML supports higher-level development concepts such as collaborations, frameworks, patterns, and components, as well as analysis and design. Information may be obtained from the Web at http://www.uml.org.

- Object Management Group (OMG) Unified Modeling Language (UML) Specification, Version 1.4, September 2001.

4.5.3(b) Emerging. 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 Document Type Definitions (DTDs) for exchanging UML information. The following object modeling 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.

4.6 DoD Data Architecture Implementation

Implementation of the DDA will be interpreted to mean that it 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 page at http://www-datadmn.itsi.disa.mil/.

4.6(a) Mandated. 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 8320.1-M-1, 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 DoD Data Model Implementation standard is mandated:

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

4.7 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 8320.1-M-1. System developers shall use this repository as a primary source of data element standards.

4.7(a) Mandated. The following DoD Data Definitions standards are mandated:

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

4.7(b) Emerging. ISO/IEC 11179 describes the standardization and registering of data elements to make data understandable and shareable. Data element standardization and registration as described in ISO/IEC 11179 allow the creation of a shared data environment in much less time and with less effort than it takes for conventional data management methodologies. If ISO/IEC 11179 is ever adopted as a mandated standard it will be necessary for it to be fully harmonized with DoD 8320.1-M-1. The following standard is emerging:

– ISO/IEC 11179, Part 3 (DRAFT), Basic attributes of data elements, 19 October 2001.

4.8 Information Exchange Standards

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 that 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.

- XML based information is the widely accepted choice of 21st Century industry data/metadata interchange and is vital to the DoD's interoperability strategy. XML is widely used for metadata definition, management, and exchanges. Integrating XML with middleware technologies, CORBA for example, and core database technologies will provide the capability to exchange DoD mission-area data among heterogeneous environments. Refer to 2.5.4.1 for XML standard.

Information Exchange standards help form the Common Operating Environment (COE), ensuring the use of system or application formats that can share data. Key references include 2.5.3, for SQL standards in Data Management Services and 2.5.4 for Data Interchange Services.

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

4.8.1 Tactical Information Exchange Standards

This section addresses standards for the following types of tactical information exchange messages:

- Bit-oriented fixed and variable formatted Tactical Data Link (TDL) standards which allow real or near real-time tactical digital information exchange among air, ground, and maritime components of U.S., NATO, other allies, and friendly nations.
- Character based information standards, which provide common, human-readable, and media independent messages used for planning and execution in joint and combined operations among U.S. forces, NATO, other allies, and friendly nations.

4.8.1.1 Bit-Oriented Formatted Messages

Link 16 is a secure, jam resistant, nodeless data link that uses the Joint Tactical Information Distribution System (JTIDS)/Multifunctional Information Distribution System (MIDS) time division multiple access (TDMA) protocols, conventions, and fixed message formats. Link 16 provides for the real/near real-time exchange of air, space, surface, subsurface, and ground tracks, and orders and commands among participating units. MIL-STD-6016B defines the Link 16 message set, minimum implementation, data forwarding, and system implementation specifications, and a common data element dictionary (DED).

4.8.1.1(a) Mandated. The following standards are mandated for bit-oriented formatted messages:

- MIL-STD-6016B, Tactical Digital Information Link (TADIL) J Message Standard, 1 August 2002.

In a NATO environment, the following standard is mandated:

- STANAG 5516, Edition 2, Tactical Data Exchange – LINK 16, Ratified 10 November 1998.

Variable Message Format (VMF) is the DoD mandated standard for fire support information digital entry device exchange over tactical broadcast communications systems. The use of VMF has been extended to all war fighting functional areas. The VMF Technical Interface Design Plan (Test Edition) (TIDP-TE) defines the VMF message set and DED. VMF minimum implementation and data forwarding requirements are under development. The following standard is mandated:

- Variable Message Format (VMF), Technical Interface Design Plan (Test Edition) Reissue 5, 18 January 2002.

Utilizing J-series messages and data elements, Link 22 uses an improved high frequency (HF) and ultra-high frequency (UHF) multimedia transmission scheme. The link uses Time Division Multiple Access (TDMA) protocols, is capable of multi-netting, and provides 300 nautical mile coverage using HF and line-of-sight connectivity using UHF. The following standard is mandated:

- STANAG 5522, Edition 1, Tactical Data Exchange – LINK 22 (September 2001) is the Multinational Group (MG) agreed Configuration Management (CM) baseline document as of 15 September 1995. It is distributed as ADSIA (DKWG)-RCU-C-74-95.

MIL-STD-6016B and the VMF-TIDP-TE, R5 are under the joint configuration management authority of the TDL Configuration Control Board (CCB). STANAG 5522 is under the configuration management authority of the NATO Data Link Working Group. However, within the U.S., the TDL CCB coordinates U.S. change proposals for STANAG 5522 and the U.S. position on change proposals submitted by NATO nations. Proposed changes to the TDL standards are submitted to the TDL CCB in the form of change proposals. Once the CCB decides an Interface Change Proposal (ICP) is "approved and awaiting incorporation," the change proposal is approved for implementation. The TDLMP, the Joint Family of Message Standards, other TDL standards, ICPs, a change proposal status report, and other TDL-related information are available on the TDL Web site at http://tdl.disa.mil.

4.8.1.1(b) Emerging. The Joint Tactical Data Link Management Plan (JTDLMP) identifies the emerging Integrated Broadcast Service (IBS) standard as a member of the Joint Family of TDL Message Standards. The IBS TIDP defines CMF data elements and forwarding rules between IBS and other members of the Joint Family of TDL Message Standards.The IBS TIDP is under the configuration management authority of the IBS Message Standard Working Group (MSWG). IBS MSWG products that impact joint interoperability with TDLs are submitted by the MSWG to the TDL CCB for joint approval.The following standard is emerging:

- IBS Technical Interface Design Plan (TIDP).

4.8.1.2 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.

4.8.1.2(a) Mandated. The following Character-Based Formatted standard for USMTF messages is mandated:

- MIL-STD-6040, United States Message Text Format (USMTF), 31 March 2002.

Note: Per service agreement, USMTF User Formats are reissued as a new release on or about 31 March each year for operational use. On the same date, the approved subsequent year's release is provided to developers for system updates within one calendar year.

4.8.1.3 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.

4.8.1.3(a) Mandated. Where not addressed by another standard within the JTA (e.g., TADIL J and VMF), 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.

4.8.2 XML-based Information Exchange

The Extensible Markup Language (XML) is a markup language, based on SGML, describing structural information for data (or documents) in tagged format. The tags themselves are not predefined, but user-defined that enables flexibility in its usage. In other words, XML models structural information of data independent of tag names. It is independent of any platform and is machine and human readable enabling it to be effectively used for data/metadata interoperability. This section is concerned with exchange involving XML data formats. Examples of such data formats include object meta-data, APIs for database, transaction request-receive, mathematical equations etc. Refer to Section 2.5.4.1 for both XML and XML Schema Standards.[1]

[1] In order to facilitate interoperability, the DoD COE has established an XML Registry for collection, storage and dissemination of XML components (schemas/DTD, XML tags, elements, XST/XSL style sheets, etc.). The DoD COE XML Registry is designated to be the single authoritative DoD repository for these XML components. System developers using XML for public interface are required to consult XML Registry before creating new components and reuse existing XML where practical.

Page intentionally left blank.

Section 5: Human-Computer Interface Standards

5.1 Introduction

This section provides a common framework for Human-Computer Interface (HCI) design and implementation in DoD automated systems.

5.2 Purpose

The objective of Section 5 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 is expected to result in higher productivity; shorter training time; and reduced development, operation, and support costs.

5.3 Scope (Applicability)

Section 5 addresses standards for the presentation and dialogue of the Human-Computer Interface. For API definitions and protocols, see JTA Section 2.

5.4 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. Operators, administrators, and maintainers interact with software-based information systems using the system's 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.

5.5 General User Interface Design

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 user interface, applications shall not mix interface styles; for example, mixing character-based interfaces and GUIs or combining Windows and Motif style elements.

5.5.1 Graphical User Interface

When developing DoD automated systems, the graphical user interface shall be based on one commercial user interface style guide consistent with 5.6.1. 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 shall be a goal. 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 2.5.2 for mandated GUI standards.

5.5.2 Character-Based Interfaces

Character-based interfaces, primarily textual, are sometimes required for specialized devices due to operational, technical, or physical constraints.

5.5.2(a) Mandated. For systems with an approved requirement for character-based interfaces, guidance for developing character-based interfaces can be found in ESD-TR-86-278, Guidelines for Designing User Interface Software (Smith and Mosier), 1986), the following standard is mandated.

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

5.6 Style Guides

A 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 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.

5.6.1 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).

5.6.1.1 X-Window Style Guides

If an X-Windows-based environment is selected, the style guide corresponding to the selected version of Motif is mandated.

5.6.1.1(a) Mandated. For Motif style guides, the following standards 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.

5.6.1.2 Windows Style Guide

Windows provide the visual means by which the user can interact with an application program. The standard in this service defines the user interface in terms of appearance and behavior according to

commercial practices for Microsoft Windows based interfaces including Windows NT and Windows 2000, but not Windows XP.

5.6.1.2(a) Mandated. For a Windows-based environment, the following standard is mandated:

- Microsoft Windows User Experience, Microsoft Press, 8 September 1999.

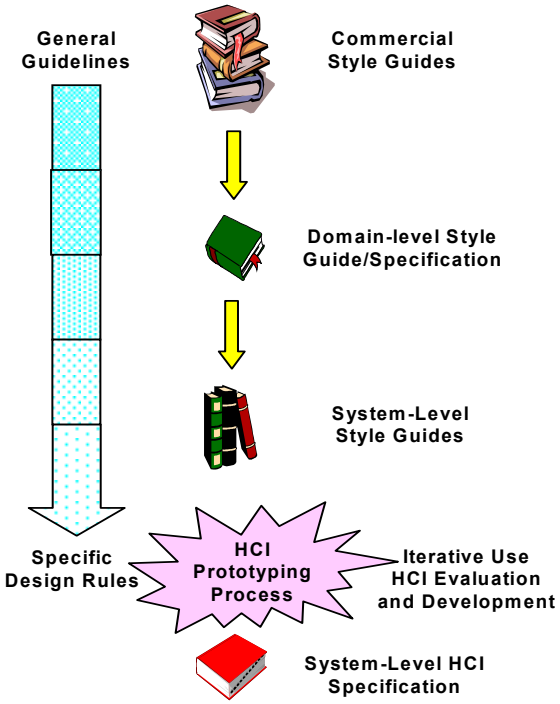


Figure 5-1: HCI Development Guidance

5.6.2 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 Common Operating Environment (COE) User Interface Specifications (UIS). Domain-level style guides should be complementary and non-conflicting with applicable commercial standards.

5.6.2(a) Mandated. For HTML, Motif, and Windows-based systems, the following domain-level style guide standard is mandated:

- Common Operating Environment (COE) User Interface Specifications (UIS), Version 4.1, 5 September 2002.

5.6.3 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 Common Operating Environment (COE) User Interface Specifications (UIS). 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-centered design processes for interactive systems" (1999), 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, reduces training and support costs, as well as improving 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/multidisciplinary design solutions to achieve the systems' interoperability and cost goals.

5.7 Symbology

The purpose of warfighting symbology is to convey information about objects in the warfighter battlespace. The display of warfighting symbology has evolved from a static, manual operation to include fully automated computer generation. This evolution has resulted in the fielding of many system-specific symbology implementations by the Combatant Commands, Services, and Agencies to meet the mission requirements of the warfighter. The 'C4I for the Warrior' concept, signed by the Chairman of the Joint Chiefs of Staff in June 1992, brings together C4I functions to provide the warfighter with a seamless, real-time, true representation of the battlespace. To achieve this capability, standardization of warfighting symbology is playing an integral role in achieving interoperability during joint service operations. Symbology has been determined to be a critical interoperability factor in today and tomorrows digital battlespace.

5.7(a) Mandated. For the display of common warfighting symbology, the following standard is mandated:

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

Section 6: Information Security Standards

6.1 Introduction

This section discusses Information Security Standards for the JTA. National Security Systems (NSS) standards should be selected such that the resultant systems and components meet validation requirements stipulated in National Telecommunications and Information Systems Security Policy (NTISSP) No. 11. Subject: National Policy Governing the Acquisition of Information Assurance (IA) and IA-enabled Information Technology Products. All other IT systems should follow FIPS PUBs on security standards and guidelines.

6.2 Purpose

This section provides the mandated and emerging information security standards necessary to implement an appropriate level of protection for DoD Information Systems.

6.3 Scope

The standards mandated in this section apply to all DoD IT systems. This section is scoped to be in compliance with the publication "Information Assurance through Defense in Depth" (February 2000) and the DoD CIO Guidance and Policy Memorandum No. 6-8510-DoD Global Information Grid Information Assurance.

The security organization is based on the Information Assurance Technical Framework (IATF) release 3.0, September 2000. Security issues are divided into the following categories: the (local) computing environment (6.4), enclave boundaries (6.5), network and infrastructure (6.6) (both internal and external to enclaves), and supporting infrastructures (6.7). The category "Evaluation Criteria" (6.8) has been added to address use of common criteria.

6.4 Computing Environment

This section covers security related standards for the local computing environment as defined by the IATF. This includes end-user workstations (both desktop and laptop) and servers. Note that some individual computing environments also need some of the services of enclave boundaries, e.g., virus detection. This section is further divided into applications (including Web browsing, e-mail, and operating system) and cryptographic security services.

6.4.1 Applications

This section provides mandated and emerging standards for secure Web browsing.

6.4.1.1 Secure Web Browsing

This service identifies the protocol used to provide communications privacy over a network. The protocol allows applications to communicate in a way designed to prevent eavesdropping, tampering, or message forgery in e-mail packages. World Wide Web services provide abilities for navigation and data transport across the internet. The protocol encapsulates various higher-level protocols and is application independent.

6.4.1.1(a) Mandated. Web browsers and web servers must first attempt to use TLS, then use SSL 3.0 if TLS is not supported. It is expected that SSL 3.0 will not be supported in the future. The following standards are both mandated for securing the communications of web browsers and web servers:

- Secure Sockets Layer (SSL) Protocol, Version 3.0, 18 November 1996.
- IETF RFC 2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999.

6.4.1.2 Secure Messaging

This service applies to the use of security implementations for the Defense Messaging System (DMS), the access control capabilities for communications with Allied partners, and for e-mail.

6.4.1.2(a) Mandated. For systems required to interface with the Defense Message System, DMS Release 3.0, for Organizational messaging, the following standard is mandated:

- FORTEZZA Interface Control Document, Revision P1.5, 22 December 1994.

ACP 120 was developed to take advantage of X.509 version 3 certificates, in particular the subjectDirectoryAttribute extension that contains the clearance attribute or the security label. This security label provides for access control based not only on hierarchical classification, but also for compartments, categories, and citizenship. For DoD message systems required to process both unclassified and classified organizational messages using DMS Release 3.0, the following messaging security protocol is mandated:

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

To support the access control capabilities of ACP 120, the following security label standards are mandated:

- ITU-T Recommendation X.411 (1999)/ISO/IEC 10021-4:1999, Information Technology – Open Systems Interconnection – Message Handling Systems (MHS) – Message Transfer System: Abstract Service Definition Procedures.
- ITU-T Recommendation X.509 (2000)/ISO/IEC 9594-8:2001, Information Technology – Open Systems Interconnection – The Directory: Public Key and Attribute Certificate Frameworks, 2001, with Technical Corrigendum 1:2002, and Technical Corrigendum 2:2002.
- ITU-T Recommendation X.481 (2000)/ISO/IEC 15816-12:2000, Information Technology – Security Techniques – Security Information Objects for Access Control.
- SDN.706, X.509 Certificate and Certificate Revocation List Profiles and Certification Path Processing Rules, Revision D, 12 May 1999.
- SDN.801, Access Control Concept and Mechanisms, Revision C, 12 May 1999.

The Secure/Multipurpose Internet Mail Extensions (S/MIME) v3 protocol suite provides application layer privacy, integrity, and non-repudiation (proof of origin) security services for messaging (e-mail). Three IETF RFCs (RFC 2630, RFC 2632, and RFC 2633) provide the above listed core security services. For individual messages that use certificates issued by the DoD PKI to protect unclassified sensitive information or sensitive information on system high networks the following standards are mandated:

- IETF RFC 2630, Cryptographic Message Syntax, June 1999.
- IETF RFC 2632, S/MIME Version 3 Certificate Handling, June 1999.
- IETF RFC 2633, S/MIME Version 3 Message Specification, June 1999.

(NOTE: that IETF RFC 2630 is being revised (draft-ietf-smime-rfc2630bis-01.txt) to remove all cryptographic algorithm specifications. Mandatory to implement algorithms will be specified in another IETF RFC (draft-ietf-smime-cmsalg-01.txt).)

IETF RFC 2634 provides optional enhanced security services, which are signed receipts (non-repudiation—proof of receipt), security labels, secure mailing lists, and signing certificates. For enhanced security services, the following standard is mandated:

- IETF RFC 2634, Enhanced Security Services for S/MIME, June 1999.

6.4.1.3 Access Control

Access control is the process to limit access to the resources of a system only to authorized processes or other systems in a network.

6.4.1.3.1 Identification and Authentication (I&A) Control: Passwords

The identification process enables recognition of an entity (subject or object) by a computer system generally by the use of unique machine-readable user names. Authentication establishes the validity of a claimed identity. This service applies to all instances where Distributed Computing Environment (DCE) 1.1 is not used. If DCE 1.1 is used see 6.4.1.3.2.

6.4.1.3.1(a) Mandated. If DCE Version 1.1 is not used, the following standard is mandated when the security policy or program security profile requires this level of protection:

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

Two additional guidance documents: NCSC-TG-017, A Guide to Understanding Identification and Authentication in Trusted Systems, 1 September 1991 (http://www.fas.org/irp/nsa.rainbow/tg017.htm); CSC-STD-002, DoD Password Management Guidance, 12 April 1985 (http://www.radium.ncsc.mil/tpep/library/rainbow.htm).

6.4.1.3.1(b) Emerging. 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 for one-time password systems:

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

6.4.1.3.2 Authentication Servers

This section provides mandated and emerging standards for Authentication Servers.

6.4.1.3.2(a) Mandated. Authentication servers are servers designed using security measures to establish the validity of a transmission, message or originator. This service applies to all instances where Distributed Computing Environment (DCE) 1.1 is used. If DCE 1.1 is not used, see 6.4.1.3.1. If DCE Version 1.1 is used, the following standard is mandated when the security policy or program security profile requires this level of protection:

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

6.4.1.4 Data Labeling

This service addresses the identification of security labels to be used with data. The data to which this service applies is defined in Section 2.5.4.

6.4.1.5 Secure Session

This service provides a secure remote login and other secure network services over a network that does not necessarily provide security services.

6.4.1.5(a) Mandated. No standards are mandated in this section.

6.4.1.5(b) Emerging. 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-13.txt, Secure Shell (SSH) Protocol Architecture, 23 September 2002.

6.4.1.6 Secure File Transfer

This service provides security requirements associated with the transfer of binary and text files between user systems.

6.4.1.6(a) Mandated. No standards are mandated in this section.

6.4.1.6(b) Emerging. IETF RFC 2228, File Transfer Protocol, October 1997, defines extensions to the File Transfer Protocol (FTP) standard (STD9/RFC 959). These extensions provide strong authentication, integrity, and confidentiality on both the control and data channels. IETF RFC 2228 also introduces new optional commands, replies, and file transfer encodings. The following standard is emerging:

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

6.4.1.7 Secure Distributed Computing

This service identifies the standards to be used when security is required in association with distributed computing. Distributed computing allows various tasks, operations, and information transfers to occur on multiple physically or logically dispersed computer platforms.

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.

6.4.1.7(a) Mandated. No standards are mandated in this section.

6.4.1.7(b) Emerging. The following standards are emerging:

– OMG document formal/01-03-08, Security Services Specification, Version 1.7, March 2001.

6.4.1.8 Operating System Security

This service defines the protection profile, and the levels of such protection profiles, to be applied to the operating system. A protection profile is defined in the Common Criteria (see 6.8.1).

6.4.1.8(a) Mandated. No standards are mandated in this section.

6.4.1.8(b) Emerging. For the application platform entity, the following protection profiles are emerging for the acquisition of security functionality for operating systems consistent with the required level of trust.

For basic robustness:

– Controlled Access Protection Profile, Version 1.d, NSA, 8 October 1999.

For medium robustness:

– Labeled Security Protection Profile, Version 1.b, NSA, 8 October 1999.

6.4.2 Cryptographic Security Services

To support interoperability using encrypted messages, products must share a common communications protocol. This protocol must include common cryptographic message syntax, common cryptographic algorithms and common modes of operation (e.g., cipher block chaining). The mechanisms to provide the required security services are as follows.

6.4.2.1 Encryption Algorithms

Encryption algorithms are a set of mathematical rules for rendering information unintelligible by effecting a series of transformation to be the normal representation of the information through the use of variable elements controlled by a key.

6.4.2.1(a) Mandated. The following standard is mandated when the security policy or the program security profile requires this level of protection, and FORTEZZA applications are in use:

- SKIPJACK and KEA Algorithm Specification, Version 2.0, NIST, 29 May 1998.

For those systems required or desiring to use a cryptographic device to protect privacy act information and other unclassified information not covered by the Warner Amendment to Public Law 100-235, the following standard is mandated:

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

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

– FIPS PUB 197, Advanced Encryption Standard (AES), 26 November 2001.

6.4.2.2 Hash Algorithms

Key-Hashing for Message Authentication (HMAC) is a mechanism for message authentication using cryptographic hash functions, and can be used with any iterative hash function in combination with a shared secret key. The cryptographic strength of HMAC depends on the properties of the underlying hash function. Note that HMAC prevents “extension” attacks that iterative hash functions do not prevent.

6.4.2.2(a) Mandated. The following standard is mandated when the security policy or program security profile requires this level of protection:

- FIPS PUB 180-1, Secure Hash Standard, 17 April 1995.

For computing shared-secret key message authentication codes (MAC), the following is mandated:

- IETF RFC 2104, HMAC: Keyed-Hashing for Message Authentication, February 1997.

6.4.2.3 Signature Algorithms

A signature algorithm is an algorithm developed to assure message source authenticity and integrity. The intent of the signature is to provide a measure of assurance that the person signing the message sent the message that is signed, and that the contents of the message have not been changed.

6.4.2.3(a) Mandated. The following standard is mandated when the security policy or program security profile requires this level of protection:

- FIPS PUB 186-2, Digital Signature Standard (DSS) Digital Signature Algorithm (DSA), 27 January 2000.

6.4.2.4 Cryptographic Tokens

Cryptographic tokens are portable, user controlled, physical devices used to store cryptographic information and possibly perform cryptographic functions. A cryptographic token is used to validate and end entity's identification and bind that identity to its public key.

6.4.2.5 Cryptographic APIs

Cryptographic algorithms are the source code formats and procedures through which an application program accesses cryptographic hash algorithms, digital signature algorithms, and key management algorithms.

6.4.2.5(a) Mandated. 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.

6.4.2.5(b) Emerging. The Generic Security Service-Application Program Interface (GSS-API), as defined in IETF RFC 1508, September 1993, 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. IETF RFC 1508 defines GSS-API services and primitives at a level independent of an underlying mechanism and programming language environment. IETF RFC 2743, GSS-API, Version 2.0, J. Linn, Update 1, January 2000, revises IETF 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, 1 January 2000.

The IETF Draft, Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API), C. Adams, 25 March 1997, http://rfc2479.x42.com, extends the GSS-API (IETF RFC 1508) for non-session protocols and applications requiring protection of a generic data unit (such as a file or message) 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.

6.4.2.6 Cryptographic Key Algorithms

Cryptographic key algorithms are mathematical expressions that develop a sequence of symbols that controls the operation of encipherment and decipherment.

6.4.2.6(a) Mandated. The following KEA Exchange Algorithm is mandated:

- Skipjack and KEA Algorithm Specifications, Version 2.0, NIST, 29 May 1998.

6.4.2.7 Cryptographic Modules

This section provides mandated standards for Cryptographic Modules. Also see the JTA's cryptologic subdomain.

6.4.2.7(a) Mandated. The following standard is mandated when the security policy or program security profile requires this level of protection:

- FIPS PUB 140-2, Security Requirements for Cryptographic Modules, 25 May 2001.

6.5 Enclave Boundary

This section defines standards for devices to support effective control and monitoring of the data flows into and out of a physical or logical enclave. This provides boundary defenses for those components within the enclave that cannot defend themselves due to technical or configuration problems.

6.5.1 Firewall

A firewall is a system or combination of systems that enforces a boundary between two or more networks. The purpose of a firewall is to protect internal information systems from external attacks. Firewalls address the requirement for authorized LAN users and administrators, as well as individual workstations or personal computer users, to safely access and be accessed by untrusted and potentially hostile external network connections.

6.5.1(a) Mandated. No standards are mandated in this section.

6.5.1(b) Emerging. The following emerging standards will apply to Firewall devices in Basic Robustness environments:

- U.S. Government Traffic Filter Firewall Protection Profile for Low Risk Environments, Version 1.1, April 1999.
- U.S. Department of Defense Application-level Firewall Protection Profile for Basic Robustness Environments, Version 1.0, June 2000.

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

- U.S. Department of Defense Traffic Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.4, 1 May 2000.
- U.S. Department of Defense Application-level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, 28 June 2000.

For firewall standards, see http://csrc.nist.gov/cc/pp.

6.5.2 Guards

Guards enable users to exchange data between private and public networks, which is normally prohibited due to information confidentiality. Guard technology can bridge across security boundaries by providing some of the interconnectivity required between systems operating at differing security levels.

6.5.3 Remote Access

Remote access is the ability for a user to log in to a server from a remote location. For security, the user must first be authenticated before gaining access.

6.5.4 Malicious Code

This service provides protection against malicious code (for example, viruses, worms, and logic bombs).

6.6 Network and Infrastructure

This section addresses the standards for secure networks at the network layer protocol and below, as well as its basic infrastructure (e.g., naming services). They include security standards for communication protocols (at the network layer, link layer, and physical layer as well as related naming services) and for Virtual Private Networks (VPNs) for secure communications using potentially insecure networks. Systems processing classified information must use Type 1 NSA-approved encryption products to provide both confidentiality and integrity security services within the network.

6.6.1 Network Layer

The Network layer is layer 3 of the Open Systems Interconnect (OSI) 7 Layer Reference Model.

6.6.1(a) Mandated. The Internet Protocol Security (IPsec) protocol suite provides privacy and authentication services at the IP (network) layer. Several documents are used to describe the IPsec protocol suite. The interrelationships and organization of the various documents are discussed in IETF RFC 2411, the “IP Security Document Roadmap”. For IPv4 and IPv6, when IP security (network layer) services are required, the following standards are mandated:

- IETF RFC 2401, Security Architecture for the Internet Protocol, November 1998.
- IETF RFC 2402, IP Authentication Header, November 1998.

- IETF RFC 2404, The Use of HMAC-SHA-1-96 within ESP and AH, November 1998.
- IETF RFC 2406, IP Encapsulating Security Payload (ESP), November 1998.
- IETF RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP, November 1998.
- IETF RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP), November 1998.
- IETF RFC 2409, The Internet Key Exchange (IKE), November 1998.

6.6.1(b) Emerging. The following standard is emerging for Virtual Private Networks (VPN) devices operating at the Network Layer:

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

6.6.2 Link Layer

The (data) link layer is layer 2 of the Open Systems Interconnect (OSI) 7 Layer Reference Model where a point-to-point communication channel connecting two subnetwork relays is established.

6.6.2(a) Mandated. No standards are mandated in this section.

6.6.2(b) Emerging. The Point-to-Point Protocol (PPP) Triple-DES Encryption Protocol (3DESE) is a complement to FIPS PUB 46-3. The following standard is emerging:

– IETF RFC 2420, The PPP Triple-DES Encryption Protocol (3DESE), September 1998.

The ATM Forum has also established requirements and control implementation for security of ATM networks. The following standards are emerging for secure ATM networks:

– ATM Forum, af-sec-0096.000, ATM Security Framework Version 1.0, February 1998.
– ATM Forum, af-sec-0100.002, ATM Security Specification Version 1.1, March 2001.

6.6.3 Physical Layer

The physical layer, Layer 1 of the OSI 7 Layer Reference Model, provides the mechanical, electrical, functional, and procedural means to activate, maintain, and deactivate physical connections for bit transmission between data link entities.

6.6.3(a) Mandated. No standards are mandated in this section.

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

– IEEE 802.10-1998, IEEE Standards for Local and Metropolitan Area Networks: Standard for Interoperable LAN/MAN Security (SILS), 17 September 1998.
– IEEE 802.10a-1999, IEEE Standards for Local and Metropolitan Area Networks: Supplement to Standard for Interoperable LAN/MAN Security (SILS) – Security Architecture Framework (Clause 1), 22 March 1999.
– IEEE 802.10c-1998, IEEE Standards Interoperable LAN/MAN Security (SILS) – Key Management (Clause 3), 17 April 1998.

6.6.4 Naming Service

A naming service: (1) is used to construct large, enterprise-wide naming graphs where naming contexts model “Directories” or “folders” and other names identify “document” or “file” types of objects; and (2) is used as the backbone of an enterprise-wide filing system.

6.6.4(a) Mandated. No standards are mandated in this section.

6.6.4(b) Emerging. 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.

The DNS is also a critical operational part of a TCP/IP-based infrastructure, and authentication and integrity mechanisms are often necessary to protect it. In cases where DNS authentication is needed and a shared secret key approach is appropriate, in particular in zone transfers between authoritative servers, the following standard is emerging:

– IETF RFC 2845, Secret Key Transaction Authentication for DNS (TSIG), May 2000.

In other cases where DNS authentication and integrity protection is needed, the DNSSEC standards are emerging. DNSSEC defines extensions to DNS to support security requirements, data integrity and authentication, through cryptographic digital signatures. However, DNSSEC as defined by IETF RFC 2535 has been shown to have serious problems, so IETF RFC 2535 is being updated. Once IETF RFC 2535 is updated to repair these problems, it is expected to be mandated. The following standard is emerging for DNS security:

– IETF RFC 2535, DNS Security Extensions, March 1999.

6.6.5 Directory Service

A directory service provides names, locations, and other information about people and organizations. In a network, this directory information may be used for e-mail addressing, user authentication (e.g., logins and passwords), or network security (e.g., user access rights).

6.7 Supporting Infrastructures

This section addresses standards for service areas providing overall security support. It includes standards for public-key infrastructure (PKI) and intrusion detection systems (IDS).

6.7.1 Public-Key Infrastructure (PKI)

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, 23 June 1999, plus additional categories not mentioned in the Roadmap.

6.7.1.1 PKI Certificates

This section provides mandated and emerging standards for PKI Certificates.

6.7.1.1(a) Mandated. 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 Recommendation X.509 (2000)/ISO/IEC 9594-8:2001, Information Technology – Open Systems Interconnection – The Directory: Public Key and Attribute Certificate Frameworks, 2001, with Technical Corrigendum 1:2002, and Technical Corrigendum 2:2002.

6.7.1.1(b) Emerging. 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:

- IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999, as profiled by TWG-98-07.
- TWG-98-07, DoD Certificate Policy, Version 6, 31 May 2002.

6.7.1.2 PKI Operational Protocol and Exchange Formats

The following paragraphs address standards for PKI Operational Protocol and exchange formats.

6.7.1.2(a) Mandated. No standards are mandated in this section.

6.7.1.2(b) Emerging. Operational protocols deliver certificates and certificate revocation lists (CRLs) to certificate-using systems. The medium-assurance pilot uses IETF RFC 2559, a profile of IETF 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. IETF 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, v1.0: Personal Information Exchange Syntax Standard, RSA, 24 June 1999.
– RSA Laboratories Public Key Cryptography Standard (PKCS) #15, v1.1: Cryptographic Token Information Format Standard, RSA, 6 June 2000.

6.7.1.3 PKI Management Protocols

The following paragraphs address standards for PKI Management Protocols.

6.7.1.3(a) Mandated. No standards are mandated in this section.

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

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

Although IETF 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.

6.7.1.4 PKI API

The following paragraphs address standards for PKI API.

6.7.1.4(a) Mandated. No standards are mandated in this section.

6.7.1.4(b) Emerging. 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, v2.10: Cryptographic Token Interface Standard, December 1999.

6.7.1.5 PKI Cryptography

The following paragraphs address standards for PKI Cryptography.

6.7.1.5(a) Mandated. No standards are mandated in this section.

6.7.1.5(b) Emerging. The following standards are emerging:

– IETF RFC 2437, PKCS #1: RSA Cryptography Specifications Version 2.0, October 1998.
– FIPS PUB 140-2, Security Requirements for Cryptographic Modules, 25 May 2001.

For systems using encryption to protect privacy act information and other unclassified, non-Warner Act exempt information, the triple-DES algorithm in the following standard is emerging:

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

The following standard is emerging for PKI Class 3 implementations:

– FIPS PUB 180-1, Secure Hash Algorithm, 17 April 1995.

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

– FIPS PUB 197, Advanced Encryption Standard (AES), NIST, 26 November 2001.

6.7.2 Key Management Infrastructure

The following paragraphs address standards for Key Management Infrastructure.

6.7.2(a) Mandated. The following standard is mandated when the security policy or program security profile requires this level of protection:

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

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

6.7.3 Intrusion Detection Systems (IDS)

The following paragraphs address standards for Intrusion Detection Systems.

6.7.3.1 Intrusion Detection Devices

The following paragraphs address standards for Intrusion Detection Devices.

6.7.3.1(a) Mandated. No standards are mandated in this section.

6.7.3.1(b) Emerging. The following standards for Intrusion Detection devices are emerging:

– Intrusion Detection System Analyzer Protection Profile, Draft 3, IATF, 15 September 2000.

- Intrusion Detection System Sensor Protection Profile, Draft 3, IATF, 15 September 2000.
- Intrusion Detection System Scanner Protection Profile, Draft 3, IATF, 15 September 2000.

For intrusion detection standards, see http://csrc.nist.gov/cc/pp.

6.7.3.2 Intrusion Detection Communications Protocol

The Intrusion Detection Exchange Protocol (IDXP) is an application-level protocol for exchanging data between intrusion detection entities. IDXP supports mutual-authentication, integrity, and confidentiality over a connection-oriented protocol. The protocol provides for the exchange of Intrusion Detection Message Exchange Format (IDMEF) messages, unstructured text, and binary data.

6.7.3.2(a) Mandated. There are no mandated standards in this section.

6.7.3.2(b) Emerging. The following Intrusion Detection Communications Protocol standard is emerging:

- draft-ietf-idwg-beep-idxp-04.txt, Intrusion Detection Exchange Protocol (IDXP), 11 September 2001.

6.7.3.3 Intrusion Detection Message Exchange Format

The Intrusion Detection Message Exchange Format (IDMEF) is intended to be a standard data format that automated intrusion detection systems can use to report alerts about events that they deem suspicious. The development of this standard format will enable interoperability among commercial, open source, and research systems, allowing users to implement heterogeneous IDS across their network infrastructures.

6.7.3.3(a) Mandated. There are no mandated standards in this section.

6.7.3.3(b) Emerging. The following Intrusion Detection Message Exchange Format standard is emerging:

- draft-ietf-idwg-idmef-xml-06.txt, Data Model and Extensible Markup Language (XML) Document Type Definition, 18 September 2001.

6.8 Evaluation Criteria

This section includes standards used to design, develop, and evaluate security components and systems.

6.8.1 Common Criteria

The Evaluation Criteria for Information Technology Security (a.k.a., 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 Common Criteria Implementation Board (CCIB), working in cooperation with the ISO, has produced a technically equivalent document entitled “The Common Criteria for Information Technology Security Evaluation (CC), Version 2.1 (CC 2.1)”. The CCIB has fully aligned CC 2.1 with ISO/IEC 15408:1999. Therefore, any security specifications written using CC 2.1, and IT products/systems shown to be compliant with

CC 2.1, are considered to be ISO/IEC 15408:1999 compliant. More information on the CC Project can be found on the NIST web site at http://csrc.ncsl.nist.gov/cc/ccv20/ccv2list.htm.

No emerging standards are in this section. However, NSA has initiated a Protection Profile effort to provide recommended guidance to Department of Defense and U.S. Government entities in the acquisition of IT security products. The objective is to provide a recommended and, eventually, DoD-wide uniform set of specifications for these security devices. This will provide a focus for the vendors, who will be motivated to produce products that satisfy DoD's requirements as expressed in these protection profiles. NSA customers must validate that these profiles accurately express DoD requirements. Vendor input is needed to ensure that these profiles represent security requirements realistic for a commercial market product. Note: See profile list at the Information Assurance Technical Framework Forum Web site (www.iatf.net).

6.8.1(a) Mandated. 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 information technology security (parts 1 through 3), 1 December 1999.

Page intentionally left blank.

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

C4ISR.1 Domain Description

This Domain (C4ISR) represents common elements within a family of related systems focusing on the functional, behavioral, and operational requirements needed to extend the JTA concept to this specific domain and its associated subdomains.

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 Core Figure 1-2.

C4ISR.2 Purpose and Scope

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.3 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 subdomains to better gauge which domain is applicable.

C4ISR.4 Information Processing Standards

This section is intended to identify the data format and information processing standards required by C4ISR systems needed in addition to the JTA Core standards to develop integrated interoperable systems.

C4ISR.4.1 Common Ground Moving Target Indicator Data Format

The Common Ground Moving Target Indicator (CGMTI) Data Format is a U.S./NATO data format used to disseminate imagery from airborne and spaceborne sensor platforms.

C4ISR.4.1(a) Mandated. No standards are mandated in this service area of the C4ISR Domain.

C4ISR.4.1(b) Emerging. The Common Ground Moving Target Indicator (CGMTI) Format is emerging as a de facto U.S./NATO data format for the dissemination of GMTI imagery from airborne and spaceborne CGMTI 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, and subsequent fusion and display of CGMTI data. Details of the Working Group are available at the CGMTI web site http://www.rl.af.mil/programs/cgmti/. The following document is identified as an emerging standard for systems that disseminate CGMTI data:

– Common Ground Moving Target Indicator (CGMTI) Format Document, DRAFT Version 1.01d5a, 27 April 2001.

C4ISR.5 Information Transfer Standards

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.5.1 Transmission Media

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

C4ISR.5.1.1 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.5.1.1.1 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 Security Equipment Integration Working Group (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.

C4ISR.5.1.1.1(a) Mandated. The following standard is mandated for use in UMS systems:

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

C4ISR.5.1.2 Network 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.

C4ISR.5.1.2(a) Mandated. No standards are mandated in this service area of the C4ISR Domain.

C4ISR.5.1.2(b) Emerging. The following standard is emerging:

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

C4ISR.5.1.3 Platform to Ground Station Direct Data Transfer Interface

Mission Tape Recorders are used to capture the raw and preprocessed data on the platform. The data is then transferred to a ground station via the recorded tape in a standard format. The two high rate digital recording standards are ANSI ID-1 and DCRSi.

C4ISR.5.1.3(a) Mandated. There are no mandated standards in this service area of the C4ISR Domain.

C4ISR.5.1.3(b) Emerging. The Air Group IV working group, under the NATO Air Force Armaments Group (NAFAG) has developed the NATO Advanced Data Storage Interface (NADSI) NATO Standardization Agreement (STANAG). This STANAG defines the standard interface for the interoperability and transfer/exchange of data among Intelligence, Surveillance, and Reconnaissance (ISR) platforms and NATO ground stations by direct physical connection to data storage subsystems. This STANAG will be promulgated by the Chairman of the Military Agency for Standardization (MAS).

The NADSI STANAG 4575 defines a multiple layer protocol for the lower levels of the interface channel as defined in the International Standards Organization – Open Systems Interconnection model (ISO/IEC 7498-1). Additionally, this STANAG is part of the NATO Imagery Interoperability Architecture (NIIA), which includes the data format standards STANAG 7023 for primary and STANAG 4545 for secondary imagery.

The STANAG 4575 interface is to be incorporated into all removable data storage elements in ISR Advanced (i.e., non-tape) Data Storage systems to allow the direct download of ISR data to ground stations via a direct connection. The following document is identified as an emerging standard for the transfer of stored ISR data:

– NATO Advanced Data Storage Interface, (NADSI) STANAG 4575, Edition 1, Ratification Draft.

C4ISR.5.2 Payload-Platform Interface

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 1.9 of the JTA Core, and as interpreted by individual Service/Agency JTA Implementation Plans, should be used to determine mandate applicability. 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 standards apply only to airborne reconnaissance systems.

C4ISR.5.2.1 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.5.2.1.1 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 the 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.

C4ISR.5.2.1.1(a) Mandated. 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.5.2.1.2 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 ISO/IEC 13213:1994 Information technology – Microprocessor systems – Control and Status Registers (CSR) Architecture for microcomputer buses.

C4ISR.5.2.1.2(a) Mandated. The following standard is mandated for serial bus communications internal to airborne reconnaissance platforms where FireWire is used:

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

C4ISR.5.2.2 Vehicle/Sensor Telemetry

Commands to various Signal Intelligence (SIGINT), Imagery Intelligence (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.

Inter-Range Instrumentation Group (IRIG) Standard 106-01 is the primary telemetry standard used throughout the world by both government and industry. IRIG Standard 106-01 covers all aspects of frequency division multiplexing and pulse code modulation (PCM) telemetry, including transmitters, receivers, and tape recorders. This is one of many comprehensive standards prepared by the Telemetry Group of the Range Commanders Council (RCC) to foster the compatibility of telemetry transmitting, receiving, and signal processing equipment at member ranges.

C4ISR.5.2.2(a) Mandated. The following chapters of the IRIG Telemetry standard are mandated for airborne reconnaissance systems:

- IRIG 106-01, Part 1, Telemetry Standards, February 2001: Chapter 4, Pulse Code Modulation Standard, and Chapter 8, MIL-STD-1553 Acquisition Formatting Standard.

C4ISR.5.3 Nuclear Command and Control Information Transfer

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

C4ISR.5.3(a) Mandated. For radio subsystems operating in the low frequency/very low frequency (LF/VLF) frequency bands, the following standards specify the special modes used by Air Force and Navy forces in support of the United States Strategic Command (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.6 Information Modeling, Metadata, and Information Exchange Standards

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.6.1 Information Exchange Standards

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

C4ISR.6.1.1 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 Assistant Secretary of Defense (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.

C4ISR.6.1.1(a) Mandated. 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.6.1.2 Nuclear Command and Control Information Exchange

The following paragraphs address standards for Nuclear Command and Control information exchange.

C4ISR.6.1.2(a) Mandated. 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.6.2 Sensor Link Protocol (SLP) Message Set

SLP was developed for use as a common interface between electro-optical sensor systems and a diverse set of host computer systems. SLP allows implementers the flexibility to select from a number of open protocol standards (e.g., RS-232/485, FireWire or Universal Serial Bus (USB)) by decoupling the message set from the underlying protocol. The SLP message set can be used to implement a common digital data exchange mechanism that offers full remote operation and control of sensors by a host computing device in both a point-to-point and networked environment.

C4ISR.6.2(a) Mandated. There are no mandated standards for this section.

C4ISR.6.2(b) Emerging. The SLP message set is defined in the following emerging standard:

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

C4ISR.7 Human-Computer Interface Standards

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.7.1 Nuclear Command and Control HCI

The HCI standards associated with Nuclear Command and Control address all the usual HCI issues with an emphasis on system safety considerations.

C4ISR.7.1(a) Mandated. No standards are mandated in this service area of the C4ISR Domain.

C4ISR.7.1(b) Emerging. This section contains emerging HCI standards applicable to Nuclear C2 systems.

Standardized HCI for all EAM injection processors will reduce training requirements. The following standard is emerging:

– HMI DIRECT ICD, “Human-Machine Interface (HMI) Design Criteria,” CDRL 135C- 03, V3.0, 5 March 1999.

C4ISR.8 Information Security Standards

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.CRY: Cryptologic Subdomain

C4ISR.CRY.1 Subdomain Description

The Cryptologic Subdomain provides the high-level foundation and guidance for interoperability and seamless flow of information between and among all Cryptologic Partners and systems and the associated Military components in a collaborative and secure environment. It promotes interoperability with other components of the U.S. Intelligence (IC) and foreign Cryptologic partners.

C4ISR.CRY.2 Purpose and Scope

The Cryptologic Subdomain is an extension of the JTA and is based on certain technical foundations for migrating Cryptologic systems within the United States (USCS) toward a common Unified Cryptologic System (UCS) architecture as directed by the Director, NSA (DIRNSA) and the Director, Central Intelligence (DCI). The migration will be accomplished through the use of mandated standards in the JTA, the Unified Cryptologic Architecture—Technical Architecture (UCA-TA) (January 1998), the Maritime Cryptologic Architecture (MCA) Technical View (TV) (version 2.1, July 2001), the NRO Integrated Overhead SIGINT Architecture (IOSA) (December 2001) and the joint Airborne SIGINT Architecture (JASA) (version 1.0, July 2000). Additional architectures and their technical views are under development by other Cryptologic Partners.

C4ISR.CRY.3 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. For the purpose of this Subdomain, a Cryptologic system is defined as any system that collects, processes, analyzed, disseminates and/or manages Signal Intelligence (SIGINT) and/or performs SIGINT related information assurance services.

C4ISR.CRY.4 Background

Faced with the challenges of keeping pace with changing intelligence requirements, budgetary uncertainty and technological revolutions, the DIRNSA, under the auspices of the Deputy Secretary of Defense and the DCI, 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 the study was the introduction of the UCA Operational, Systems and Technical Architectures. Parallel efforts in the Cryptologic community led to the development of subordinate architecture views. Some of the subordinate architectures are complementary to the JTA and will be used in conjunction with the JTA Core and JTA C4ISR Domain by all members of the Cryptologic community.

The current status of the Cryptologic architectures and technical views is this: The Cryptologic community is coordinating and vetting the mandatory C4ISR architecture views to create a community approved UCA version 1.0 by the end of FY02. Additional views will be developed in FY03. The C4ISR TV-1 will likely be delivered in FY03, and will include a set of standards common to the Cryptologic community. Configuration management will begin as the C4ISR products are finished and approved by the community. As the community completes an approved common set of C4ISR views, the Cryptologic Community Partner architectures will be brought into concordance with the approved UCA, although as necessary they may contain more detail in appropriate areas of interest, including additional standards in the technical view.

C4ISR.CRY.5 Subdomain-Specific Services and Interfaces

The following section presents mandatory and emerging standards for Cryptologic Subdomain-specific services and interfaces.

C4ISR.CRY.5.1 Small-Scale Special Purpose Devices

Some cryptologic processing is performed using Small-Scale 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.5.1(a) Mandated. A SPD consists of one or more special-purpose boards (may be Government-developed) hosted by a 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 Peripheral Component Interconnect (PCI) cards shall comply with the following mandated standard:

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

The PC Card standard is a Personal Computer Memory Card International Association (PCMCIA) standards body and trade association standard. Cryptologic systems using PCMCIA cards shall comply with the following mandated standard:

- PC Card Standard, Release 7.0, March 1997.

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 Virtual Memory Extended (VME) backplanes and circuit cards shall comply with the following mandated standard:

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

Cryptologic systems using VMEbus Extensions for Instrumentation (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.5.1(b) Emerging. CompactPCI (cPCI) is a competing bus standard that uses the same form factor as VME and the protocols of the much smaller Peripheral Component Interconnect (PCI) standard, which is emerging for backplanes and circuit cards.

– CompactPCI (cPCI), Version 1.0, 1996.

C4ISR.CRY.5.2 Collaborative Data Sharing

The following sections address mandatory and emerging cryptologic standards for transfer of collaborative data.

C4ISR.CRY.5.2(a) Mandated. There are no mandated standards in this section.

C4ISR.CRY.5.2(b) Emerging. The Common Cryptologic Data Model (CCDM) and Common Cryptologic Data Format (CCDF) Release 2.3, 6 July 2001, represent a new family of metadata/formats (implemented in XML) for the exchange of Cryptologic data. In limited use today, CCDM/CCDF was approved by NSA/CSS Enterprise Standards Program – Standards Board as an NSA/CSS standard in January 2001 and is emerging as the Cryptologic community standard for collaborative data sharing functions:

– The Common Cryptologic Data Model (CCDM) and Common Cryptologic Data Format (CCDF), Release 2.3, 6 July 2001.

Page intentionally left blank.

C4ISR.SR: Space Reconnaissance Subdomain

C4ISR.SR.1 Subdomain Introduction

The purpose of the Space Reconnaissance (SR) Subdomain (SRS) of the C4ISR Domain is to identify the minimum set of technical standards for interfaces among SR Information Technology (IT) systems, and between those systems and other Department of Defense (DoD) systems. The standards contained here are in addition to those applicable standards found in the C4ISR Domain and in the JTA Core.

The scope of the SRS includes space-related functions unique within the JTA. The SRS identifies additional standards that are unique to SR communications and data processing. Standards not unique to SR are contained in the C4ISR Domain or in the JTA Core.

The SRS applies to acquisitions of new and upgraded SR IT systems, as well as advanced technology demonstrations. The standards mandated in the JTA Core, C4ISR Domain, and SRS are all applicable to the external SR IT interfaces.

The SRS is developed and maintained by the SRS Working Group (SRS WG) under the auspices and procedures of the JTA Development Group (JTADG). The SRS WG is chaired by the National Reconnaissance Office (NRO).

C4ISR.SR.2 Information Processing Standards

This section identifies standards for interoperability among SR IT and other DoD Intelligence, Surveillance, & Reconnaissance (ISR) systems in addition to the standards cited in the JTA Core Section 2 and C4ISR Domain C4ISR.4.

C4ISR.SR.2.1 Hardware Product Data Interchange

Hardware product data interchange defines the service for transmitting computer aided data that describes parts, geometry, arrangement, construction, connectivity, manufacturing, assembly, integration, maintenance, or operation of component, subsystems or systems. This product data may be used in Computer Aided Design (CAD), Computer Aided Manufacturing (CAM), or Computer Aided Engineering (CAE), which are collectively referred to as CAx.

C4ISR.SR.2.1(a) Mandated. Hardware product data interchange standards are mandated for specific functions. This ANSI/US PRO standard, known as Initial Graphics Exchange Specification (IGES), establishes information structures for the digital representation and exchange of product definition data. It supports exchanging this data among CAD/CAM systems. The following standards are 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.
- MIL-PRF-28000B, Digital Representation for Communications Product Data: IGES Application Subsets and IGES Application Protocols, 30 September 1999.

These standards establish the minimum standards for product data management (PDM) systems that will store and control all data, in any format, related to a design project and what the interchange tools must support.

Effective use of Standard for the Exchange of Product Data Model (STEP) to share product model data for systems requires this companion standard, ISO/IEC 13584, to exchange CAD Part Libraries (PLIP). The PLIP supplies a data model of the supplier part library, supplier identification, and part geometry.

- ISO/IEC 10303-209:2001, Industrial automation systems and integration – Product data representation and exchange – Part 209: Application protocol: Composite and metallic structural analysis and related design.
- ISO/IEC 10303-210:2001, Industrial automation systems and integration – Product data representation and exchange – Part 210: Application protocol: Electronic assembly, interconnection, and packaging design.
- ISO/IEC 10303-224:2001, Industrial automation systems and integration – Product data representation and exchange – Part 224: Application protocol: Mechanical product definition for process planning using machining features.
- 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.

This standard establishes the minimum standards for electronic design and analysis processes required for the Very High Speed Integrated Circuit (VHSIC) Hardware Description Language (VHDL).

- ANSI/IEC 61691-1, Design Automation – Part 1: VHDL Language Reference Manual, 1st edition, 1997.

This standard defines the VHSIC Hardware Description Language. VHDL is a formal notation intended for use in all phases of the creation of electronic systems. Because it is both machine-readable and human-readable, VHDL supports the development, verification, synthesis, and testing of hardware designs; the communication of hardware design data; and the maintenance, modification, and procurement of hardware. Its primary audiences are the implementers of tools supporting the language and the advanced users of the language.

- IEEE 1076-2002, IEEE Standard VHDL Language Reference Manual.

This standard specifies record formats used to describe printed board products with detail sufficient for tooling, manufacturing, and testing requirements. These formats may be used for transmitting information between a printed board designer and a manufacturing facility. The records are also useful when the manufacturing cycle includes computer-aided processed and numerically controlled machines. The information can be used for both manual and digital interpretations. The data may be defined in either English or international standard (SI) units.

- ANSI/IPC-D-350D-1992, Printed Board Description in Digital Form, 17 June 1992.

This standard is a description of the two-dimensional bar code symbology, Code 39, used to identify packages and products including symbol structure, start and stop characters, quiet zones, and check character. It includes necessary additional pass-fail parameters for the symbology required by ANSI X3.182. It can be used to help identify products being shipped and stocked; hence, it is used mainly in Logistics. This standard replaces MIL-STD-1189B.

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

This interface standard establishes the logical structure and formats for the transfer of digital information between organizations or systems exchanging digital forms of technical information. This standard facilitates the development and support of systems throughout their life cycle and the conduct of business by electronic means. The areas addressed by this standard involve the interface with computer technologies that are automating the creation, storage, retrieval, and delivery of hard copy forms of technical manuals and engineering drawings. The standard also addresses electronic product data technology and the packaging of data for electronic commerce. The standard defines a logical file independent exchange of technical information.

- MIL-STD-1840C, Automated Interchange of Technical Information, 26 June 1997.

C4ISR.SR.2.2 Object-Oriented Database Management

This service supports the definition, design, storage, and retrieval of data elements managed by commercial or custom-developed object-oriented database management systems.

C4ISR.SR.2.2(a) Mandated. Object-oriented databases should conform to the syntax and requirements for The Object Data Standard, which is defined by the Object Data Management Group (ODMG). The following standard is mandated:

- The Object Data Standard: ODMG 3.0, Morgan Kaufman Publishers, 2000, ISBN 1-55860-647-5.

C4ISR.SR.3 Information Transfer Standards

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 Intelligence, Surveillance, & Reconnaissance (ISR) systems in addition to the standards cited in the JTA Core Section 3 and C4ISR Domain C4ISR.5.

C4ISR.SR.3.1 Synchronous Optical Network Transmission Facilities

In addition to standards contained in 3.7.4 of the JTA Core, the following standard applies to SR communication systems that use Synchronous Optical Network (SONET).

C4ISR.SR.3.1(a) Mandated. The following standard is mandated:

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

C4ISR.SR.4 Information Modeling, Metadata, and Information Exchange Standards

The U.S. Electronic Intelligence (ELINT) establishes, defines, and explains the reporting format and promulgation of data formats and codes for reducing ELINT intercept data to processing media (magnetic data tape, punch card, or punched paper tape).

C4ISR.SR.4(a) Mandated. The following standard is mandated:

- Standard ELINT Data Systems Codes and Formats (SEDSCAF) Manual, October 1991.

Page intentionally left blank.

CS: Combat Support Domain

CS.1 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 1-2, the domain has four subdomains: Automatic Test Systems (CS.ATS), Defense Transportation System (CS.DTS), Human Resources (CS.HR), and Medical (CS.MED). This domain uses the Technical Reference Model (TRM) cited in 1.8 of the JTA as its framework. Combat Support Application Platform Entity service areas are addressed in CS.2 as additions to the JTA Core. Additional Application Software Entity service areas required to support Combat Support Domain systems are addressed in CS.5.2 as domain-specific service areas.

CS.2 Purpose and Scope

The Combat Support 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 Domain are: 1) to improve applications interoperability, promote improved business practices, and reduce operations costs within the Combat Support Domain, and 2) to improve interoperability and increase combat support information access with C4ISR systems. The Combat Support Domain embraces the principles established in the JTA Core. Only those paragraphs from the Core that have additions are included in this domain.

CS.3 Applicability

The Combat Support Domain identifies standards applicable to DoD Combat Support elements, e.g., Logistics, Electronic Data Interchange (EDI), Continuous Acquisition and Life-Cycle Support (CALS), Medical, and Transportation.

CS.4 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.5 Core-Related Information Technology Categories

In addition to the standards found in the JTA Core, the Combat Support Domain includes additional standards in the following document and data interchange, and information exchange service areas.

CS.5.1 Document Interchange

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).

CS.5.1(a) Mandated. 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.5.2 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.

CS.5.2(a) Mandated. 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.5.3 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.

CS.5.3(a) Mandated. 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/IPC-D-350D, Printed Board Description in Digital Form, 17 June 1992.
- ANSI/IEEE 1076:2002, IEEE Standard VHDL Language Reference Manual, 21 March 2002.

- 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.5 for two-dimensional standard.) The following standard is mandated:

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

The U.S. Navy is employing several parts of the standard for the exchange of product model data (ISO 10303). NAVSEA 9040.3, Development, Maintenance, and Exchange of Product Model Data by Ship and System Programs dated 04 March 1998, describes how to use ISO 10303. The following standards are mandated for use in ship building:

- 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, with Technical Corrigendum 1:1999.
- 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 10303-21:2002, 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 10303-41:2000, Industrial automation systems and integration – Product data representation and exchange – Part 41: Integrated generic resources: Fundamentals of product description and support, with Technical Corrigendum 1:1999.
- ISO 10303-42:2000, Industrial automation systems and integration – Product data representation and exchange – Part 42: Integrated generic resources: Geometric and topological representation, with Technical Corrigendum 1:2001 and Corrigendum 3:2001.
- ISO 10303-43:2000, Industrial automation systems and integration – Product data representation and exchange – Part 43: Integrated generic resources: Representation structures, with Technical Corrigendum 1:1999, and Technical Corrigendum 2:2000.
- ISO 10303-44:2000, 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, with Technical Corrigendum 1:1999.
- ISO 10303-105:1996, Industrial automation systems and integration – Product data representation and exchange – Part 105: Integrated application resources: Kinematics, with Technical Corrigendum 1:2000 and Technical Corrigendum 2:2000.
- 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 10303-224:2001, Industrial automation systems and integration – Product data representation and exchange – Part 224: Application protocol: Mechanical product definition for process planning using machining features.

CS.5.3(b) Emerging. The following standards are emerging for use in building a ship:

- ISO 10303-203:1994, Industrial automation systems and integration – Product data representation and exchange – Part 203: Application protocol: Configuration controlled design, with Amendment 1:2000.
- ISO/DIS 10303-204:2002, Industrial automation systems and integration – Product data representation and exchange – Part 204: Application Protocol: Mechanical design using boundary representation.
- ISO 10303-207:1999, Industrial automation systems and integration – Product data representation and exchange – Part 207: Application Protocol: Sheet metal die planning and design with Technical Corrigendum 1:2001.
- ISO 10303-209:2001, Industrial automation systems and integration – Product data representation and exchange – Part 209: Application Protocol: Composite and metallic structural analysis and related design.
- ISO 10303-210:2001, Industrial automation systems and integration – Product data representation and exchange – Part 210: Application Protocol: Electronic assembly, interconnection, and packaging design.
- ISO 10303-214:2001, Industrial automation systems and integration – Product data representation and exchange – Part 214: Application Protocol: Core data for automotive mechanical design processes.
- ISO/CD 10303-215, Industrial automation systems and integration – Product data representation and exchange Part: 215 Application Protocol: Ship Arrangements. 13 November 2001.
- ISO/CD 10303-218, Industrial automation systems and integration – Product data representation and exchange Part: 218 Application Protocol: Ship Structures, 28 August 2001.

- ISO 10303-225:1999, Industrial automation systems and integration – Product data representation and exchange – Part 225: Application Protocol: Building elements using explicit shape representation.

Effective use of Standard for the Exchange of Product Data Model (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 standards are 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.5.4 Electronic Data Interchange

Electronic Data Interchange (EDI) is a 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.

CS.5.4(a) Mandated. The following standard is mandated:

- ANSI ASC X12 Electronic Data Interchange, as profiled by FIPS PUB 161-2, Electronic Data Interchange, 22 May 1996.

CS.5.4(b) Emerging. The following standards are emerging:

- ISO 9735-1:1988, Electronic data interchange for administration, commerce and transport (EDIFACT) – Application level syntax rules (Syntax version number 4) – Part 1: Syntax rules common to all parts.
- ISO 9735-2:1998, Application level syntax rules (Syntax version number: 4) – Part 2: Syntax rules specific to batch EDI.
- ISO 9735-3:1998, Application level syntax rules (Syntax version number: 4) – Part 3: Syntax rules specific to interactive EDI.

- ISO 9735-4:1998, Application level syntax rules (Syntax version number: 4) – Part 4: Syntax and service report message for batch EDI.
- ISO 9735-5:1999, Application level syntax rules (Syntax version number: 4) – Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin).
- ISO 9735-6:1999, Application level syntax rules (Syntax version number: 4) – Part 6: Secure authentication and acknowledgement message (message type – AUTACK).
- ISO 9735-7:1999, Application level syntax rules (Syntax version number: 4) – Part 7: Security rules for batch EDI (confidentiality).
- ISO 9735-8:1998, Application level syntax rules (Syntax version number: 4) – Part 8: Associated data in EDI.
- ISO 9735-9:1999, Application level syntax rules (Syntax version number: 4) – Part 9: Security key and certificate management message (message type – KEYMAN).

CS.5.5 Information Modeling, Metadata, and Information Exchange Standards

This section specifies additional information modeling, metadata, and information exchange standards that pertain to the DoD Combat Support Elements.

CS.5.5.1 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.

CS.5.5.1(a) Mandated. 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.5.6 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.6 Domain-Specific Standards

This section contains additional Application Software Entity service areas required to support Combat Support Domain Systems.

CS.6.1 Electronic Business/Electronic Commerce

The Electronic Business/Electronic Commerce (EB/EC) Section provides standards useful for any DoD effort involved in electronic business operations. DoD needs to take full advantage of the significant process improvement and reengineering opportunity available through the implementation of EB/EC concepts and technology. EB/EC within DoD can support a variety of areas, including Finance, Procurement, Logistics, Personnel, Medical, Transportation, and Acquisition functions.

CS.6.1.1 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. Smart Card standards are essential for interoperability between multivendor cards and readers.

CS.6.1.1(a) Mandated. The following ISO/IEC Series Standards for Smart Cards are mandated:

- ISO/IEC 14443-1:2000, Identification cards – Contactless integrated circuit(s) cards – Proximity integrated circuit(s) cards – Part 1: Physical characteristics.
- ISO/IEC 14443-2:2001, Identification cards – Contactless integrated circuit(s) cards – Proximity integrated circuit(s) cards – Part 2: Radio frequency power and signal interface.
- ISO/IEC 14443-3:2001, Identification cards – Contactless integrated circuit(s) cards – Proximity integrated circuit(s) cards – Part 3: Initialization and anti-collision.
- ISO/IEC 14443-4:2001, Identification cards – Contactless integrated circuit(s) cards – Proximity integrated circuit(s) cards – Part 4: Transmission protocols.
- 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/AM1:1997: Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange, AM1: Impact of secure messages of APDE structures.
- ISO/IEC 7816-5/AM1:1996, Identification cards – Integrated circuit(s) cards with contacts – Part 5: Numbering system and registration procedure for application identifiers, AM1: Proposal for a set of Registered Application provider Identifiers (RIDs).
- ISO/IEC 7816-6:1996/Amd 1:2000, Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements/Amd 1:2000 IC manufacturer registration.
- ISO/IEC 7816-7:1999, Interindustry commands for Structured Card Query Language (SCQL).

CS.6.1.1(b) Emerging. 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 14443 and 15693 specify the standards for various types of contactless Smart Cards. The following Smart Card standards are emerging:

- ISO/IEC 7816-8:1999, Identification cards – Integrated circuit(s) card with contacts – Part 8, Security architecture and related interindustry commands.
- ISO/IEC 7816-9:2000, Identification cards – Integrated circuit(s) card with contacts – Part 9: Enhanced interindustry commands.
- ISO/IEC 7816-10:1999, Identification cards – Integrated circuit(s) card with contacts – Part 10: Electronic signals and answer to reset for synchronous cards.
- ISO/IEC CD 7816-11:2000, Identification cards – Integrated circuit(s) card with contacts – Part 11: Personal verification through biometric methods in integrated circuit cards.
- ISO/IEC CD 7816-15:2000, Identification cards – Integrated circuit(s) card with contacts – Part 15: Cryptographic information application.
- ISO/IEC 15693-1:2000, Identification cards – Contactless integrated circuit(s) – Vicinity cards – Part 1: Physical characteristics.
- ISO/IEC 15693-2:2000, Identification cards – Contactless integrated circuit(s) – Vicinity cards – Part 2: Air interface and initialization, with Technical Corrigendum 1:2001.
- ISO/IEC 15693-3:2001, Identification cards – Contactless integrated circuit(s) – Vicinity cards – Part 3: Anticollision and transmission protocol.

Page intentionally left blank.

CS.ATS: Automatic Test Systems Subdomain

CS.ATS.1 Subdomain Description

An Automatic Test System (ATS) has three major components: Automated Test Equipment (ATE), Test Program Sets (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 (UUTs), 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.

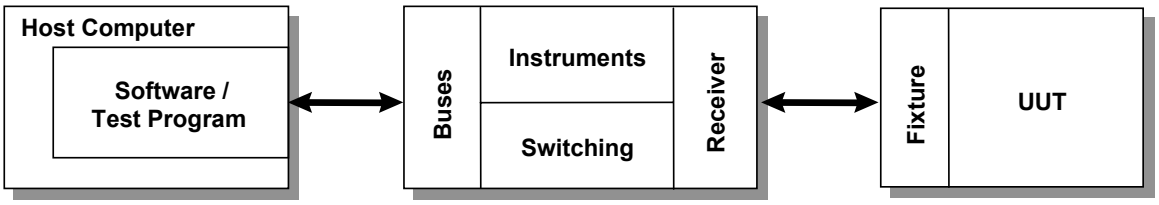


Figure CS.ATS-1: Generic ATS Architecture

CS.ATS.2 Purpose

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 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.3 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.4 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.5 Core-Related Information Technology Categories

The standards in the ATS Subdomain apply in addition to the standards in the Combat Support Domain (standards, interfaces, and service areas) and the JTA Core. These additions are common to the majority of ATSs and support the functional requirements of these systems.

CS.ATS.5.1 Data Interchange Services

This section identifies data interchange services required by the ATS in addition to the standards cited in the JTA Core and Combat Support Domain.

CS.ATS.5.1.1 Instrument Driver API Standards

The Instrument Driver Application Programming Interface (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.

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

CS.ATS.5.1.1(a) Mandated. The following standard is mandated:

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

CS.ATS.5.1.2 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 Logic Automated Simulus and Response (LASAR) Teradyne ASCII Postprocessor (TAP) (LSRTAP), has become a de facto industry standard.

CS.ATS.5.1.2(a) Mandated. The following standard is mandated in this version of the JTA:

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

CS.ATS.5.1.3 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.

CS.ATS.5.1.3(a) Mandated. No standards are mandated for Resource Adapter Interface.

CS.ATS.5.1.3(b) Emerging. The following standards are emerging:

- VPP-3.1, VXI plug&play Systems Alliance: Instrument Drivers Architecture and Design Specification, Revision 4.1, 4 December 1998.
- VPP-3.2, VXI plug&play Systems Alliance: Instrument Driver Functional Body Specification, Revision 5.0, 4 December 1998.
- VPP-3.3, VXI plug&play Systems Alliance: Instrument Driver Interactive Developer Interface Specification, Revision 4.01, 13 December 2001.
- VPP-3.4, VXI plug&play Systems Alliance: Instrument Driver Programmatic Developer Interface Specification, Revision 2.3, 17 March 2000.

Emerging Interchangeable Virtual Instruments (IVI) Foundation Standards are the following:

- IVI-4.1: IviScope Class, Revision 3.0, 4 April 2002.
- IVI-4.2: IviDmm – Digital Multimeter Class, Revision 3.0, 8 March 2002.
- IVI-4.3: IviFGen – Function Generator/Arbitrary Waveform Generator Class, Revision 3.0, 18 December 2002.
- IVI-4.4: IviDCPwr Class Specification, Revision 2.0, April 2002.
- IVI-4.6: IviSwitch Class Specification, Revision 3.0, April 2002.
- IVI-4.7: IviPwrMeter Class Specification, Revision 1.0, April 2002.

- IVI-4.8: IviSpecAn Class Specification, Revision 1.0, April 2002.
- IVI-4.10: IviRFSigGen Class Specification, Revision 1.0, March 2002.

CS.ATS.5.1.4 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.

CS.ATS.5.1.4(a) Mandated. No standards are mandated for diagnostic processing in this section.

CS.ATS.5.1.4(b) Emerging. The following standards are emerging:

- IEEE 1232-2002, 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.5.1.5 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.

CS.ATS.5.1.5(a) Mandated. No standards are mandated in this section.

CS.ATS.5.1.5(b) Emerging. The following standard is emerging:

- IEEE Computer Society Test Technology Technical Committee, Test Requirements Model (TeRM).

CS.ATS.6 Information Transfer Standards

This section identifies information transfer standards required by the ATS in addition to the standards cited in the JTA Core and Combat Support Domain.

CS.ATS.6.1 Instrument Communication Manager Standards

The Instrument Communication Manager (ICM) interface includes bus-specific options for communicating from the instrument driver to a supporting input/output (I/O) library. Until recently, vendors of IEEE-488 and 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, Application Development Environments (ADEs), and test programs from one set of hardware to another. Without a standard ICM interface, vendors cannot provide interoperable or portable instrument drivers because different vendors would use different I/O drivers at the very lowest layer of the software. This forces instrument drivers to be tailored to specific I/O calls for each test station and lowers the likelihood that instrument drivers will be commercially available for each configuration. In addition, standard I/O software allows one to place parameters such as bus addresses and instrument addresses in the instrument driver instead of the test program.

A standard ICM interface enables higher-level software to be interoperable and portable between vendors and across different platforms. This improves the interoperability of test software and the ability to re-host test software from one test system to another.

CS.ATS.6.1(a) Mandated. The following standard is mandated:

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

CS.ATS.6.1(b) Emerging. The following standard is emerging:

– VPP-4.3, VXI plug&play (VPP) Systems Alliance Virtual Instrument Standard Architecture (VISA) Library, Revision 2.2, 17 March 2000.

CS.ATS.6.2 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 Diagnostic Processing Interface Protocol interface by providing information that can supplement diagnostic capabilities.

CS.ATS.6.2(a) Mandated. There are no mandated standards in this section.

CS.ATS.6.2(b) Emerging. The following standards are emerging:

– IEEE P1522, IEEE Testability Standard.
– IEEE 1545-1999, Trial Use Standard for Parametric Data Logging and Format.

CS.ATS.6.3 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.

CS.ATS.6.3(a) Mandated. No standards are mandated in this section.

CS.ATS.6.3(b) Emerging. The following standard is emerging:

– ANSI/EIA 682-1996: EDIF Electronic Design Interchange Format, Version 400, Reference Manual and Information Model.

CS.ATS.6.4 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.

CS.ATS.6.4(a) Mandated. There are no mandated standards in this section.

CS.ATS.6.4(b) Emerging. The following standards are emerging:

– IEEE 1149.1-2001, IEEE Standard Test Access Port and Boundary-Scan Architecture.
– IEEE 1149.4-1999, 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.7 Subdomain-Specific Service Areas

This section addresses Subdomain-Specific Service Areas required by the ATS in addition to the standards cited in the JTA Core and Combat Support Domain.

CS.ATS.7.1 Platform/Environment Services

This section identifies platform/environment services required by the ATS in addition to the standards cited in the JTA Core and Combat Support Domain.

CS.ATS.7.1.1 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.

CS.ATS.7.1.1(a) Mandated. The following standard is mandated:

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

CS.ATS.7.1.1(b) Emerging. The following standard is emerging:

– VPP-2, VXI plug&play (VPP) Systems Alliance System Frameworks Specification, Revision 4.2, 17 March 2000.

CS.ATS.7.1.2 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.

CS.ATS.7.1.2(a) Mandated. There are no mandated standards in this section.

CS.ATS.7.1.2(b) Emerging. The following standard is emerging:

– IEEE P1505, Receiver Fixture Interface (RFI) Standard, Volume RFI-3, Revision 4.0, 16 July 2001.

CS.ATS.7.1.3 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.

CS.ATS.7.1.3(a) Mandated. There are no mandated standards in this section.

CS.ATS.7.1.3(b) Emerging. The following standard is emerging:

– IEEE P1552-1999, Standard Architecture for Test Systems (SATS).

CS.ATS.7.1.4 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.7.1.4.1 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.7.1.4.2 Host Computer Interface

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.7.1.4.3 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.7.1.4.4 Instrument Command Language

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.7.2 Application Development Environments

The Application Development Environments (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 Description

The Defense Transportation System (DTS) 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. Information concerning the 35 DTS systems can be found in the Defense Transportation System Enterprise Architecture, Version 2.0, 11 January 2001, at https://business.transcom.mil/J6/j6a/arch1.html (accessible from .mil domains only).

CS.DTS.2 Purpose and Scope

The Defense Transportation System 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. 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. Military standards are mandated only when suitable commercial standards are not available, are not mature, or do not meet the requirements.

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.3 Applicability

This subdomain applies to all new and existing information systems that make up the Defense Transportation System including upgrades to existing systems.

CS.DTS.4 Background

The DTS was selected for inclusion in the CS Domain based on critical requirements for current, reliable, and accessible visibility of in-transit, scheduled, and actual cargo and personnel movements, through which warfighter resources and operations may be based. Visibility can only be achieved if information from a variety of DoD and non-DoD sources is available. The DTS must be able to readily exchange information with commercial suppliers as well as traditional DoD communities of interest.

CS.DTS.5 Core-Related Information Technology Categories

This section identifies additional standards (mandatory and emerging) unique to the DTS Subdomain of the Combat Support Domain.

CS.DTS.5.1 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. To effectively use PDF-417 requires a method of identifying and parsing the multiple data elements that can now be encoded in a single media. Use of standard data syntax and standard data semantics facilitates the accurate and efficient interpretation of these multiple data elements. ISO 15418 lists the approved data identifiers and their definitions. ISO 15434 describes the message structure and format for encoding data into high capacity automatic data capture (ADC) media. 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.5.1(a) Mandated. The following standards are mandated as profiling documents of PDF-417:

- ISO/IEC 15434:1999, Information technology – Transfer Syntax for High Capacity ADC Media.
- ISO/IEC 15418:1999, Information technology – EAN/UCC Application Identifiers and Fact Data Identifiers and Maintenance.

CS.DTS.5.2 Information Security Standards

This section identifies information security standards required by the DTS in addition to the standards cited in the JTA Core and Combat Support Domain.

CS.DTS.5.2(a) Mandated. There are no additional mandated information security standards in the DTS subdomain.

CS.DTS.5.2(b) Emerging. 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-15.txt, SSH Transport Layer Protocol, 20 September 2002.
- draft-IETF-secsh-userauth-16.txt, SSH Authentication Protocol, 20 September 2002.
- draft-IETF-secsh-connect-16.txt, SSH Connection Protocol, 20 September 2002.

CS.HR: Human Resources Subdomain

CS.HR.1 Subdomain Description

Military personnel and pay functions support Active duty, Guard, and Reserve personnel (and their families) throughout their entire military careers—through periods of peacetime, mobilization and war—and beyond their military service. These functions comprise the military personnel mission area as described in the Defense Information Infrastructure Version 3.1 and support the management, planning, administration, training, and programming of resources for military manpower functions as prescribed by Federal law as well as DoD and Service directives and regulations. Many of the core military personnel and pay functions are performed in the field and are directly related to readiness, force management, and strength accounting. OMB Policy Letter 92-1 defines an inherently governmental function as one involving an exercise of the Government's discretionary authority in choosing among courses of action. Virtually all of the underlying military personnel management functional activities meet this definition (e.g., decisions on accessions, rating, rewarding, promoting, mobilizing, assigning, retaining, and separating).

DoD Human Resources systems will evolve and/or be replaced to provide for this functionality. In their place will be a single, fully integrated military personnel and pay management system for all of the Department of Defense (DoD) military Services and Components. It will significantly improve support to Joint Commanders by providing the capability to track personnel regardless of Service/Component in any location or environment. Additionally, it will provide the military Service headquarters with an enhanced capability to manage the force, as well as providing individual Service members with simplified, easily available personnel and pay management support. The single system will implement reengineered DoD field, headquarters, and corporate business processes based on best practices for core human resource and pay functions used by the military community and the commercial sector. In achieving full integration of personnel and pay management functions, the single system will provide the following:

- The means for Joint Commanders to access for timely, accurate, and consistent information on personnel assets
- One-time entry of data that automatically triggers all associated personnel and pay management transactions
- Simplified, easily available, accurate personnel and pay management support for Active, Reserve/Guard, and Retired Service members
- A mechanism for the Services to quickly and selectively activate, mobilize, and deploy personnel assets, while maintaining an accurate accounting of the status and location of those assets

CS.HR.2 Purpose and Scope

The Human Resources Subdomain for the Combat Support Domain identifies additions to standards, interfaces, and service areas contained in the DoD Joint Technical Architecture (JTA) Core and Combat Support Domain that pertain to Human Resources systems and external systems that must interoperate with them.

The standards specified in the JTA Core and the Combat Support Domain, combined with those in this document, comprise the minimum set of standards for use by DoD Human Resource systems.

Military standards are mandated only when suitable commercial standards are not available, are not mature, or do not meet the requirements.

CS.HR.3 Applicability

This subdomain applies to all new and existing information systems being upgraded that address Human Resource needs of DoD.

CS.HR.4 Background

Standards beyond those in the JTA Core and the Combat Support Domain are necessary to be specified in this subdomain to minimize interoperability risks as new HR systems come online and as existing ones get upgraded. JTA Core and Combat Support Domain standards facilitate minimizing interoperability risks to a degree. Standards specified in this document further minimize those risks by clarifying information exchange XML tags and semantics, with and between human resource systems.

CS.HR.5 Core-Related Information Technology Categories

Standards in the Information Processing – Data Interchange Standards area are specified below. Additional standards in this and other standards areas may soon be specified, providing further elaboration of hierarchically superior standards.

CS.HR.5.1 Information Processing

This section identifies information processing standards required by the human resources community in addition to the standards cited in the JTA Core and Combat Support Domain.

CS.HR.5.1.1 Document Interchange

This section identifies document interchange standards required by the human resources community in addition to the standards cited in the JTA Core and Combat Support Domain.

CS.HR.5.1.1(a) Mandated. There are no mandated standards.

CS.HR.5.1.1(b) Emerging. The following standard describes the form of the Person Name object used in HR-XML specifications and is emerging:

– HR-XML Consortium Standard for Person Name, Version: 1.0, (8 November 2000).

Staffing Exchange Protocol (SEP) is simple protocol for communication of information about job or position opportunities to job boards and other Internet recruiting venues. The protocol also provides the return of information about job/position seekers. The following standard is emerging:

– HR-XML Consortium Standard for Staffing Exchange Protocol (SEP), Version: 1.0, (8 November 2000).

CS.MED: Medical Subdomain

CS.MED.1 Subdomain Description

The Medical (MED) Subdomain includes the information systems, information, personnel, and facilities engaged in providing healthcare and medical support functions within the Department of Defense (DoD). These consist of component systems that support the following information management core business processes within the Medical Subdomain:

- Access to Care: the front-end process that starts with the identification of a care need(s) by the beneficiary or provider and stops prior to the care being delivered.
- Provision of Health Services: beneficiary- and command-focused proactive, continual process of achieving the best possible health status for individuals and populations through screening, assessment and intervention.
- Population Health Management: process for optimizing the health, health planning, and health management of all beneficiaries.
- Manage the Business: administrative infrastructure support and physical infrastructure support processes that include financial services, operational support, human resources, managed care contracting, billing, materials management and other administrative services.

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.2 Purpose and Scope

The Medical Subdomain identifies additions to the standards, interfaces, and service areas contained in the DoD Joint Technical Architecture (JTA) Core and Combat Support Domain that pertain to medical systems. These additions are common to the majority of systems in the Medical Subdomain and support the interoperability requirements of those systems.

The standards specified in the JTA Core and the Combat Support Domain, combined with those in this subdomain, comprise the minimum set of standards for the Military Health System (MHS).

CS.MED.3 Applicability

This subdomain applies to all new and upgraded medical information systems.

CS.MED.4 Background

The MHS is an integrated healthcare delivery system that provides health care to its beneficiary population largely consisting of active-duty personnel, their dependents, and retirees. 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.5 Core-Related Information Technology Categories

The following medical-specific standards concerning medical Electronic Data Interchange (EDI), medical still imagery data interchange, medical information exchange, and information security have been identified by the Medical Subdomain in addition to the standards found in the JTA Core and the Combat Support Domain.

CS.MED.5.1 Medical Electronic Data Interchange

The following EDI standards are used for clinical, healthcare administrative, and retail pharmacy transactions. This section includes the standards required by the final rules for implementing the Health Insurance Portability and Accountability Act (HIPAA).

CS.MED.5.1.1 Clinical Transactions

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 Standards 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).

CS.MED.5.1.1(a) Mandated. 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.5.1.2 Healthcare Administrative Transactions

As published in the Federal Register/Vol. 65, No. 160/Thursday, August 17, 2000/Rules and Regulations, final rules implementing HIPAA require the use of revised versions of implementation specifications for specific health insurance EDI transactions developed by the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12 Insurance Subcommittee (X12N). Current information on the required compliance date can be found on the Department of Health and Human Services' Administrative Simplification web site at http://aspe.hhs.gov/admnsimp/index.htm.

CS.MED.5.1.2(a) Mandated. The following standards are mandated:

- ASC X12N 270/271, Health Care Eligibility Benefit Inquiry and Response, Version 4010, May 2000, Washington Publishing Company, 004010X092.
- ASC X12N 276/277, Health Care Claim Status Request and Response, Version 4010, May 2000, Washington Publishing Company, 004010X093.
- ASC X12N 278, Health Care Services Review – Request for Review and Response, Version 4010, May 2000, Washington Publishing Company, 004010X094.
- ASC X12N 820, Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, May 2000, Washington Publishing Company, 004010X061.

- ASC X12N 834, Benefit Enrollment and Maintenance, Version 4010, May 2000, Washington Publishing Company, 004010X095.
- ASC X12N 835, Health Care Claim Payment/Advice, Version 4010, May 2000, Washington Publishing Company, 004010X091.
- ASC X12N 837, Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096.
- ASC X12N 837, Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097.
- ASC X12N 837, Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X098.

These implementation specifications can be downloaded from the Washington Publishing Company website at http://hipaa.wpc-edi.com/HIPAA_40.asp.

CS.MED.5.1.3 Retail Pharmacy Transactions

The National Council for Prescription Drug Programs (NCPDP) has published standards for retail pharmacy claims EDI. These standards apply 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.

As published in the Federal Register/Vol. 65, No. 160/Thursday, August 17, 2000/Rules and Regulations, final rules implementing HIPAA require the use of NCPDP standards for the transmission of health plan transactions concerning prescription drugs and pharmaceuticals. Current information on the required compliance date can be found on the Department of Health and Human Services' Administrative Simplification web site at http://aspe.hhs.gov/admnsimp/index.htm.

CS.MED.5.1.3(a) Mandated. The following standards are mandated for retail pharmacy claims EDI:

- NCPDP Telecommunication Standard Implementation Guide, Version 5 Release 1, September 1999.
- NCPDP Batch Standard Batch Implementation Guide, Version 1 Release 0, February 1996.

CS.MED.5.2 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).

Additional information can be found on the DICOM web page at http://medical.nema.org/DICOM.html.

CS.MED.5.2(a) Mandated. 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.5.3 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.

CS.MED.5.3(a) Mandated. 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.5.3(b) Emerging. The following standard is emerging:

– ISBT 128, Bar Code Symbology and Application Specification for Labeling of Whole Blood and Blood Components, Version 1.4.0, June 2001.

CS.MED.5.4 Information Security Standards

This section identifies information security standards required to ensure secure interoperability of medical data that is processed, stored and transmitted on MHS Automated Information Systems (AISs) and Networks.

The Military Health Services System (MHSS) Automated Information System (AIS) Security Policy Manual, Version 1.0, April 1996, published by the Office of the Assistant Secretary of Defense (Health Affairs) contains information security policies, procedures, and guidance for the Military Health System (MHS) AISs and Networks that process, store and transmit medical and patient data. This manual is currently under revision.

M&S: Modeling and Simulation Domain

M&S.1 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.

M&S.2 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.3 Scope and Applicability

In November 2000, the Under Secretary of Defense for Acquisition and Technology (USD[A&T]) approved a Memorandum of Agreement (MoA) between members of the DoD Executive Council for Modeling and Simulation (EXCIMS). The MoA reaffirms the adopting of the High Level Architecture (HLA) as the standard technical architecture for DoD simulation interoperability. 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. For compliance guidance, see MoA at http://www.dmso.mil (Home: Warfighter: HLA: Helpful Resources).

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.

M&S.4 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.5 Core-Related Information Technology Categories

The following standards apply in addition to those found in the JTA Core. The HLA Rules, the HLA Interface Specification and the HLA Object Model Template Specification define the HLA. 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.5.1 Information Processing Standards

In addition to those mandates for information processing standards described in Section 2 of the JTA Core, the following are unique mandates applicable to the Modeling and Simulation Domain.

M&S.5.1(a) Mandated. The HLA Framework and 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).

HLA Federate Interface Specification interacts 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 Interface Definition Language (IDL) and Application Programming Interface (IDLAPI). The following standards are mandated:

- OMG Facility for Distributed Simulation Systems, Version 1.1, December 2000.
- U.S. Department of Defense, High-Level Architecture Interface Specification, Version 1.3, dated 2 April 1998.

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.5.1(b) Emerging. The Standards Board of the Institute of Electrical and Electronics Engineers (IEEE) voted on September 21, 2000, to accept the HLA as an IEEE standard. As a result of that decision, Defense Modeling and Simulation Office (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, 2000.
- IEEE 1516.1-2000, IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Federate Interface Specification, 2000.

– IEEE 1516.2-2000, IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Object Model Template (OMT) 2000.

M&S.5.2 Information Modeling, Metadata, and Information Exchange Standards

In addition to those mandated standards for Information Modeling, Metadata, and Information Exchange Standards described in 4.8 of the JTA, the following mandated standards are applicable to the Modeling and Simulation Domain.

M&S.5.2(a) Mandated. This Federation Execution Details 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:

- U.S. Department of Defense, High-level Architecture (HLA) Interface Specification, Version 1.3, 2 April 1998, Section 12.

Object Model Template Data Interchange Format is the data interchange format that 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:

- U.S. Department of Defense, High-level Architecture (HLA) – Object Model Template Specification, Version 1.3, 5 February 1998 (20 April 1998 Document Release), Annex E.

Standard Simulator Database Interchange Format is a DoD data exchange standard (MIL-STD-1821) that 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.5.2(b) Emerging. Synthetic Environment Data Representation and Interchange Specification (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.The following SEDRIS standards are emerging for M&S system use in the exchange of product-independent environmental data:

– ISO/IEC AWI WD 18024: SEDRIS Language Bindings: C, Version 1, 21 January 2000.

WS: Weapon Systems Domain

WS.1 Domain Description

The Weapon Systems Domain is applicable to weapon systems, which are defined as a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.[1] Weapon systems have special attributes (e.g., timeliness, embedded nature, space and weight limitations), adverse environmental conditions, and critical requirements (e.g., survivability, low power/weight, and dependable hard real-time processing) that drive system architectures and make system hardware and software highly interdependent and interrelated. The position of the Weapon Systems Domain in the Joint Technical Architecture (JTA) Hierarchy Model is shown in Figure 1-2.

WS.2 Purpose and Scope

The purpose of this section is to identify standards for the Weapon Systems (WS) Domain, including information standards and analogous standards applicable to weapon systems.

The Weapon Systems Domain encompasses a subset of the JTA and the specific supporting standards profile.The family of systems (FoS) comprised in this domain has the primary function of supporting attack and/or defense against an adversary. These systems are intentionally designed to interoperate with other weapon systems and/or with systems external to the Weapon Systems Domain.

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 domain or subdomains or are integrated, based on operational requirements, into a 'system of systems' on the battlefield and therefore developers must also consider applicable standards from the pertinent domains or 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 and munition systems —wheeled and tracked, manned, and unmanned.
- **Missile Defense Subdomain** – Includes any system or subsystem (including associated Battle Management/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.

[1] Joint Publication 1-02, DoD Dictionary of Military and Associated Terms.

- **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.

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.[2] The Weapon Systems Domain is applicable to all weapon systems meeting that definition.

WS.3 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.3.1 Technical Reference Model

The Weapon Systems Domain and subdomains use both the DoD Technical Reference Model (TRM) Service View and the Interface View, as described in 1.8. 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 1-3 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

[2] Ibid.

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-runtime 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.

WS.4 uses the Service View and identifies additions to the JTA Core standards, and WS.5 uses the layers identified in the Interface View as a context for classifying interface standards used in the design of weapon systems platforms. WS.4 and WS.5 both include emerging standards that represent current standards work within the Weapon Systems Domain.

WS.4 JTA Core-Related Information Technology Categories

The following categories contain standards that apply to mission-area, support application, and application platform service software developed or procured to process information for weapon systems. These categories specify standards and, in some cases, service areas that are beyond those in the JTA Core, yet are required for interoperability in the Weapon Systems Domain.

WS.4.1 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.4.1(a) Mandated. There are no mandated Information Modeling, Metadata, and Information Exchange standards for this domain.

WS.4.1(b) Emerging. The following emerging standards are being considered for mandate by the Weapon Systems Domain as an addition to the JTA information-modeling standards:

– IEEE 1076:2002, Standard VHSIC Hardware Description Language (VHDL) Reference Manual, 2002. (VHDL is a high-level hardware language).

- IEEE 1076.2: VHDL Mathematical Package, 1996.
- IEEE 1076.3: Standard VHDL Synthesis Packages, 1997.
- IEEE 1076.4: VITAL Application-Specific Integrated Circuit (ASIC) Modeling Specification, 2000.

WS.4.2 Human-Computer Interface Standards

This section provides a common framework for Human-Computer Interfaces (HCI) design and implementation in weapon systems. 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.4.2(a) Mandated. No standards are mandated for this domain.

WS.4.2(b) Emerging. 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 3.0, December 1999.

WS.4.3 Symbology

Weapon systems require the use of multiple symbology standards to meet platform or system performance requirements.

WS.4.3(a) Mandated. For weapons platforms that require the use of Force Operations symbology, the following standard is mandated:

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

WS.5 Domain-Specific Services and Interfaces

This section of the Weapon Systems Domain specifies standards applicable to designing real-time and embedded hardware/software computing systems.

WS.5.1 Systems Services Layer Interfaces

The following interfaces are System Service Layer Interfaces. Some of these interfaces have multiple roles, such as security, internationalization, system management services, and distributed computing services.

WS.5.1.1 Operating Environment Interface

Operating Environment interfaces provide the core services needed to operate and administer the application platform and provide an interface between the application software and the platform. Application programmers will use operating environment interfaces to access operating system functions. To separate sensitive data within an information system, the kernel must include mechanisms to control access to that information and to the underlying hardware.

WS.5.1.1(a) Mandated. There are no mandated Operating Environment Interface standards for this domain.

WS.5.1.1(b) Emerging. The Weapon Systems Technical Architecture Working Group (WSTAWG) Operating Environment (OE) Application Programmer's Interface (API) provides a standardized interface to a set of distributable objects that can be utilized in the creation of rehostable distributed real time embedded weapon systems applications. This API has been defined in a scaleable, extensible, language independent manner such that it can be tailored to application specific requirements, resulting in an increased potential for application reuse throughout the weapon systems domain. The following standard is emerging:

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

For more information on the WSTAWG OE API, go to http://wstawg.army.mil.

WS.5.2 Physical Resources Layer Interfaces

Standards that conform to the class of interfaces specified by the Physical Resources Layer of the DoD TRM interface view are addressed in this section. 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.5.2.1 Parallel Buses

A parallel bus is one wherein information (data, interrupts, arbitration, timing, etc.) is transferred by sending a number of bits (such as 8 or 16) at the same time using multiconductor cables and connectors.

WS.5.2.1.1 Single Board Computers (SBCs) Expansion Buses

The SBC expansion bus is a high-speed I/O bus which allows microprocessor to communicate with external devices.

WS.5.2.1.1(a) Mandated. There are no standards are mandated for Physical Resources Layer Interface standards in this domain.

WS.5.2.1.1(b) Emerging. PCI (peripheral component interface) is a high speed local bus being used by several CICS and RISC microprocessors. PCI specification defines a 4.2 inch by 12.3 inch board that plugs into a motherboard in a perpendicular fashion. These perpendicular boards are not usable in many Weapon Systems because they use too much vertical space. The following emerging standard defines the mechanics of a low profile modular horizontal mezzanine card family that uses the logical and electrical layers of the PCI specification for the local bus with I/O accessible via the front panel and/or through the connector to the host computer for rear panel I/O.

- IEEE 1386.1-2001, IEEE for a Common Mezzanine Card Family: CMC and IEEE Standard Physical and Environmental Layers for PCI Mezzanine Cards: PMC, 2001.
- ATSC Document A/53, ATSC Digital Television Standard, 16 September 1995.

WS.AV: Aviation Subdomain

NOTE: The standards and guidelines contained in this Subdomain are precedent for aviation systems as prepared by the Joint Aeronautical Commanders Group (JACG), Aviation Engineering Board (AEB), and Interoperability Subboard (ISB).

WS.AV.1 Aviation Subdomain Overview

The Aviation Subdomain has been created with the intention that it will be the principal reference for Service Acquisition Executives, Program Executive Officers, and aviation Program teams to identify interoperability standards for aviation systems. In consonance with this reasoning, all relevant standards that are found in higher tier sections (the Core and the Weapon Systems Domain) of the Joint Technical Architecture (JTA) have been absorbed into the body of this document. All standards in this subdomain are designated "preferred"; which means that they should be given first consideration while addressing interoperability requirements (see WS.AV.1.5). These standards should be applied in consonance with Performance-Based Business Environment (PBBE) principles, and within the context of the Performance-Based Systems Engineering Process.

WS.AV.1.1 Purpose

This subdomain identifies preferred standards applicable to external (skin-to-skin) interfaces for DoD aviation weapon systems that enable system-to-system interoperability, including airborne-to-airborne/space/surface (afloat)/ground interfaces. Adoption of external interface standards facilitates interoperability, and is recognized as a necessary part of the systems engineering process to ensure that the system's interoperability requirements are properly addressed.

WS.AV.1.2 Background

Preferred standards listed in section WS.AV.2 of this subdomain are based on work performed by the Aviation Subdomain Working Group (AVSDWG) for the Joint Aeronautical Commanders Group Aeronautical Engineering Board Interoperability Subboard. AVSDWG membership consists of representatives from the military Services, the United States Coast Guard, the Federal Aviation Administration, and aerospace industry.

WS.AV.1.3 Scope and Applicability

The Aviation Subdomain is applicable to all DoD aviation weapon systems. These include both fixed-wing and rotary-wing aircraft (manned and unmanned), and exclude missiles and missile defense systems (which are covered elsewhere in the Weapon Systems Domain of the JTA). Specifically excluded are interoperability standards that apply to other JTA domains/subdomains such as C4I and munitions. These standards do not fit within the scope of the JTA "minimum set" concept.

WS.AV.1.4 Subdomain Organization

This subdomain is divided into four sections: WS.AV.1, Overview; WS.AV.2, Preferred Interoperability Standards; WS.AV.3, Other JTA Standards; and WS.AV.4, Terms, Definitions and Acronyms. Four distinct Aviation Subdomain functional areas have been defined: Communications, Data Links, Navigation/Landing Aids, and Identification Aids. Aviation Subdomain preferred standards have been grouped into these four functional areas.

WS.AV.1.5 Preferred Standards Selection Process

Preferred standards have been selected by the AVSDWG in accordance with the JTA Aviation Subdomain Preferred Standards Selection Process (Figure WS.AV-1). Standards were screened to

ensure that they enable interoperability among and between DoD aviation weapon systems, including associated airborne-to-airborne, space, surface (afloat), and ground interface elements. The Aviation Subdomain Preferred Standards List (section WS.AV.2) contains standards that meet interoperability requirements and meet the "best fit" ground rules, i.e., "forward looking" and "open." Standards that do not meet interoperability requirements and/or do not meet the "best fit" ground rules, but are found elsewhere in the JTA, are regarded as "other JTA standards" as explained in section WS.AV.3. Only systems and technologies that have associated standards have been included.

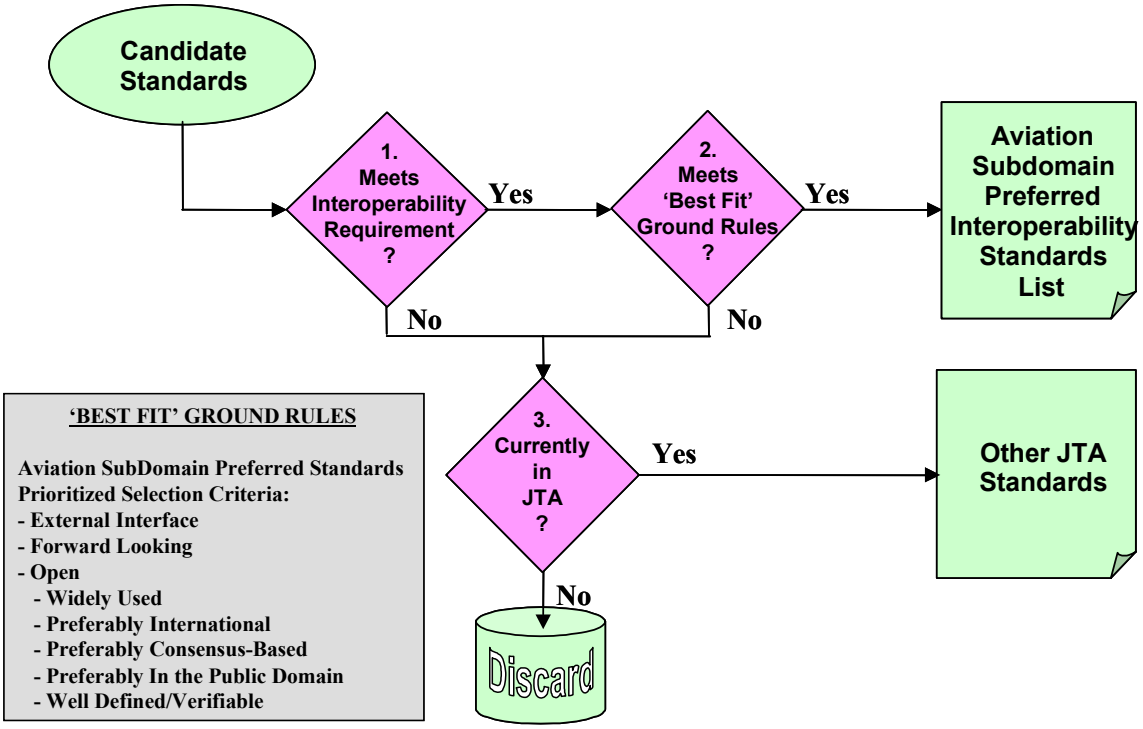


Figure WS.AV-1: JTA Aviation Subdomain Preferred Standards Selection Process

WS.AV.1.5.1 Best Fit Ground Rules

Aviation Subdomain preferred standards include the minimum set of standards required to enable system-to-system interoperability. In addition, Aviation Subdomain preferred standards must also be forward looking and/or open. Forward looking is considered a higher priority in selecting preferred standards. In addition, only standards that address an external interoperability requirement are considered for this subdomain.

WS.AV.1.5.1.1 Forward Looking

Forward looking standards are those required to enable interoperability on future DoD aviation weapon systems and major upgrades to existing systems. Legacy standards are considered forward looking if they are required for future systems. If a legacy standard is no longer required for future aviation weapon systems, it would be removed from the preferred list; however, it may still meet specific performance-based requirements.

WS.AV.1.5.1.2 Open

Open standards are widely used, preferably international, preferably consensus-based, preferably in the public domain, and well defined (verifiable). To be considered open, a standard does not have to meet

all criteria listed. These criteria are listed below in priority order for consideration in selecting preferred standards.

WS.AV.1.5.1.2.1 Widely Used

Widely used is conceptual in nature and as a result difficult to define. There can be a wide range of users, from one to thousands. Typically, the concept requires some judgement; e.g., if there are two standards, and one has a single user and the other has multiple users, the standard with multiple users would be preferred.

WS.AV.1.5.1.2.2 International

Standards that are accepted by more than one nation or international organizations are preferred.

WS.AV.1.5.1.2.3 Consensus Based

Consensus based means that more than one entity, or a standard development organization representing more than one entity, has agreed upon or promulgated the standard.

WS.AV.1.5.1.2.4 Public Domain

Public domain means the standard is not owned by a single company and is publicly available. Any company could use the standard without paying license or royalty fees.

WS.AV.1.5.1.2.5 Well Defined (Verifiable)

A well-defined standard contains readily available documentation that is complete enough for use by a design team, and includes verification criteria to check the design solution for compliance.

WS.AV.2 Aviation Subdomain Preferred Interoperability Standards

This section identifies the preferred interoperability standards for the Aviation Subdomain. It is divided into four distinct service areas for aviation platform interoperability: Communications, Data Links, Navigation/Landing Aids, and Identification Aids. Preferred standards that are duplicated elsewhere in the DoD JTA are marked "●" for mandated standards and "–" for emerging standards. Standards that are unique to the Aviation Subdomain are marked "♠."

WS.AV.2.1 Communications

WS.AV.2.1.1 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.

For 5-kHz or 25-kHz single-channel access service supporting the transmission of either voice or data:

- MIL-STD-188-181B, Interoperability Standard for Single Access 5-kHz and 25-kHz UHF Satellite Communications Channels, 20 March 1999.

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:

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

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:

- MIL-STD-188-183A, Interoperability Standard for 25-Khz TDMA/DAMA Terminal Waveform (Including 5-Khz and 25-Khz Slave Channels), 20 March 1998, with Notice of Change 1, 9 September 1998.

For data controllers operating over single-access 5-kHz and 25-kHz UHF SATCOM channels:

- MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993, with Notice of Change 1, 9 September 1998.

This standard describes a robust link protocol that can transfer error-free data efficiently and effectively over channels that have high error rates.

For MILSATCOM equipment that control access to DAMA UHF 5-kHz and 25-kHz MILSATCOM channels:

- 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.

WS.AV.2.1.2 Radio Communications

WS.AV.2.1.2.1 High Frequency

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

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

For anti-jamming capabilities for HF radio equipment:

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

For HF data modem interfaces:

- ♠ ARINC 635-2, High Frequency (HF) Data Link Protocols, 27 February 1998.
- MIL-STD-188-110B, Interoperability and Performance Standards for Data Modems, 27 April 2000.

WS.AV.2.1.2.2 Very High Frequency

For radio subsystem requirements operating in the Very High Frequency (VHF) bands:

- ♠ ARINC 750-2, VHF Data Radio, December 1997.

- RTCA DO-186A, Minimum Operational Performance Standards for Airborne Radio Communications Equipment Operating Within the Radio Frequency Range (117.975-137.000 MHz), October 1995.
- MIL-STD-188-241, RF Interface Requirements for VHF Frequency Hopping Tactical Radio Systems. This standard identifies the anti-jamming capabilities for VHF radio systems. This is a classified document currently under development (no date yet).
- MIL-STD-188-242, Tactical Single Channel (VHF) Radio Equipment, 20 June 1985.

WS.AV.2.1.2.3 Ultra High Frequency

For radio subsystem requirements operating in the Ultra High Frequency (UHF) bands:

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

For anti-jamming capabilities for UHF radio equipment:

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

WS.AV.2.1.2.4 Combat Net Radio

The Combat Net Radio (CNR) network supports the Army battlefield. It uses existing radio waveforms to physically transmit the data for airborne and mobile ground users. The following standards define CNR interoperability requirements at present:

- MIL-STD-188-220C, Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, 22 May 2002.
- MIL-STD-2045-47001C, Interoperability Standard for Connectionless Data Transfer Application Layer Standard, 22 March 2002.
- Variable Message Format (VMF), Technical Interface Design Plan (Test Edition) Reissue 5, 18 January 2002.

WS.AV.2.1.2.5 Global Air Traffic Management – Communications

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 integrated system of ATM. As a result, DoD aircraft must conform, where required, to appropriate civil requirements and industry standards to meet future civil airspace requirements. These aircraft must be properly equipped to operate in the defined civil aviation regulated airspace environment, and accommodate its evolution. If not, they will be unable 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 provided passage in the airspace but may encounter non-optimal routes and traffic delays according to Euro Control documents or may be excluded from operating in that airspace. The focus of this section is on communications and information-transfer standards for civil ATM interoperability.

The following Air Traffic Management Interoperability Standards covering VHF Digital Link Mode 2, HF Data Link, Aeronautical Mobile Satellite Services, Traffic Alert and Collision Avoidance System

(TCAS), and Mode S capabilities needed to interoperate with civil communications infrastructures are considered preferred standards:

- – ICAO Annex 10, Volume III, International Standards and Recommended Practices (SARPs) for High Frequency Data Link (HFDL), July 1995.
- ♠ RTCA DO-181B, Minimum Operational Performance Standards for Air Traffic Control Radar Beacon System/Mode Select (ATCRBS/Mode S), Airborne Equipment, 29 July 1999.
- ♠ RTCA DO-210C, Minimum Operational Performance Standards for Aeronautical Mobile Satellite Services (AMSS), 16 January 1996.
- ♠ RTCA DO-212, Minimum Operational Performance Standards for Airborne Automatic Dependent Surveillance (ADS) Equipment, 26 October 1992. This is now referred to as Automatic Dependent Surveillance-Address (ADS-A).
- ♠ RTCA DO-219, Minimum Operational Performance Standards for ATC Two-Way Data Link Communications, 27 August 1993.
- ♠ RTCA DO-224, Signal-in-Space Minimum Aviation Systems Performance Standards (MASPS) Advanced VHF Digital Data, Communications Including Capability with Digital Voice Technique, 12 September 1994.
- ♠ 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.
- ♠ RTCA DO-240, Minimum Operational Performance Standards for Aeronautical Telecommunication Network (ATN) Avionics, 29 July 1997.
- ♠ RTCA DO-246A, GNSS-Based Precision Approach Local Area Augmentation System (LAAS) – Signal-in-Space Interface Control Document (ICD), 11 January 2000.

WS.AV.2.1.2.5.1 Traffic Information

- ♠ RTCA DO-239, Minimum Operational Performance Standards for Traffic Information Service (TIS) Data Link Communications, 2 April 1997, Errata, 17 October 1997.

WS.AV.2.1.2.5.2 Area Navigation

- ♠ FAA Advisory Circular (AC) No. 90-96, Approval of U.S. Operators and Aircraft to Operate Under Instrument Flight Rules (IFR) in European Airspace Designated for Basic Area Navigation (BRNAV/RNP-5), 20 March 1998.
- ♠ FAA Order 8400.12A, Required Navigation Performance 10 (RNP-10) Operational Approval, 9 February 1998.
- ♠ RTCA DO-236, Minimum Aviation System Performance Standards: Required Navigation Performance for Area Navigation, 27 January 1997.

WS.AV.2.2 Data Links

WS.AV.2.2.1 Link 4A

Link 4A is used in combat direction systems and Link 4A controlled aircraft. It is also used for aircraft carrier deck landings (Navy only).

- ♠ MIL-STD-188-203-3, Subsystem Design Performance Standards for Tactical Digital Information Link (TADIL) C, 5 October 1983.

WS.AV.2.2.2 Link 11

This data link is for communicating with tactical data systems of U.S. and allied forces.

- MIL-STD-6011B, Tactical Digital Information Link (TADIL) A/B Message Standard for Achieving Compatibility and Interoperability, 30 April 1999.

WS.AV.2.2.3 Link 16

For communicating with Tactical Digital Information Link (TADIL) J, and for communicating with the Joint Tactical Information Distribution System (JTIDS)/Multi-functional Information Distribution System (MIDS) radios, the following standards are mandated:

- STANAG 4175, Edition 1, Technical Characteristics of the Multifunctional Information Distribution System (MIDS), 29 August 1991.
- STANAG 5516, Edition 2, NATO Standardization Agreement for Tactical Data Exchange-Link 16, February 1998.
- MIL-STD-6016B, Tactical Digital Information Link (TADIL) J Message Standard, 1 August 2002.

WS.AV.2.3 Navigation/Landing Aids

WS.AV.2.3.1 Global Positioning

The CJCS (CJCSI 6130.01A, 1998 CJCS Master Positioning, Navigation, and Timing Plan) has declared that the GPS will be the primary radio navigation source of positioning, navigation and timing (PNT) for the 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.

- STANAG 4294, NAVSTAR Global Positioning System (GPS) – System Characteristics (Part 1, Edition 2 dated December 1997) plus Summary of Performance Requirements (Part 2, Edition 2 dated June 1995).
- RTCA DO-208 – Change 1, Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment Using Global Positioning System, 23 September 1993.
- ICD-GPS-200C, NAVSTAR GPS Space Segment/Navigation User Interfaces, 16 October 1997.

WS.AV.2.3.1.1 Global Air Traffic Management – Navigation

The following civil global navigation standards provide interoperability for DoD aircraft to navigate and land in the evolving global civil aviation airspace arena. Two types of global navigation satellite augmentation have been standardized by ICAO – the Space-Based Augmentation System (SBAS) and the Ground-Based Augmentation System (GBAS). These are known in the United States as Wide Area Augmentation System (WAAS) and Local Area Augmentation System (LAAS), respectively. Interoperability standards include ICAO Annex 10 documentation and RTCA standards as well as specific operational approval documents such as FAA Advisory Circulars (AC). Compliance or equivalence with these standards is necessary for authorized IFR operations.

- ICAO SARPs, Aeronautical Telecommunications, Annex 10 to the Convention on International Civil Aviation. Proposed SARPs for the Global Navigation Satellite System (GNSS), Space-Based Augmentation System (SBAS), and Ground-Based Augmentation System (GBAS), DRAFT, 9 June 2000.

- FAA AC No. 90-94, Guidelines for Using GPS Equipment for IFR En Route & Terminal Operations & for Nonprecision Instrument Approaches in the U.S. National Airspace System, 14 December 1994.
- FAA AC No. 90-96, Approval of U.S. Operators and Aircraft to Operate Under Instrument Flight Rules (IFR) in European Airspace Designated for Basic Area Navigation (BRNAV/RNP-5), 20 March 1998.
- FAA Order 8400.12A, Required Navigation Performance 10 (RNP-10) Operational Approval, 9 February 1998.
- FAA Notice 8110.60, GPS as a Primary Means of Navigation for Oceanic/Remote Operations, 4 December 1995.
- RTCA DO-229B, Minimum Operational Performance Standards for Global Positioning System/Wide Area Augmentation System Airborne Equipment, 6 October 1999.
- RTCA DO-245, Minimum Aviation System Performance Standards for Local Area Augmentation System (LAAS), 28 September 1998.
- RTCA DO-246A, GNSS-Based Precision Approach Local Area Augmentation System (LAAS) – Signal-in-Space Interface Control Document (ICD), 11 January 2000.
- RTCA DO-247, The Role of the Global Navigation Satellite System (GNSS) in Supporting Airport Surface Operations, 7 January 1999.
- RTCA DO-253, Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment, 11 January 2000.

WS.AV.2.3.2 Tactical Area Navigation

- MIL-STD-291C, Standard Tactical Air Navigation (TACAN) Signal, 10 February 1998.

WS.AV.2.3.3 Airborne Radio Marker

- RTCA DO-143, Minimum Performance Standards – Airborne Radio Marker Receiving Equipment Operating on 75 MHz, March 1970.

WS.AV.2.3.4 Landing Aids

WS.AV.2.3.4.1 Instrument Landing Aids

- ICAO International Standards and Recommended Practices (SARPs), Aeronautical Telecommunications, Annex 10 to the Convention on International Civil Aviation, Volume I (Radio Navigation Aids), July 1996.
- RTCA DO-192, ILS Instrument Landing Systems Glideslope Minimum Operational Performance Standards for Airborne ILS Glide Slope Receiving Equipment Operating Within the Radio Frequency Range of 328.6-335.4 MHz, 18 July 1986.
- RTCA DO-195, ILS Localizer Receiving Equipment Operating within the Radio Frequency Range of 108-112 MHz, 17 November 1986.

WS.AV.2.3.4.2 Microwave Landing Aids

- ICAO International Standards and Recommended Practices (SARPs), Aeronautical Telecommunications, Annex 10 to the Convention on International Civil Aviation, Volume I (Radio Navigation Aids), July 1996.
- EUROCAE ED-36A, Minimum Operational Performance Specification for Microwave Landing System (MLS) Airborne Receiving Equipment, January 1995.
- RTCA DO-177 Change 2, Minimum Operational Performance Standards for Microwave Landing System (MLS) Airborne Receiving Equipment, 19 September 1986.
- STANAG 4184, Microwave Landing System (MLS) Edition 3, November 1988.

WS.AV.2.3.4.3 GPS Landing Aids

- ICAO International Standards and Recommended Practices (SARPs), Aeronautical Telecommunications, Annex 10 to the Convention on International Civil Aviation. Proposed SARPs for the Global Navigation Satellite System (GNSS), Space-Based Augmentation System (SBAS), and Ground-Based Augmentation System (GBAS), DRAFT, 9 June 2000.
- RTCA DO-229B, Minimum Operational Performance Standards for Global Positioning System/ Wide Area Augmentation System Airborne Equipment, 6 October 1999.
- RTCA DO-245, Minimum Aviation System Performance Standards for Local Area Augmentation System (LAAS), 28 September 1998.
- RTCA DO-246A, GNSS-Based Precision Approach Local Area Augmentation System (LAAS) – Signal-in-Space Interface Control Document (ICD), 11 January 2000.
- RTCA DO-253, Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment, 11 January 2000.
- STANAG 4550, Local Area Differential GPS for Military Prevision Approach, DRAFT Edition 1, 7 April 2000.
- STANAG 4392, Edition 2, A Data Interchange Format for GPS; Annex D Format and Usage of PPS DGPS Messages for Aviation and Other High Performance Applications, 9 February 2000.

WS.AV.2.3.4.4 Multimode Landing Aids

- STANAG 4565, Airborne Multi-Mode Receiver (MMR) for Precision Approach and Landing, DRAFT Edition 1, November 1999.

WS.AV.2.4 Identification Aids

WS.AV.2.4.1 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 systems. 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. This is 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.

- ICAO Aeronautical Telecommunications: Annex 10 to the Convention on International Civil Aviation, Volume IV (Surveillance Radar and Collision Avoidance Systems), Edition 1 with Supplements (31 May 1996, 10 November 1997, and July 1998).
- ARINC 718A, Mark 4, Air Traffic Control Transponder (ATCRBS/Mode-S), 15 February 2002.
- FAA 1010.51A, US National Aviation Standard for the Mark X (SIF) Air Traffic Control Radar Beacon System (ATCRBS) Characteristics, 8 March 1971.
- STANAG 4193, Part 1, NATO Standard Agreement Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders, Edition 2, 12 November 1990, with Amendment 1, 15 December 1997.
- STANAG 4193, Part 2, (SECRET), NATO Standard Agreement Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders, Edition 1, 12 November 1990.
- STANAG 4193, Part 3, NATO Standard Agreement Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders, Edition 1, 12 November 1990, with Amendment 1, 31 January 1995.

- STANAG 4193, Part 4, NATO Standard Agreement Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders, 28 November 1997.
- STANAG 4193, Part 5, Annex A through D, (SECRET NATO RESTRICTED), NATO Standard Agreement Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders, 4 September 1998.
- DoD AIMS 97-900, Performance/Design and Qualification Requirements Mode 4 Input/Output Data, 18 March 1998.
- 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.

WS.AV.2.4.2 Traffic Alert and Collision Avoidance

- ARINC 735A, Mark 2 Traffic Alert and Collision Avoidance System (TCAS), December 1997.
- ARINC 735-2, Traffic Alert and Collision Avoidance System (TCAS), (Includes Supplements 1 and 2), January 1993.
- RTCA DO-185A, VOL I, Minimum Operational Performance Standards for Traffic Alert and Collision Avoidance System II (TCAS II) Airborne Equipment Volume I, 16 December 1997.
- RTCA DO-185A, VOL II, Minimum Operational Performance Standards for Traffic Alert and Collision Avoidance System II (TCAS II) Airborne Equipment Volume II, 16 December 1997.
- RTCA DO-197A, Minimum Operational Performance Standards for an Active Traffic Alert and Collision Avoidance System I (Active TCAS I) Errata 11/22/1994, Chg. No. 1 – 1997.

WS.AV.2.4.3 Automatic Dependent Surveillance - Broadcast

- RTCA DO-242, Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B), 19 February 1998.

WS.AV.3 Aviation Subdomain “Other JTA” Standards

All JTA Standards not listed in the Aviation Subdomain Preferred Standards list (sections WS.AV.2.1 – WS.AV.2.4) are “other JTA” standards. The use of other JTA standards on DoD aviation weapon systems is encouraged when a standard can meet a stated or derived requirement. (See step 3 of the Preferred Standards Selection Process.)

WS.AV.4 Aviation Subdomain Terms, Definitions and Acronyms

The following terms have not been sufficiently defined elsewhere, or are easily misunderstood. Their definitions appear here for clarification.

WS.AV.4.1 Performance-Based Business Environment (PBBE)

PBBE is a “state of being” where government customers and contractors/suppliers jointly capitalize on commercial practice efficiencies to improve the acquisition and sustainment environment. In this new environment, solicitations and contracts describe system performance requirements in a way that permits contractors greater latitude than under historical acquisition methods to use their own design and manufacturing ingenuity to meet needs. Additionally, suppliers will compete and be selected based on their proposed approaches, process effectiveness, and prior performance.

WS.AV.4.2 Verifiable

Verification includes substantiation that performance requirements have been satisfied as well as confirmation that delivered products exhibit functionally equivalent performance to the qualified design. This is accomplished through the use of product acceptance criteria that are developed as part

of the engineering development effort. Interface standards should include rigorously defined verification criteria. For electronics and software, a “gold standard” is often used to verify that performance requirements have been achieved.

Page intentionally left blank.

WS.GV: Ground Vehicle Subdomain

WS.GV.1 Subdomain Description

Identify information and analogous standards applicable to ground vehicle systems. Systems covered within the Ground Vehicle Subdomain include all DoD weapon systems on moving ground platforms—wheeled and tracked (except missiles), manned and unmanned.

WS.GV.2 Purpose and Scope

This subdomain specifies standards needed for interoperability between Ground Vehicles and other DoD systems.

WS.GV.3 Background

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

WS.GV.4 Subdomain-Specific Services and Interfaces

The Interfaces View of the Technical Reference Model (TRM), depicted in Figure 1-3, 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 Vehicles 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. Only those layers of the TRM that have subdomain-specific mandated or emerging standards identified are addressed in this section.

WS.GV.4.1 Application Software Layer Interfaces

The Application Software Layer Interfaces provide a set of resources that support the services on which application software will execute. It provides interfaces to services that, as much as possible, make the implementation specific characteristics of the platform transparent to the application software.

WS.GV.4.1(a) Mandated. Currently, there are no subdomain-specific mandated standards identified for this section of the Ground Vehicles Subdomain.

WS.GV.4.1(b) Emerging. The Sensor Link Protocol Message Set (SLP) was developed for use as a common interface between electro-optical sensor systems and a diverse set of host computer systems. The SPL message set is decoupled from lower layer protocols to allow implementers the flexibility to select from a number of open standards such as RS-232/485, FireWire or Universal Serial Bus (USB). The SLP message set is used in conjunction with the SLP Interface Control Document to develop a common digital data exchange mechanism between sensors and host computing devices that offer full remote operation and control of those sensors by a host computing device in both a point-to-point and networked environment. The following emerging standard defines the SLP message set:

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

WS.GV.4.2 System Services Layer Interfaces

The following interfaces are System Service Layer Interfaces. Some of these interfaces have multiple roles, such as security, internationalization, system management services, and distributed computing services.

WS.GV.4.2.1 Operating Environment Interface

The Operating Environment (OE) Application Programmer's Interface (API) provides a standardized interface to a set of distributable objects that can be utilized in the creation of rehostable distributed real time embedded weapon systems applications. This API has been defined in a scaleable, extensible, language independent manner such that it can be tailored to application specific requirements, resulting in an increased potential for application reuse throughout the Weapon System Domain.

WS.GV.4.2.1(a) Mandated. The following operating environment interface standard is mandated for ground vehicles:

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

WS.GV.4.3 Physical Resources Layer Interfaces

Standards that conform to the class of interfaces specified by the Physical Resources Layer of the DoD TRM interface view are addressed in this section. 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.GV.4.3.1 Serial Buses

Serial Buses are buses that transmit information one bit at a time in a sequential or serial manner.

WS.GV.4.3.1(a) Mandated. The MIL-STD-1553B data bus standard will be used by applications requiring digital, command/response, time division multiplexing techniques and defines the data bus line and its interface electronics, the concept of operation and information flow on the multiplex data bus, and the electrical and functional formats to be employed. The following standard is mandated:

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

Society of Automotive Engineers (SAE) J1850 establishes the requirements for a Class B Data Communication Network Interface applicable to all On- and Off-Road Land-Based Vehicles. It defines a minimum set of data communication requirements such that the resulting network is cost effective for simple applications and flexible enough to use in complex applications. The following standard is mandated:

- SAE J1850, Class B Data Communication Network Interface, 1 July 1995.

WS.GV.4.3.1(b) Emerging. Ground vehicle systems is also evaluating the Controller Area Network Bus (CANBUS) protocol and Class C networks documented in SAE J1939 as an emerging standard for use in its heavy trucks and off road vehicles:

- SAE J1939, Recommended Practice for a Serial Control and Communications Vehicle Network, April 2000.

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, which defines the requirements for the hardware and basic protocol needed to implement the requirements of SAE J1587. The following information transfer standard is emerging for ground vehicles:

– SAE J1587, Joint SAE/TMC Electronic Data Interchange Between Microcomputer Systems in Heavy-duty Vehicle Applications, July 1998.

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 information transfer standard is emerging for ground vehicles:

– SAE J1708, Serial Data Communications Between Microcomputer Systems in Heavy-duty Vehicle Applications, October 1993.

The Digital Visual Interface (DVI) Specification Revision 1.0, 02 April 1999, developed by the Digital Display Working Group (DDWG) defines a high-speed digital connection for providing the distribution of visual data information between a processor element and a display device. This specification is meant to serve as a guide toward standard practice information exchange among microcomputer based modules. The following specification is emerging for Ground Vehicles:

– Digital Visual Interface (DVI), Digital Display Working Group (DDWG), Revision 1.0, 02 April 1999.

WS.GV.4.3.2 Parallel Buses

A parallel bus is one wherein information (data, interrupts, arbitration, timing, etc.) is transferred by sending a number of bits (such as 8 or 16) at the same time using multiconductor cables and connectors.

WS.GV.4.3.2.1 Backplane Buses

Backplane buses are designed to allow processors, memory, and I/O devices to coexist on a single bus; they balance the demands of processor-memory communication with the demands of I/O device-memory communication. Backplane buses received their name because they were often built in the backplane, an interconnection structure within the chassis; processor, memory, and I/O boards would then plug into the backplane using the bus for communication.

WS.GV.4.3.2.1(a) Mandated. The VME64 standard defines a framework for 8-, 16-, 32-, and 64-bit parallel bus computer architectures that can implement single and multiprocessor systems. It is based on the VMEbus specification released by the VMEbus Manufacturers Group (now VITA) in August 1982 and includes the initial four basic subbuses: (1) data transfer bus, (2) priority interrupt bus, (3) arbitration bus, and (4) utility bus. The following standards are mandated:

- ANSI/VITA 1, VME64 Specification, 1994.
- ANSI/VITA 1.1, VME64 Extensions, 1997.

PC/104 and PC/104-*Plus* provide a low cost, power and space-saving solution for embedded applications. Both of these mezzanine modules provide an effective method of adding I/O to a host motherboard or single-board computer, and are ideal for military applications because of their small form-factor (3.8" x 3.6") as compared to other backplane buses such as VME (9.18" x 6.29") and cPCI (6.3" x 3.9"). PC/104 and PC/104-*Plus* support low bandwidth applications, such as data acquisition and control (using the ISA bus), as well as high bandwidth applications, such as video, networking and disk storage (using the PCI bus). The following standards are mandated:

- PC/104-*Plus* Specification, V1.2, August 2001.
- PC/104 Specification, V2.4, August 2001.

WS.GV.4.3.2.2 I/O Buses

I/O buses can be lengthy, can have many types of devices connected to them, and often have a wide range in the data bandwidth of devices connected to them. I/O buses do not typically interface directly to the memory but use either a processor-memory or a backplane bus to connect to memory.

WS.GV.4.3.2.2(a) Mandated. The following industrial bus standard is mandated for applications requiring high-speed data transfer, rugged construction, excellent shock and vibration resistance, Plug'n Fight capability, and the desire for future hot-swappable support:

- PCI Industrial Computer Manufacturer's Group (PICMG): Compact PCI Specification, R2.1, September 1997.

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 communication devices.

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

WS.GV.4.3.2.3 Single Board Computers (SBCs) Expansion Buses

The SBC expansion bus is a high-speed I/O bus which allows microprocessors to communicate with external devices.

WS.GV.4.3.2.3(a) Mandated. The PC Card standard will be used by applications requiring hot-swappable peripherals that add memory, mass storage, and I/O capabilities to computers in a rugged, compact form factor. The following standard is mandated:

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

WS.MD: Missile Defense Subdomain

WS.MD.1 Subdomain Description

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. 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 Technical Reference Model (TRM).

WS.MD.2 Purpose and Scope

There is a need for interoperability among lower tier missile defense systems, upper tier missile defense systems, and other systems such as space-based sensors to support the overall mission of missile defense. Such interoperability would need to support activities such as minimum cueing, track exchange, and weapon coordination. This requires standards to deal with how information should be transferred (e.g., geospatial values). This JTA subdomain specifies such standards to support interoperability to fulfill missile-defense mission objectives.

The scope of this subdomain is the entire domain of missile defense. 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.3 JTA Core-Related Information Technology Categories

This section identifies standards for the Missile Defense Subdomain that are additional to standards in the JTA Core to promote interoperability within the Missile Defense Subdomain.

WS.MD.3.1 Navigation

Missile defense system interoperability, which is necessary to increase mission effectiveness, requires accurate agreements on navigation-related data.

WS.MD.3.1(a) Mandated. 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 Systems [WGS84] and Coordinated Universal Time [UTC] U.S. Naval Observatory [USNO]). The following standard is mandated:

- Ballistic Missile Defense (BMD) Positioning, Navigation, and Timing (PNT) Standard, 20 July 2000, Ballistic Missile Defense Organization.

[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.3.2 Time Synchronization

The time basis for missile defense operations shall be UTC USNO as disseminated by the Navstar Global Positioning System (GPS).

WS.MD.3.2(a) Mandated. The GPS standards identified in 3.4.5 are mandated.

WS.MD.3.3 Information Transfer Standards

This section identifies the information transfer standards required for interoperability among DoD missile defense systems.

WS.MD.3.3(a) Mandated. No Information Transfer Standards are mandated.

WS.MD.3.3(b) Emerging. 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:

– MIL-STD-3011, Interoperability Standard for Joint Range Extension Application Protocol (JREAP), Defense Information Systems Agency (DISA), Information Exchange Management Panel (IXMP), 30 September 2002.

WS.MD.3.4 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.

WS.MD.3.4(a) Mandated. The following standard is mandated for transportable missile defense systems.

- MIL-STD-6016B, Tactical Digital Information Link (TADIL) J Message Standard, 1 August 2002.

WS.MD.3.5 Missile Defense Data Element Descriptions

The Missile Defense Agency through the Data Interoperability and Standardization Steering Group (DISSG) is developing a Data Element Descriptions (DED) document for Interoperability. This DED is composed of data elements selected from the TADIL-J Message Standard and the Variable Message Format (VMF)-based message set for the Ground-based Midcourse Defense System. The data elements were selected for the DED based on the need for sharing this information between and among operational elements of Missile Defense Systems.

There is ongoing work through the Data Element and Exchange Rule Working Group (DEER WG), the working group under the DISSG, to define the objective data elements and exchange rules for the DED to promote information sharing across the Missile Defense community. By identifying and controlling objective data elements that are key to interoperability for new systems, as well as providing

appropriate exchange rules for those data elements when used by legacy systems, current and future message set developers will be confident that they have selected data elements that can be used and properly shared within Missile Defense.

WS.MD.3.5(a) Mandated. No additional standards are mandated for missile defense data element descriptions.

WS.MD.3.5(b) Emerging. The following standard is emerging:

– Ballistic Missile Defense Interoperability Data Element Descriptions (BMD-I DED), Ballistic Missile Defense Organization, Version 3, 28 September 2001.

Page intentionally left blank.

WS.MS: Missile Systems Subdomain

WS.MS.1 Subdomain Description

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).

WS.MS.2 Purpose and Scope

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 1.7.3 for relationships between Core, Domain, and Subdomain standards.)

The scope of this subdomain is all DoD Missile Systems as defined above. However, the standards listed in this 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.3 Background

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.4 JTA Core-Related Information Technology Categories

This section identifies standards for the Missile Systems Subdomain that are additional to standards in the JTA Core to promote interoperability within the Missile Systems Subdomain.

WS.MS.4.1 Information Processing Standards

This section specifies the information processing standards that the DoD will use to develop interoperable missile systems that support warfighter operations.

WS.MS.4.1.1 Geospatial Data Interchange

Geospatial services are also referred to as mapping, charting, and geodesy (MC&G) services. This section specifies the standards to be implemented to ensure seamless exchange of geospatial data across DoD missile systems.

WS.MS.4.1.1(a) Mandated. There are no mandated standards identified for this section of the Missile Systems Subdomain.

WS.MS.4.1.1(b) Emerging. The following standard is being evaluated as an emerging extension to the WGS 84 geospatial data interchange standard for use with Missile Systems:

– ANSI/AIAA R-004-1992, Recommended Practice for Atmospheric and Space Flight Vehicle Coordinate Systems.

WS.MS.4.2 Information Transfer Standards

This section identifies the information transfer standards required for interoperability between DoD missile systems.

WS.MS.4.2(a) Mandated. There are no mandated standards identified for this section of the Missile Systems Subdomain.

WS.MS.4.2(b) Emerging. 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:

– MIL-STD-3011, Interoperability Standard for Joint Range Extension Application Protocol (JREAP), Defense Information Systems Agency (DISA), Information Exchange Management Panel (IXMP), 30 September 2002.

WS.MS.5 Subdomain-Specific Services and Interfaces

The Interfaces View of the Technical Reference Model (TRM), depicted in Figure 1-3, 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. Only those layers of the TRM that have subdomain-specific mandated or emerging standards identified are addressed in this section.

WS.MS.5.1 Physical Resources Layer Interfaces

Standards that conform to the class of interfaces specified by the Physical Resources Layer of the DoD TRM interface view are addressed in this section. 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.5.1.1 Serial Buses

Serial buses are buses that transmit information one bit at a time in a sequential or serial manner.

WS.MS.5.1.1(a) Mandated. There are no additional mandated standards in this Missile System Subdomain.

WS.MS.5.1.1(b) Emerging. The MIL-STD-1553B data bus standard will be used by applications requiring digital, command/response, time division multiplexing techniques and defines the data bus line and its interface electronics, the concept of operation and information flow on the multiplex data bus, and the electrical and functional formats to be employed. The following standard is emerging:

– 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.

WS.MS.5.1.2 Parallel Buses

A parallel bus is one wherein information (data, interrupts, arbitration, timing, etc.) is transferred by sending a number of bits (such as 8 or 16) at the same time using multiconductor cables and connectors.

WS.MS.5.1.2.1 Backplane Buses

Backplane buses are designed to allow processors, memory, and I/O devices to coexist on a single bus; they balance the demands of processor-memory communication with the demands of I/O device-memory communication. Backplane buses received their name because they were often built in the backplane, an interconnection structure within the chassis; processor, memory, and I/O boards would then plug into the backplane using the bus for communication.

WS.MS.5.1.2.1(a) Mandated. There are no mandated standards for the Backplane section of this Missile System Subdomain.

WS.MS.5.1.2.1(b) Emerging. The VME 64 standard defines a framework for 8-, 16-, 32-, and 64-bit parallel bus computer architectures that can implement single and multiprocessor systems. It is based on the VMEbus specification released by the VMbus Manufacturer 2s Group (now VITA) in August 1982 and includes the initial four basic subbuses: (1) data transfer bus, (2) priority interrupt bus, (3) arbitration bus, and (4) utility bus. The following standards are emerging:

– ANSI/VITA 1, VME64 Specification, 1994.
– ANSI/VITA 1.1, VME64 Extensions, 1997.

WS.MS.5.1.2.2 I/O Buses

I/O buses can be lengthy, can have many types of devices connected to them, and often have a wide range in the data bandwidth of devices connected to them. I/O buses do not typically interface directly to the memory but use either a processor-memory or a backplane bus to connect to memory.

WS.MS.5.1.2.2(a) Mandated. There are no mandated standards for the I/O Buses section of the Missile Systems Subdomain.

WS.MS.5.1.2.2(b) Emerging. 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 communication devices.

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

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 Manufacturer's Group (PICMG): Compact PCI Specification, R2.1, September 1997.

WS.MS.5.1.2.3 Single Board Computers (SBCs) Expansion Buses

The SBC expansion bus is a high-speed I/O bus which allows microprocessors to communicate with external devices.

WS.MS.5.1.2.3(a) Mandated. There are no mandated standards for the Single Board Computers Expansion Buses section of the Missile Systems Subdomain.

WS.MS.5.1.2.3(b) Emerging. The PC Card standard will be used by applications requiring hot-swappable peripherals that add memory, mass storage, and I/O capabilities to computers in a rugged, compact form factor. The following standard is emerging:

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

WS.MUS: Munition Systems Subdomain

WS.MUS.1 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.

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.2 Purpose and Scope

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 1.7.3 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.

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.3 Background

This subdomain was developed to specify the unique interoperability standards for DoD Munitions and their corresponding systems.

WS.MUS.4 Subdomain-Specific Services and Interfaces

The Interfaces View of the Technical Reference Model (TRM), depicted in Figure 1-3, 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 Interfaces View also facilitates the identification of critical functions and interfaces within the real-time and embedded-computing systems of the Munition Systems Subdomain.

This section provides a common framework identifying mandated and emerging embedded-computing interface standards associated with the logical and direct interface classes defined for the layers depicted in the Interfaces View of the TRM. Only those layers of the TRM that have subdomain-specific mandated or emerging standards identified are addressed in this section.

WS.MUS.4.1 Application Software Layer Interfaces

The Application Software Layer Interfaces provide a set of resources that support the services on which application software will execute. It provides interfaces to services that, as much as possible, make the implementation specific characteristics of the platform transparent to the application software.

WS.MUS.4.1(a) Mandated. Currently, there are no mandated standards for this part of the Weapon Munition Systems Subdomain.

WS.MUS.4.1(b) Emerging. The Sensor Link Protocol Message Set (SLP) was developed for use as a common interface between electro-optical sensor systems and a diverse set of host computer systems. The SLP message set is decoupled from lower layer protocols to allow implementers the flexibility to select from a number of open standards such as RS-232/485, FireWire or Universal Serial Bus (USB). The SLP message set is used in conjunction with the SLP Interface Control Document to develop a common digital data exchange mechanism between sensors and host computing devices that offer full remote operation and control of those sensors by a host computing device in both a point-to-point and networked environment. The following emerging standard defines the SLP message set:

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

WS.MUS.4.2 Physical Resources Layer Interfaces

Standards that conform to the class of interfaces specified by the Physical Resources Layer of the DoD TRM interface view are addressed in this section. 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.4.2.1 Parallel Buses

A Parallel bus transfers information (data, interrupts, arbitration, timing, etc.) by sending a number of bits (such as 8 or 16) at the same time using multiconductor cables and connectors.

WS.MUS.4.2.1.1 I/O Buses

I/O buses can be lengthy, can have many types of devices connected to them, and often have a wide range in the data bandwidth of devices connected to them. I/O buses do not typically interface directly to the memory but use either a processor-memory or a backplane bus to connect to memory.

WS.MUS.4.2.1.1(a) Mandated. 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 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.

WS.MUS.4.2.1.2 Single Board Computers (SBCs) Expansion Buses

The SBC expansion is high-speed I/O bus which allows microprocessors to communicate with external devices.

WS.MUS.4.2.1.2(a) Mandated. The PC Card standard will be used by applications requiring hot-swappable peripherals that add memory, mass storage, and I/O capabilities to computers in a rugged, compact form factor. The following standard is mandated:

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

Page intentionally left blank.

WS.SS: Soldier Systems Subdomain

WS.SS.1 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 (GFE) and the use of commercial off-the-shelf (COTS) technologies to meet the key performance parameters (KPPs) of soldier systems. These systems are optimized to minimize the total weight carried by the individual while minimizing the weight carried by the soldier as well as 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.2 Purpose and Scope

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 1.7.3 for relationships between JTA Core, domain, and subdomain standards.)

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.3 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, 1 October 2001.

WS.SS.4 Subdomain-Specific Services and Interfaces

The Interfaces View of the Technical Reference Model (TRM), depicted in Figure 1-3, 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 Interfaces View of TRM. Only those layers of the TRM that have subdomain-specific mandated or emerging standards identified are addressed in this section.

WS.SS.4.1 Application Software Layer Interfaces

The Application Software Layer Interfaces provide a set of resources that support the services on which application software will execute. It provides interfaces to services that, as much as possible, make the implementation specific characteristics of the platform transparent to the application software.

WS.SS.4.1(a) Mandated. Currently, there are no mandated standards for the Application Software Layer Interfaces section of this subdomain.

WS.SS.4.1(b) Emerging. The Sensor Link Protocol Message Set (SLP) was developed for use as a common interface between electro-optical sensor systems and a diverse set of host computer systems. The SLP message set is decoupled from lower layer protocols to allow implementers the flexibility to select from a number of open standards such as RS-232/485, FireWire or USB. The SLP message set is used in conjunction with the SLP Interface Control Document to develop a common digital data exchange mechanism between sensors and host computing devices that offer full remote operation and control of those sensors by a host computing device in both a point-to-point and networked environment. The following emerging standard defines the SLP message set:

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

WS.SS.4.2 Physical Resources Layer Interfaces

Standards that conform to the class of interfaces specified by the Physical Resources Layer of the DoD TRM interface view are addressed in this section. 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.4.2.1 Serial Buses

Serial Buses are buses that transmit information one bit at a time in a sequential or serial manner.

WS.SS.4.2.1(a) Mandated. The IEEE 1394 (aka FireWire) bus supports scalable performance by supporting rates of 100, 200 and 400 Mbit/s in both the guaranteed delivery asynchronous mode as well as the guaranteed bandwidth isochronous transmission mode. Each topology can support up to a total of 64 nodes with up to 16 contiguous hops, and up to a total of 1024 buses. For serial bus infrastructures requiring transmission of video, voice and data where guaranteed bandwidth for video and voice, and guaranteed delivery of data are required, the following standards are mandated:

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

WS.SS.4.2.1(b) Emerging. The IEEE 1394b-2001 is a full use standard whose scope is to provide a supplement to IEEE 1394-1995 and IEEE 1394-2000 that defines features and mechanisms conducive

to gigabit speeds in a backward compatible fashion and the ability to signal over single hop distances of up to 100m. The following standard is emerging:

– IEEE 1394b-2001, IEEE Standard for a High Performance Serial Bus, 2001.

The Digital Visual Interface (DVI) is a display technology independent interface standard between a host and a display. DVI provides a plug and play capability in a single connector supporting both analog and digital or digital only. This standard is sponsored by the Digital Display Working Group (DDWG) comprised of Intel Corp., Silicon Image, Compaq Computer, Fujitsu. HP, IBM and NEC, and is considered an open standard. The following standard is emerging:

– Digital Visual Interface (DVI), Digital Display Working Group (DDWG), Revision 1.0, 02 April 1999.

Low Voltage Differential Signaling (LVDS) is denoted by the EIA/TIA-644 standard, which is a balanced (differential) bus wherein only the electrical layer (RCVR/TX) is defined. LVDS is an approach to achieve high bandwidth with low EMI, which is applicable to a myriad of commonly used media, and is also pin-to-pin compatible with RS-422 transmitters and receivers. LVDS is an approved standard through ANSI forum. This standard is used for high-bandwidth, low-power, digital serial interface, used in displays and cameras. The following standard is emerging

– Electrical Characteristics of LVDS Interface Circuits, March 1996.

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
ADC	Automatic Data Capture
ACTD	Advanced Concept Technology Demonstration
ADE	Application Development Environment
ADS	Automatic Dependent Surveillance
ADS-A	Automatic Dependent Surveillance – Address
ADS-B	Automatic Dependent Surveillance – Broadcast
ADT	Air Data Terminal
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)
ARTS	Automated Radar Terminal System
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
ASR	Airport Surveillance Radar
ATA	Army Technical Architecture
ATCRBS	Air Traffic Control Radar Beacon System
ATE	Automated Test Equipment
ATM	Asynchronous Transfer Mode; Air Traffic Management
ATN	Aeronautical Telecommunications Network
ATS	Automatic Test Systems
AV	Air Vehicle; Aviation
AVSDWG	Aviation Subdomain Working Group
BER	Bit Error Rate
BGP	Border Gateway Protocol
BIIF	Basic Image Interchange Format
BioAPI	Biometric API
bits/s	Bits per second
B-ISDN	Broadband-Integrated Services Digital Network
BLoS	Below Line-of-Sight
BMC3	Ballistic Missile Command, Control, and Communications
BMD	Ballistic Missile Defense
BOOTP	Bootstrap Protocol
bps	Bits Per Second
BRI	Basic Rate Interface
BUFR	Binary Universal Format for Representation
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
CBEFF	Common Biometric Exchange File Format
CBR	Constant Bit Rate
CBS	Commission for Basic Systems
CC	The Common Criteria for Information Technology Security Evaluation
CCB	Change Control Board
CCDF	Common Cryptologic Data Format
CCDM	Common Cryptologic Data Model
CCEB	Combined Communications-Electronics Board
CCIB	Common Criteria Implementation 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
CDRL	Contract Data Requirements List
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
CIM	Common Information Model
CIPSO	Common Internet Protocol Security Options
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
CMI	Computer Managed Instruction
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
DEER WG	Data Element and Exchange Rule Working Group
DES	Data Encryption Standard
3DESE	Triple-DES Encryption
DHCP	Dynamic Host Configuration Protocol
DIA	Defense Intelligence Agency
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
DISSG	Data Interoperability and Standardization Steering Group
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
DMTF	Distributed Management Task Force
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
EAO	Executive Agent Office

EAP	Emergency Action Procedure
EB	Electronic Business
EC	Electronic Commerce
ECAPMO	Electronic Commerce Acquisition Program Management Office
ECN	Explicit Congestion Notification
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
EXCIMS	Executive Council for Modeling and Simulation
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
GBAS	Ground-Based Augmentation System
GeoSym	Geospatial Symbols for Digital Displays
GFE	Government Furnished Equpment
GIC	Generic Instrument Class Interface
GIF	Graphics Interchange Format
GIS	Geographic Information System
GNSS	Global Navigation Satellite 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
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/O	Input/Output
IAB	Internet Architecture Board
IATF	Information Assurance Technical Framework
IBS	Integrated Broadcast Service
IC	Intelligence Community
ICAO	International Civil Aviation Organization
ICB	Instrument Communication Bus Interface
ICD	Interface Control Document
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
IDL API	Interface Definition Language Application Program Interface
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
IMINT	Imagery Intelligence
IMT	International Mobile Telecommunications
IOSA	Integrated Overhead SIGINT Architecture
IKE	Internet Key Exchange
IP	Internet Protocol
IPC	Institute for Interconnecting and Packaging Electronic Circuits
IPCP	Internet Protocol Control Protocol
IPsec	Internet Protocol Security
IPT	Integrated Product Team
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Next Generation Version 6
IR	Infrared
IRIG	Inter-Range Instrumentation Group
IRV	International Reference Version
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)
ITOT	ISO Transport Service on Top of TCP
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

JASA	Joint Airborne SIGINT Architecture
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
KEA	Key Exchange Algorithm
kHz	Kilohertz
KMP	Key Management Protocol
KPP	Key Performance Parameters
LAAS	Local Area Augmentation System
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
LMES	List of Mandated and Emerging Standards
LOM	Learning Object Metadata
LOS	Line-of-Sight
LPI	Low Probability of Intercept
LQM	Link Quality Monitoring

LRAs	Local Registration Authorities
LSRTAP	Logic Automated Stimulus and Response (LASAR) Teradyne ASCII Post-processor (TAP)
LSB	Linux Standard Board
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
MDA	Missile Defense Agency
MDAPS	Major Defense Acquisition 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
MHS	Military Health System
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
MPLS	Multiprotocol Label Switching
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
MXF	Material Exchange Format
NAFAG	NATO Air Force Armaments Group
NAS	National Airspace System
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
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
NSGI	National System for Geospatial Intelligence
NSIF	NATO Secondary Imagery Format
NSM	Network and Systems Management
NSS	National Security Systems

NTIS	National Technical Information Service
NTISSP	National Telecommunications and Information Systems Security Policy
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
PBBE	Performance Based Business Environment
PCE	Platform Communications Element
PCI	Peripheral Computer Interface
PCIMG	PCI Industrial Computer Manufacturer's Group
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Services
PESQ	Perceptual Evaluation of Speech Quality
PHY	Physical Layer
PICS	Protocol Implementation Conformance Statement
PIDP	Programmable Interface Data Processor
PKI	Public-Key Infrastructure
PLDs	Programmable Logic Devices

PMNV/RSTA	Program Management Office for Night Vision/Reconnaissance and Target Acquisition
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
RCC	Range Commanders Council
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
RNP	Required Navigation Performance
ROHC	Robust Header Compression
RPF	Raster Product Format
RR	Resource Records
RSVP	Resource Reservation Protocol
RTCA	Radio Technical Commission for Aeronautics
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
SARPS	Standards and Recommended Practices
SAR SDE	Synthetic Aperture Radar Support Data Extension
SATCOM	Satellite Communications
SBAS	Space-Based Augmentation System
SBU	Sensitive but unclassified
SCC	Standards Coordinating Committee
SCE	Surface Communications Element
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
SDT	Surveillance Data Translator
SEDRIS	Synthetic Environment Data Representation and Interchange Specification
SEIWG	Security Equipment Integration Working Group
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
SIP	Session Initiation Protocol
SIPE	Soldier Integrated Protective Ensemble
SIPRNET	Secure Internet Protocol Router Network
SIS	Signal-in-Space
SIU	System Interface Unit
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
SOAP	Simple Object Access 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
SR	Space Reconnaissance
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]
STARS	Standard Terminal Automation Replacement System
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
TCAP	Transaction Capabilities Application Part
TCAS	Traffic Alert and Collision Avoidance System
TCDL	Tactical Common Data Link
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
TIDP-TE	Technical Interface Design Plan (Test Edition)
TIS	Technical Interface Specification
TIS	Traffic Information Service
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
TUAV	Tactical Unmanned Air Vehicle
TV	Technical View
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
UIS	User Interface Specification
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)
USIS	United States Imagery System
USM	User-based Security Model
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	UUT Test Requirements
UUT	Unit Under Test
UVMap	Urban Vector Smart Map
VACM	View-based Access Control Model
VCEG	Video Coding Expert Group
VHDL	VHSIC Hardware Description Language
VHF	Very High Frequency
VHS	Vertical Helical Scan
VHSIC	Very High Speed Integrated Circuit
VISA	Virtual Instrument Standard Architecture
VITC	Vertical Interval Time Code
VITD	VPF Interim Terrain Data
VLF	Very Low Frequency
VMap	Vector Map
VME	Virtual Memory Extended
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: 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 Technical Reference Model.	http://trm.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 Industries 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
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://jta.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/
MISB	Motion Imagery Standards Board	http://164.214.2.51/vwg/
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
NCSA	National Center for Supercomputing Applications 605 E. Springfield Avenue Champaign, IL 6182-5518 USA	http://hdf.ncsa.uiuc.edu

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/
NSGI	The National System for Geospatial Intelligence (NSGI) 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 National Imagery and Mapping 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
NTB	NITFS Technical Board	http://164.214.2.51/ntb
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

Organization	Source Location	URL
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
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/

Organization	Source Location	URL
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).	http://library.disa.mi/tafim/html
TELCORDIA	(Formerly Bellcore)	http://www.telcordia.com/
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 Interoperability Directorate (IN) TADIL Division, Code IN5	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/
USIS	See NSGI	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 C: References

- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01B, Interoperability and Supportability of National Security Systems, and Information Technology Systems, 8 May 2000.
- 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: Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), January 11, 2002.
- 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 2.0, 9 April 2001.
- 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 Industries Alliance: Electronic Design Interchange Format (EDIF), Version 4 0 0, 1996.
- 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 D: 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 prespecified 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)
- The application platform is defined as the set of resources that support the services on which application software will execute. It provides services at its interfaces that, as much as possible, make the implementation-specific characteristics of the platform transparent to the application software. (DoD TRM)

Application 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)

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)
- The means by which an application designer enters and retrieves information. (DoD TRM)

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)

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) 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.

Authentication Servers

A server designed using security measures to establish the validity of a transmission, message or originator, or a means of verifying an individual's eligibility to receive specific categories of information.

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 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 or functional responsibilities. [Joint Pub 1-02 http://www.dtic.mil/doctrine/jel/doddict]

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. Also called C2. (Joint Pub 1-02 http://www.dtic.mil/doctrine/jel/doddict)

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. Also called C4 systems. (Joint Pub 1-02 http://www.dtic.mil/doctrine/jel/doddict)

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)

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)

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).

Cryptographic Algorithms

An algorithm that employs the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms.

Cryptographic APIs

The source code formats and procedures through which an application program accesses cryptographic services, which are defined abstractly compared to their actual implementation.

Cryptographic Modules

A set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the module's cryptographic boundary, which is an explicitly defined contiguous perimeter that establishes the physical bounds of the module.

Cryptographic Key Algorithms

An algorithm that develops a sequence of symbols that controls the operations of encipherment and decipherment

Cryptographic Tokens

A portable, user controlled, physical device used to store cryptographic information and possibility perform cryptographic functions.

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).

Directory Service

A Directory Service provides names, locations and other information about people and organizations. In a LAN or WAN, this directory information may be used for e-mail addressing, user authentication (e.g., logins and passwords), or network security (e.g., user-access rights). A directory may also contain information on the physical devices on a network (e.g., PCs, servers, printers, routers and communication servers) and the services available on a specific device (such as operating systems,

applications, shared-file systems, print queues). This information may be accessible to computer applications as well as being eye-readable for end users.

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)

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: <https://www.dmso.mil/public>.

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: <https://www.dmso.mil/public>.

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: <https://www.dmso.mil/public>.

Firewall

A system or combination of systems that enforces a boundary between two or more networks.

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.).

Guards

Highly assured devices that negotiate the transfer of data between enclaves operating at different security levels.

Hash

The Hash function provides a check for data integrity.

Hash Algorithms

Algorithms developed to compute values using parity or hashing for information requiring protection against error or manipulation.

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 <https://www.dmso.mil/public>.

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)

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 http://www.dtic.mil/doctrine/jel/doddict)

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.

Internet Protocol Security Services

Services that provide specific security architecture and protocols that provide security services for Internet Protocol traffic.

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.

Intrusion Detection System

An intrusion is an attempt to break into or misuse your system. An intrusion detection system, attempts to detect an intruder breaking into your system or a legitimate user misusing system resources. The intrusion detection system should run constantly on your system, working away in the background, and only notifying you when it detects something it considers suspicious or illegal. What is suspicious or illegal depends on the security policy you have established for the system.

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 http://www.dtic.mil/doctrine/jel/doddict] [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.

Key Management Infrastructure

The process of handling and controlling cryptographic keys and related material (such as initialization values) during their life cycle in a cryptographic system, including ordering, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying material.

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)

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)

Link Layer

Layer 2 of the OSI 7 Layer Reference Model where a point-to-point communication channel connecting two sub-network relays is established. From ISO 7498, the OSI Reference Model: The Data Link Layer provides functional and procedural means for connectionless mode among network entities, and for connection mode for the establishment, maintenance, and release data-link-connections among network entities and for the transfer of data-link service data units. A data-link connection is built upon one or several physical-connections. The Data Link Layer detects and possibly corrects errors that may occur in the Physical Layer. In addition, the Data Link Layer enables the Network Layer to control the interconnection of data circuits within the Physical Layer.

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.

Naming Service

A Naming Service is used to construct large, enterprise-wide naming graphs where Naming Contexts model "directories" or "folders" and other names identify "document" or "file" kinds of objects. In other words, the naming service is used as the backbone of an enterprise-wide filing system. The Naming Service provides the principal mechanism through which most clients of an Object Request Broker-based system locate objects that they intend to use (make requests of).

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>.

Network Management

In simple terms, network management may be defined as the capability to track, monitor and control network resources across an entire network (i.e., in the core, edge, and access portions of the network).

Effective network management solutions should include the following:

- Fault management, to quickly identify potential network problems
- Configuration management, which involves changing network and user configurations to optimize network performance and productivity
- Performance management, for tracking important network events, projecting future upgrade requirements and troubleshooting
- Accounting management, to track and bill network users for their services and software
- Security management, to protect the network from unauthorized access to critical business data.

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: <https://www.dmso.mil/public>.

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 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)

See 1.5.1.

Passwords

Protected/private character string used to authenticate an entity or to authorize access to data.

Physical Layer

Layer 1 of the OSI 7 Layer Reference Model where a communication path is established in the physical media for Open System Interconnections among two or more physical-entities, together with the facilities necessary in the Physical Layer for the transmission of bits on it. The Physical Layer provides the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical-connections for bit transmission between data-link entities. A physical connection may involve intermediate open systems, each relaying bit transmission within the Physical Layer. Physical Layer entities are interconnected by means of a physical medium.

PKI Certificates

Digital certificates that bind a system entity's identity to a public-key value, and possibility to additional data items; a digitally signed data structure that attests to the ownership of a public-key.

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)

Practice

A recommended implementation or process that further clarifies the implementation of a standard or a profile of a standard.

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.

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)

Public Key Cryptography

The asymmetric cryptography used to support the Public Key Infrastructure, which is a system of Certificate Authorities that perform some set of certificate management, archive management, key management, and token management functions for a community of users.

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.

Real-Time Control System

Systems capable of responding to external events with negligible delays.

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 http://www.dtic.mil/doctrine/jel/doddict)

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).

Remote Access

The ability for a user to log in to a server from a remote location. For security, the user must first be authenticated before gaining access.

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://www.dmso.mil/public>.

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.

Security Algorithms

Algorithms developed to ensure message source authenticity and integrity.

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 at <https://www.dmso.mil/public>.

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)

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 http://www.dtic.mil/doctrine/jel/doddict)

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.
- An integrated composite of people, products, and processes that provides a capability or satisfies a stated need or objective.

Systems Architecture (SA)

See 1.5.3.

Technical Architecture (TA)

See 1.5.2.

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.

Virtual Private Networks

A way of using a public network (typically the Internet) to provide a restricted-use logical computer network to link two sites of an organization.

Virus Code Detection

A system that can detect a virus which is a program or code that replicates, that is infects another program, boot sector, partition sector or document that supports macros by inserting itself or attaching itself to that medium. Most viruses just replicate, a lot also do damage.

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 http://www.dtic.mil/doctrine/jel/doddict) See also National Security Systems.

Page intentionally left blank.