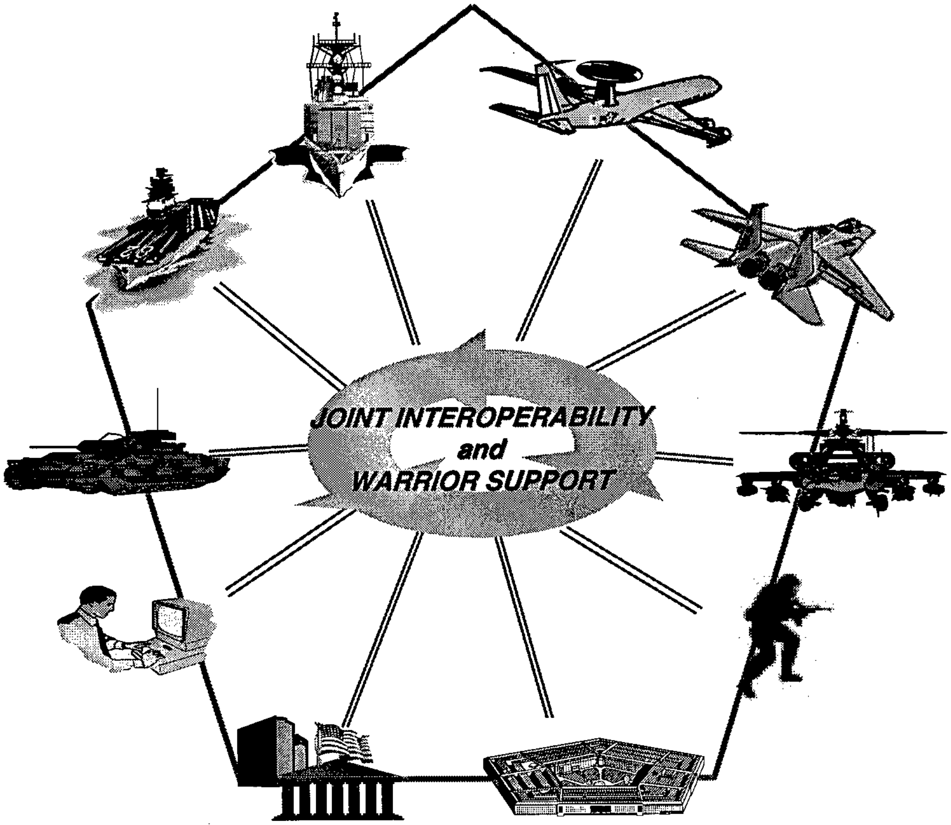
Department of Defense
Joint Technical Architecture



Version 2.0

26 May 1998

19980805 050

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited

AQ I98-10-2169

DTIC QUALITY INSPECTED 1

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Department of Defense Joint Technical Architecutre, Version 2.0

B. DATE Report Downloaded From the Internet: 29 July 98

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #: JTA is a Collaborative effort, Conducted by the JTA Development Group JTADG)

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by: DTIC-OCA, Initials: __PM__ Preparation Date: 29 July 98

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

ok
Tom

AQ I98-10-2169

This page intentionally left blank.

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 the recent conflicts of Desert Shield/Desert Storm have resulted in a new vision for the Department of Defense (DoD). Joint Vision 2010 (JV2010) is the conceptual template for how America's Armed Forces will channel the vitality and innovation of our people, and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting. The DoD Joint Technical Architecture (JTA) is crucial to achieving JV2010.

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. Wherever possible, they are commercially supported, and validated off-the-shelf commercial implementations from multiple vendors are available. Standards and guidelines that do not yet meet these criteria, but are expected to mature to meet them in the near-term, 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 Annexes. The JTA core contains the minimum set of JTA elements applicable to all DoD systems to support interoperability. The JTA Annexes contain additional JTA elements applicable to specific functional domains (families of systems). These elements are needed to ensure interoperability of systems within each domain, but may be inappropriate for systems in other domains. The current version of the JTA, JTA Version 2.0, was extended to include Annexes for: the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) domain; the Combat Support domain; the Modeling and Simulation domain; and the Weapon Systems domain. Where subsets of an application domain (subdomains) have special interoperability requirements, the JTA includes Subdomain Annexes containing JTA elements applicable to systems within that subdomain. The intention is that a system within a specific subdomain shall adopt the JTA elements contained in the relevant Subdomain Annex, the JTA elements contained in the parent Domain Annex, 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 the DoD's Specification and Standards Reform; Implementation of the Information Technology Management Reform Act (ITMRA); Defense Modeling and Simulation Initiative; Evolution of the DoD TRM; Defense Information Infrastructure Common Operating Environment (DII COE); and Open Systems Initiative.

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

DTIC QUALITY INSPECTED 1

TABLE OF CONTENTS

COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) DOMAIN ANNEX

AIRBORNE RECONNAISSANCE SUBDOMAIN ANNEX FOR THE C4ISR DOMAIN

COMBAT SUPPORT DOMAIN ANNEX

AUTOMATIC TEST SYSTEMS SUBDOMAIN ANNEX FOR THE COMBAT SUPPORT DOMAIN

MODELING AND SIMULATION DOMAIN ANNEX

WEAPON SYSTEMS DOMAIN ANNEX

AVIATION SUBDOMAIN ANNEX FOR THE WEAPON SYSTEMS DOMAIN

GROUND VEHICLE SUBDOMAIN ANNEX FOR THE WEAPON SYSTEMS DOMAIN

MISSILE DEFENSE SUBDOMAIN ANNEX FOR THE WEAPON SYSTEMS DOMAIN

SECTION 1: JTA OVERVIEW

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

As shown in Figure 1-1, Warfighters must be able to work together within and across Services in ways not totally defined in today's operational concepts and/or architectures. They must be able to obtain and use intelligence from national and theater assets that may be geographically dispersed among national and international locations. 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 flows quickly and seamlessly among DoD's sensors, processing and command centers, and shooters to achieve dominant battlefield awareness, and move inside the enemy's decision loop.

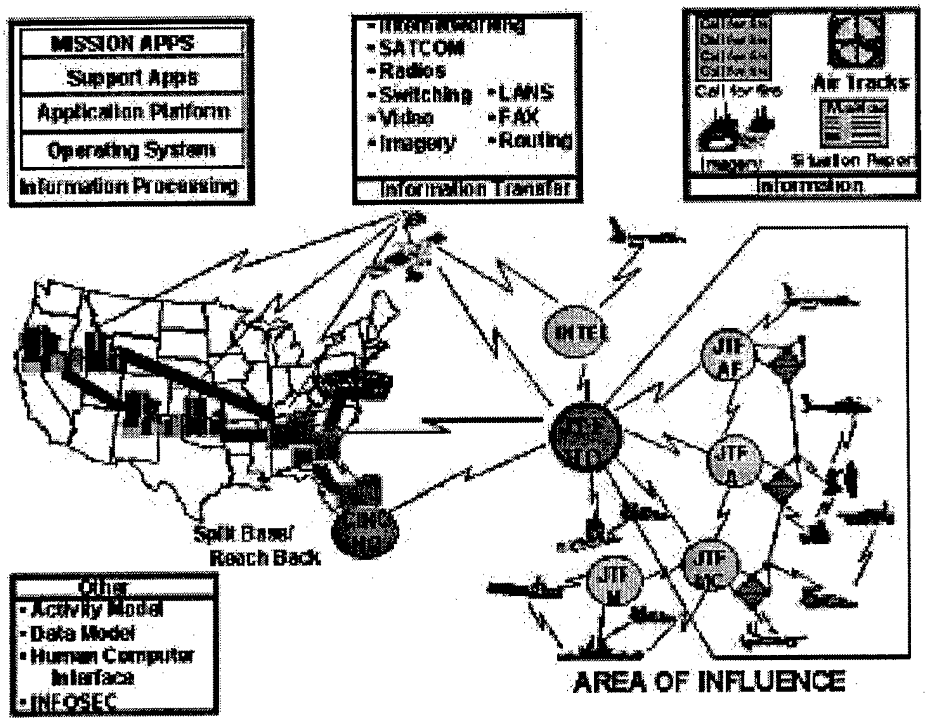


Figure 1-1 DoD Warfighter Information Technology Environment

The Joint Technical Architecture (JTA) provides the minimum set of standards that, when implemented, permits this flow of information in support of the Warfighter. As shown in Figure 1-1, there must be:

- A distributed information processing environment in which applications are integrated.
- Applications and data independent of hardware to achieve true integration.
- Information transfer assets to ensure seamless communications within and across diverse media.
- Information in a common format with a common meaning.
- Common human-computer interfaces for users, and effective means to protect the information.

The current JTA concept is focused on the interoperability and standardization of information technology (IT). However, the JTA concept lends itself to application in other technology areas, when required to support IT interoperability requirements.

1.1 INTRODUCTION TO THE JOINT TECHNICAL ARCHITECTURE

This section 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.

1.1.1 Purpose

A foremost objective of the JTA is to improve and facilitate the ability of our systems to support joint and combined operations in an overall investment strategy.

The DoD JTA:

- Provides the foundation for interoperability among all tactical, strategic, and combat support systems.

- Mandates interoperability standards and guidelines for system development and acquisition that will facilitate joint and coalition force operations. These standards are to be applied in concert with DoD Standards Reform.
- Communicates to industry the DoD's intent to consider open systems products and implementations.
- Acknowledges the direction of industry's standards-based development.

1.1.2 Scope

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, and commercial product availability. The scope of JTA Version 2.0 includes information technology and information technology-related standards in the DoD systems that may exchange information or services across a joint, functional, or organizational boundary. Information technology (IT) means any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. IT includes computers, communications systems, ancillary equipment, software, firmware, and their related procedures, services (including support services), and related resources.

The JTA is critical to achieving the envisioned objective of a cost-effective, seamless integration environment; achieving and maintaining this vision requires interoperability:

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

1.1.3 Applicability

This version of the DoD JTA mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. The JTA shall be 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 shall be cognizant of the JTA in developing requirements and functional descriptions. System developers shall use the JTA to facilitate the achievement of interoperability for new and upgraded systems (and the interfaces to such systems). System integrators shall use it to foster the integration of existing and new systems.

The JTA will be updated periodically with continued DoD Component participation. Future versions of the JTA will extend the Version 2.0 scope in two dimensions: into other functional domains and into other technology areas. Version 2.0 begins the functional expansion by moving beyond the C4I domain to include other DoD domains.

1.1.4 Background

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

Joint Vision 2010 (JV 2010) creates a broad framework for understanding joint warfare in the future, and for shaping Service programs and capabilities to fill our role within that framework. JV 2010 defines four operational concepts - Precision Engagement, Dominant Maneuver, Focused Logistics, and Full Dimensional Protection. These concepts combine to ensure American forces can secure Full Spectrum Dominance - the capability to dominate an opponent across the range of military operations and domains. Furthermore, Full Spectrum Dominance requires Information Superiority, 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 (ASD) Command, Control, Communications, and Intelligence (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 towards interoperability."

A Joint Technical Architecture Working Group (JTAWG), chaired by ASD (C3I), C4I Integration Support Activity (CISA), was formed and its members agreed to use the 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 Under Secretary of Defense, Acquisition 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)/CISA and USD (A&T) Open Systems Joint Task Force (OS-JTF). The applicability of Version 2.0 of the JTA is expanded to include the information technology in all DoD systems.

1.1.5 Architectures Defined

DoD has many efforts underway in support of the Warfighters' environment, one of which is the development and maintenance of the Joint Technical Architecture. In addition, other efforts are defining and consolidating DoD Architecture guidance through work in the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework and the evolution of the Technical Architecture Framework for Information Management (TAFIM). Work is currently being done at the DoD level to consolidate the guidance currently contained in the C4ISR Architecture Framework, the TAFIM, and other pertinent documents.

The C4ISR Architecture Framework 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. As such, the development of the JTA aligns with the intended products and presentation schemes depicted in the C4ISR Architecture Framework. The C4ISR Architecture Framework document defines the process of developing systems within the construct of the three architectures defined. The content and structure of the JTA takes its definition from the C4ISR Framework.

An architecture is defined by the Institute for Electrical and Electronics Engineers (IEEE) in IEEE 610.12A-1990 as the structures or 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 architectures: Operational, Systems, and Technical. Figure 1-2 shows the relationship among the three architectures. The definitions are provided here to ensure a common understanding of the three architectures[1].

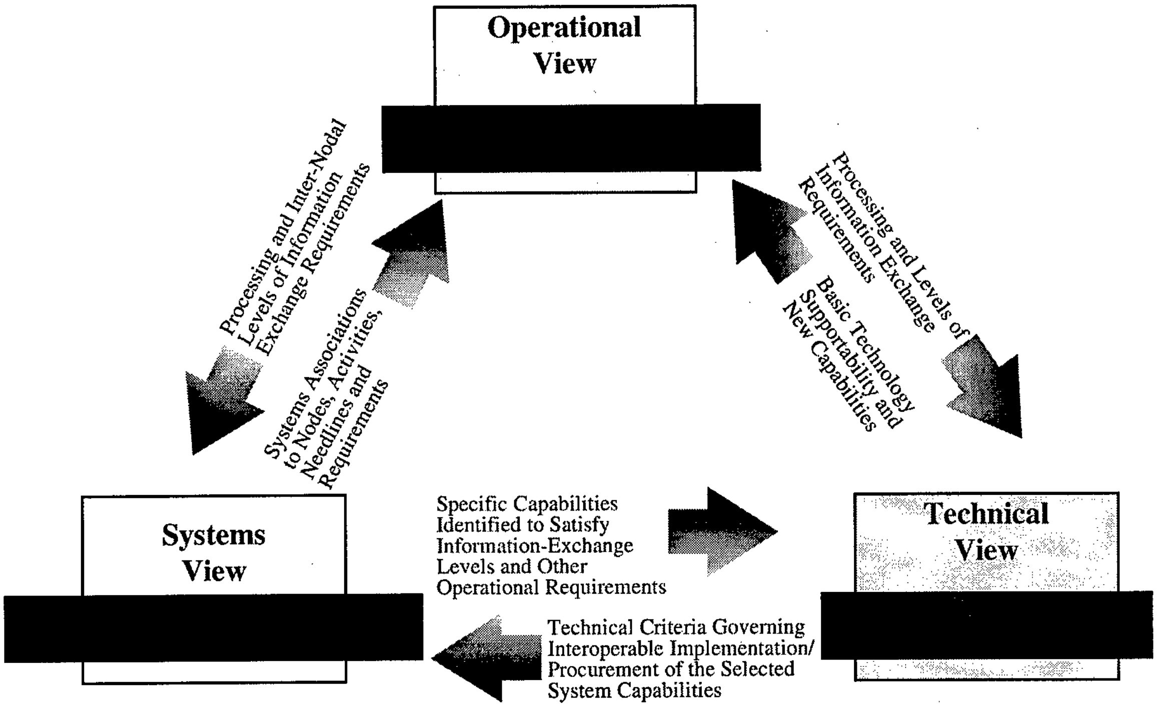

Operational View
[redacted]
Processing and Inter-Nodal Levels of Information Exchange Requirements
Systems Associations to Nodes, Activities, Needlines and Requirements
Processing and Levels of Information Exchange Requirements
Basic Technology Supportability and New Capabilities
Systems View
[redacted]
Specific Capabilities Identified to Satisfy Information-Exchange Levels and Other Operational Requirements
Technical Criteria Governing Interoperable Implementation/ Procurement of the Selected System Capabilities
Technical View
[redacted]

Figure 1-2 Architecture Relationships

1.1.5.1 Operational Architecture (OA) View

The operational architecture 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.

1.1.5.2 Technical Architecture (TA) View

The technical architecture view is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

The technical architecture view provides the technical systems-implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The technical architecture view includes a collection of the technical standards, conventions, rules and criteria organized into profile(s) that govern system services, interfaces, and relationships for particular systems architecture views and that relate to particular operational views.

[1] 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.

1.1.5.3 Systems Architecture (SA) View

The systems architecture view is a description, including graphics, of systems[2] and interconnections[3] providing for, or supporting, warfighting functions.

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

1.2 DOCUMENT ORGANIZATION

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

1.2.1 General Organization

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

- Introduction - This subsection is for information purposes only. It defines the purpose and scope of the subsection and provides background descriptions and definitions that are unique to the section.
- Mandates - This subsection identifies mandatory standards or practices. Each mandated standard or practice is clearly identified on a separate bulletized line and includes a formal reference citation that is suitable for inclusion within Requests for Proposals (RFP), Statements of Work (SOW) or Statements of Objectives (SOO).
- Emerging Standards - This subsection provides an information-only description of standards which are candidates for possible addition to the JTA mandate. The purpose of listing these candidates is to help the program manager determine those areas that are likely to change in the near term (within three years) and suggest those areas in which "upgradability" should be a concern. The expectation is that emerging standards will be elevated to mandatory status when implementations of the standards mature. Emerging standards may be implemented, but shall not be used in lieu of a mandated standard.

1.2.2 Information Technology Standards

Section 2, also called the JTA core or main body, addresses commercial and Government standards common to most DoD information technology, grouped into categories; Information Processing Standards; Information Transfer Standards; Information Modeling, Metadata, and Information Exchange Standards; Human-Computer Interface Standards; and Information Systems Security Standards. Each category addresses a set of functions common to most DoD IT systems.

1.2.3 Domain and Subdomain Annexes

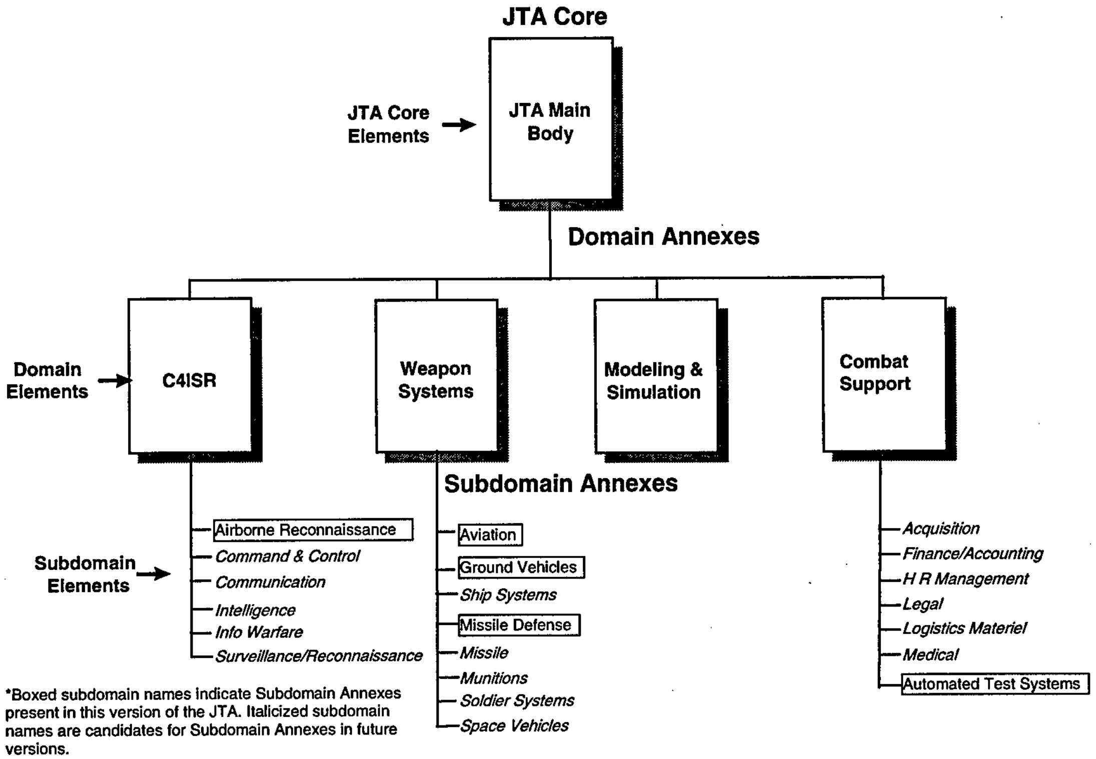
The JTA core contains the common service areas, interfaces and standards (JTA elements) applicable to all DoD systems to support interoperability. Recognizing that there are additional JTA elements common

[2] Systems: People, machines, and facilities organized to accomplish a set of specific functions, which cannot be further subdivided while still performing required functions. Includes the radios, terminals, command, control, and support facilities, sensors and sensor platforms, automated information systems, etc., necessary for effective operations.

[3] 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.

within families of related systems (i.e., domains), the JTA adopted the Domain and Subdomain annex notion. A domain represents a grouping of systems sharing common functional, behavioral and operational requirements. JTA Domain and Subdomain annexes are intended to exploit the common service areas, interfaces and standards supporting interoperability across systems within the domain/subdomain.

The JTA Domain Annexes contain 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. Domains 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. Subdomain Annexes contain 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 Annex. The relationships between the JTA core, Domain Annexes, and Subdomain Annexes currently included in the JTA are illustrated in Figure 1-3.



*Boxed subdomain names indicate Subdomain Annexes present in this version of the JTA. Italicized subdomain names are candidates for Subdomain Annexes in future versions.

Figure 1-3 JTA Hierarchy Model

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 annex.

As shown in Figure 1-3, the following Domain and Subdomain annexes are currently populated:

Domain Annexes:

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

Subdomain Annexes:

- Airborne Reconnaissance (AR).
- Automated Test Systems (ATS).
- Missile Defense (MD).
- Ground Vehicles (GV).
- Aviation (AV).

The goal is to build on these annexes by incorporating the requirements of additional domains and subdomains. Each Annex includes an introduction clearly specifying the purpose, scope, description of the domain, and background of the annex. As necessary, each annex provides a list of domain specific standards and guidance in a format consistent with the JTA core. Annexes generally use the TAFIM DoD Technical Reference Model (TRM) defined in Section 2.1.3.1, but may include a different or expanded model. Annex developers should define which standards apply to which system interfaces in their domain. They may address emerging standards that are of interest to the domain.

1.2.4 Appendices (Appendix A, B, C)

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

Appendix A, "Acronyms and Glossary", includes an acronym list and glossary of terms referenced in the JTA.

Appendix B, "List of Mandated Standards and Sources", includes "retired," "mandated," and "emerging" standards for each JTA service area; and a list of organizations from whom documents cited in the JTA may be obtained.

Appendix C, "JTA Relationship to DoD Standards Reform", describes the relationship of the JTA to the DoD Standards Reform begun in June 1994 and addresses the relevance of the reform waiver policy to the JTA.

1.3 KEY CONSIDERATIONS IN USING THE JTA

In general, the JTA shall be used to determine the specific service areas and standards for implementation within new or upgraded systems. However, there are several key considerations in using the JTA.

The JTA service areas are based on the DoD TRM. For a more complete description of the DoD TRM and service areas refer to Section 2.1.3.1.

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

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

If cited, requirements documents not identified in the JTA should complement and not conflict with the JTA core, and applicable Domain and Subdomain Annexes.

1.4 ELEMENT NORMALIZATION RULES

As the JTA evolves, the JTA elements contained in the JTA core, Domain Annexes and Subdomain Annexes will need to be periodically revisited and updated to ensure correctness. The JTA normalization rules in this section address the movement of elements across the core or annexes following the definitions and scope.

All standards are placed in the core unless they are justified as unacceptable to meet domain-specific requirements. When core standards cannot meet the requirements of a specific domain, JTA elements are removed from the JTA core and placed in the appropriate Domain Annex(es). Likewise, when domain standards cannot meet subdomain-specific requirements, those will be removed from the Domain Annex and placed in the appropriate Subdomain Annex(es).

The intent of the above normalization rules is as follows. (1) The core applies to all DoD systems. (2) The JTA core contains selected standards for as many JTA services as possible. (3) A service area provides the minimum number of alternative standards applicable to DoD.

Figure 1-3 also illustrates a notional hierarchy of JTA core, domains and subdomains – as defined by the Committee on Open Electronic Standards (COES) [Committee on Open Electronic Standards (COES) Report, DoD Open Systems-Joint Task Force (OS-JTF), July 1996], and tailored by the Joint Technical Architecture Development Group.

1.5 JTA RELATIONSHIP TO DOD STANDARDS REFORM

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

The JTA implements standards reform by selecting the minimum standards necessary to achieve joint interoperability. The JTA mandates commercial standards and practices to the maximum extent possible. Use of JTA mandated standards or specifications in acquisition solicitations will not require a waiver from standards reform policies. All mandatory standards in the JTA are of the types that have been identified by the DoD Standards Reform as waiver-free or for which an exemption has already been obtained. Additional information on this topic can be found in Appendix C.

1.6 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 SOURCES:** 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.

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.

1.7 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. The following organizations have voting memberships in both groups:

JTA VOTING MEMBERSHIP LIST
Assistant Secretary of Defense Command, Control, Communications and Intelligence/C4I Integration Support Activity (ASD (C3I)/CISA)
Ballistic Missile Defense Organization (BMDO)
Defense Airborne Reconnaissance Office (DARO)
Defense Information Systems Agency (DISA)
Defense Intelligence Agency/DoD Intelligence Information Systems (DIA/DoDIIS)
Defense Logistics Agency (DLA)
Defense Modeling and Simulation Office (DMSO)
Joint Staff/J6
National Imagery and Mapping Agency (NIMA)
National Reconnaissance Office (NRO)
National Security Agency (NSA)
US. Air Force (USAF)
US. Army (USA)
US. Marine Corps (USMC)
US. Navy (USN)
Under Secretary of Defense for Acquisition and Technology Open Joint Systems Task Force (USD (A&T) OS-JTF)

The JTA Management Plan describes the process by which the JTA will be configuration managed. This document, as well as the charter for the JTADG, may be found on the Defense Information Systems Agency (DISA) Center for Standards (CFS) JTA World Wide Web home page:

http://www-jta.itsi.disa.mil

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

Industry and other non-DoD comments and suggested changes should be submitted through DISA CFS via electronic mail to **jta-comment@www.disa.mil**. All comments and suggested changes must be in the standard comment format described on the JTA World Wide Web home page.

This page intentionally left blank.

SECTION 2: INFORMATION TECHNOLOGY STANDARDS

2.1 GENERAL

2.1.1 Background

Section 2 of the JTA is essentially a technical refreshment of Version 1.0 of the JTA. This section is intended as the basis from which to develop the main body of the JTA (i.e., the JTA core). As the JTA evolves, the structure of this section will also evolve to be more reflective of the goal of the JTA structure.

2.1.2 Scope

This section of the JTA establishes the minimum set of rules governing information technology within DoD systems. The scope includes standards for information processing, information transfer, the structure of information and data, human-computer interface standards for information entry and display, and information security standards. Information technology includes 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.

2.1.3 DoD Technical Architecture Framework for Information Management

The Technical Architecture Framework for Information Management (TAFIM) version 3.0 is a set of eight volumes consisting of very specific guidance on building and maintaining DoD systems architectures. It describes the process for defining a technical architecture. Volume 2, the Technical Reference Model, as described below and referenced as the TAFIM DoD TRM, is the basis for the structure and standards selected for Section 2 of the JTA.

For applicable systems, the specific guidance in the JTA replaces the general standards guidance in the TAFIM 3.0, Volume 7: Adopted Information Technology Standards (AITS).

2.1.3.1 TAFIM DoD Technical Reference Model

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

The model is partitioned into the following: Application Software Entity that includes both mission area and support applications; Application Platform Entity that contains the system support services and operating system services; External Environment; and a number of interfaces. The interfaces provide support for a wide range of applications and configurations, and consist of the following: Application Program Interfaces (APIs), and External Environment Interfaces (EEIs).

The following JTA core services are contained within the DoD TRM's application platform entity:

Software Engineering Services
User Interface Services
Data Management Services
Data Interchange Services
Graphic Services
Communications Services

Security Services
System Management Services
Distributed Computing Services
Internationalization Services
Operating System Services

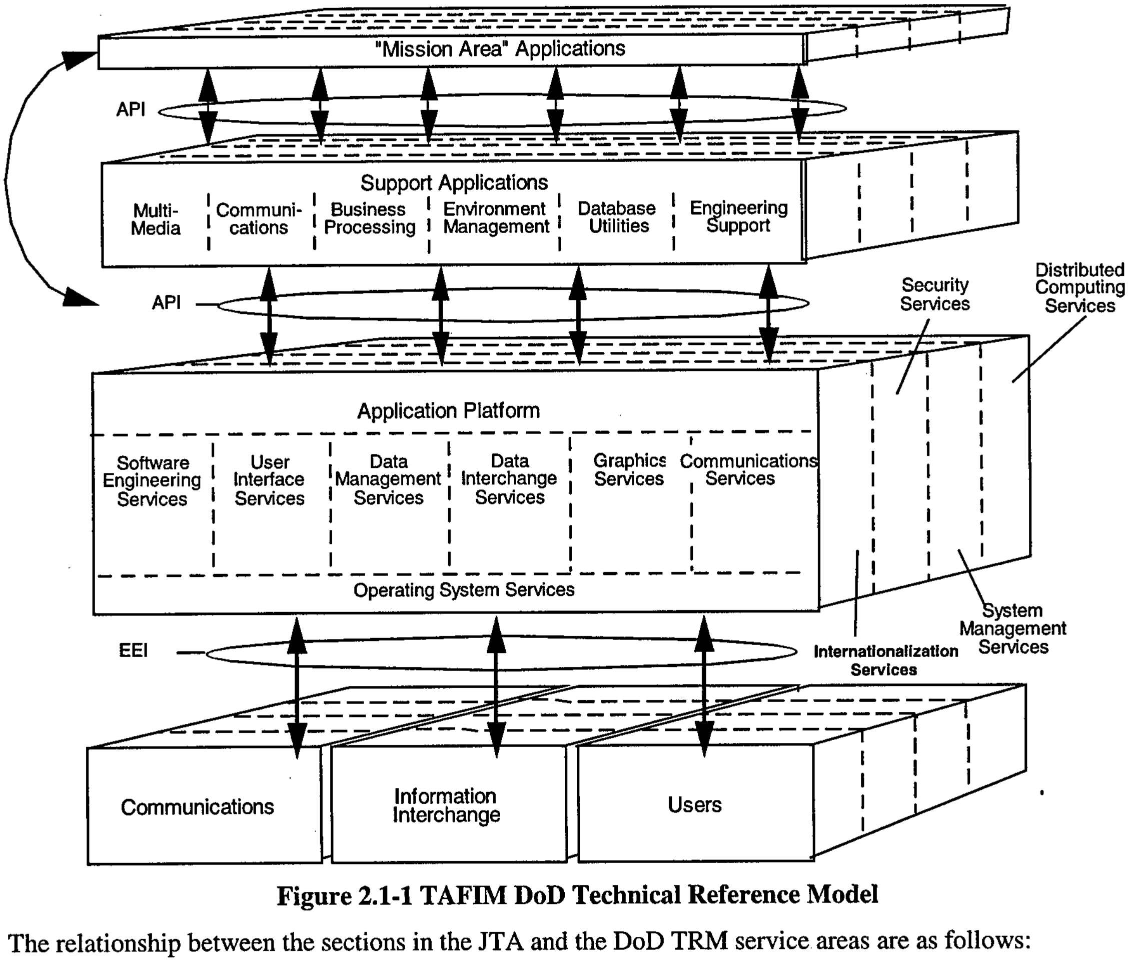


Figure 2.1-1 TAFIM DoD Technical Reference Model

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

Section 2.2, Information Processing Standards, specifies standards for the User Interface (2.2.2.2.1.2), Data Management (2.2.2.2.1.3), Data Interchange (2.2.2.2.1.4), Graphics (2.2.2.2.1.5), Operating System (2.2.2.2.1.7), Internationalization (2.2.2.2.2.1), and Distributed

Computing (2.2.2.2.2.4) service areas, and the latter's two subordinate paragraphs become 2.2.2.2.2.4.1 and 2.2.2.2.2.4.2 respectively. This section also references, but does not specify any standards for the Software Engineering (2.2.2.2.1.1), Communications (2.2.2.2.1.6), Security (2.2.2.2.2.2), and System Management (2.2.2.2.2.3) service areas.

Section 2.3, Information Transfer Standards, specifies standards for the Communications (2.3.2.1 through 2.3.2.3) and System Management (2.3.2.4) service areas applicable to both system and network management.

Section 2.4, 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 DoD TRM.

Section 2.5, Human-Computer Interface Standards, addresses standards for what is often referred to as TAFIM Volume 8, Version 3.0. The standards specified in Section 2.5 complement those cited for User Interface Services in Section 2.2.2.2.1.2.

Section 2.6, Information Systems Security Standards, specifies security standards that are relevant to the service areas discussed in Sections 2.2, 2.3, and 2.5.

In this version of the JTA, the DoD TRM does not embrace all service areas within the weapon systems domain, and is applicable to the JTA core as described above. In cases where new services are identified, they should be presented to the Technical reference Model Working Group (TRMWG) for adjudication and potential inclusion into the TRM.

2.1.3.2 Emerging "Integrated" DoD Technical Reference Model

To support a more extensive, dynamic and complete set of JTA services, interfaces and platform configurations, an "integrated" DoD TRM (I-DoD TRM) has been developed (Figure 2.1-2). This TRM represents an enhancement to, and uses as a foundation, the TAFIM DoD TRM structure, service features and definitions (as defined in TAFIM Version 3.0, Volume 2, DoD Technical Reference Model). The model also derives interface features that have been identified as essential from the Society of Automotive Engineers (SAE) Generic Open Architecture (GOA) model and other derived models used by certain segments of the Weapons community to support their real-time needs. Thus, the enhanced "integrated" model combines the best of service/interface capabilities and definitions from several existing models. It has the added advantage of providing greater detail in the Application Software and External Environment Entity levels, and is tailorable to accommodate different DoD users and performance needs, both hardware and real-time. Interfaces are defined in Table 2.1-1. The "integrated" model is defined in its entirety in the emerging document, DoD Technical Reference Model, Version 1.0 Draft, dated April 1998.

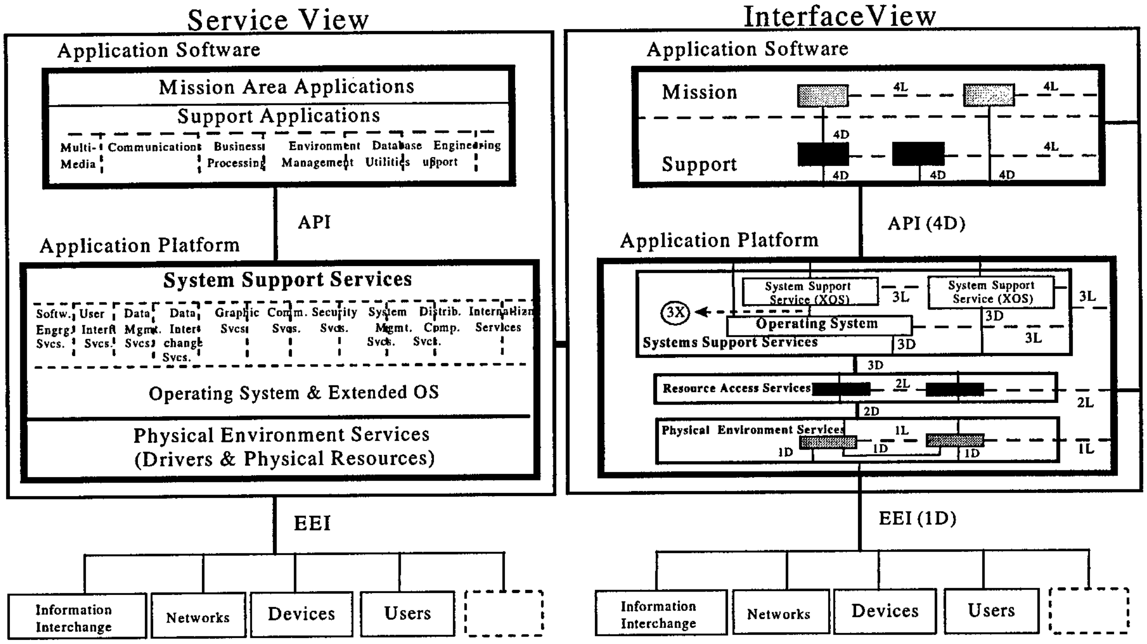


Figure 2.1-2 Integrated DoD Technical Reference Model

Table 2.1-1 Interface Translation Table

Interface Type	Definition
1D	Physical Resources Direct
1L	Physical Resource 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

The I-DoD TRM is directly mappable to both the TAFIM DoD TRM services and the interface categories of the GOA model. Transition to and usage of the I-DoD TRM should present no barriers to any current user of existing DoD models (e.g., TAFIM or GOA). DoD ownership of the model, together with its flexibility, will enable it to keep pace with newly emerging service and interface needs ongoing within DoD.

The "integrated" model is currently overseen by the DoD Technical Reference Model Working Group (TRMWG). The TRMWG is a JTA chartered support group assigned to the DISA Center for Standards. The TRMWG's membership is diverse and composed of the various DoD communities (C4ISR, Weapon Systems, Services, Agencies, and Defense Contractors) requiring a model to support and adjudicate their interoperability and open system needs. The resulting model is consensus driven and viewed as evolutionary to enable it to remain current with emerging DoD needs. The model is consistent with and will continue to support other programs (e.g., the DII COE - see section 2.1.4.2) in addition to the JTA. Upon formal release, the enhanced TRM document together with the JTA is to be used for defining the target technical environment for DoD information technology needs. The I-DoD TRM document, when approved, will supersede the existing TAFIM Version 3.0, Volume 2, DoD TRM.

2.1.4 Mandates

2.1.4.1 Year 2000 (Y2K) Compliance

To ensure proper data interchange beyond the year 2000, it is DoD policy that all new software and data acquired by the DoD shall be Year 2000 (Y2K) compliant. "Year 2000 compliant" means information technology that accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations. Furthermore, Year 2000 compliant information technology, when used in combination with other information technology, shall accurately process date/time data if the other information technology properly exchanges date/time data with it.[1] Refer to JTA Section 2.4 for guidance on specific date data formats to be used.

DoD policy guidance on this matter can be found in the "DoD Year 2000 Management Plan." The plan is available on the World Wide Web at:

http://www.dtic.mil/c3i/

For procurement and acquisition purposes, the General Services Administration (GSA) has made available the following documents:

1. "Recommended Year 2000 Contract Language (1996-09-11)"
2. "Federal Acquisition Regulation Interim Rule on the Year 2000 (1997-01-02)"

These documents can be used by contracting officers to help ensure that acquired products and services are Y2K compliant. They are available on the GSA World Wide Web site at:

http://www.itpolicy.gsa.gov/

2.1.4.2 Defense Information Infrastructure Common Operating Environment (DII COE)

The Common Operating Environment (COE) concept is described in the Integration and Runtime Specification (I&RTS), Version 3.0, 1 July 1997. The Defense Information Infrastructure COE (DII COE) is implemented with a set of modular software that provides generic functions or services, such as operating system services. These services or functions are accessed by other software through standard APIs. The DII COE may be adapted and tailored to meet the specific requirements of a domain. COE Implementations provide standard, modular software services that are consistent with the service areas identified in the DoD Technical Reference Model. Application programmers then have access to these software services through standardized APIs.

The DII COE, as defined in the DII COE I&RTS Version 3.0, is fundamental to a Joint System Architecture (JSA). In the absence of a JSA, the JTA mandates that all Command, Control, Communications, Computers, and Intelligence (C4I) systems shall use the DII COE. The strict definition of C4I, as given in JTA 1.0, is expanding to cover information technology areas that cut across JTA Version 2.0 domain boundaries. The DII COE mandate is therefore intended for all applicable systems. All applications of a system which must be integrated into the DII shall be at least DII COE I&RTS level 5 compliant (software is segmented, uses DII COE Kernel, and is installed via COE tools) with a goal of achieving level 8.

[1] August 1, 1997 Interim FAR Rule on Year 2000 Compliance

The DII COE implements the appropriate JTA standards applicable to the COE functionality. The DII COE implementation will continue to evolve in compliance with all applicable JTA specifications, standards, and source references. Additional functionality not contained in the DII COE is subject to the JTA mandate.

2.1.5 Organization of Section 2

The Information Technology section of the JTA consists of six sections. The first section is the overview. The next sections are: (2.2) Information Processing Standards; (2.3) Information Transfer Standards; (2.4) Information Modeling, Metadata, and Information Exchange Standards; (2.5) Human-Computer Interface Standards; and (2.6) Information Systems Security Standards.

Information Processing Standards - Section 2.2 describes government and commercial information processing standards the DoD shall use to develop integrated, interoperable systems that meet the Warfighters' information processing requirements.

Information Transfer Standards - Section 2.3 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 2.4 describes the use of integrated information modeling and mandates applicable standards. Information modeling consists of Activity and Data Modeling. This section explains the use of the DoD Command and Control (C2) Core Data Model (C2CDM) and the Defense Data Dictionary System (DDDS), formerly the Defense Data Repository System (DDRS). This section also mandates information standards including message formats.

Human-Computer Interface Standards - Section 2.5 provides a common framework for Human-Computer Interface (HCI) design and implementation in DoD systems. The objective is the standardization of user interface implementation options, enabling DoD applications to appear and behave in a reasonably consistent manner. The section specifies HCI design guidance, mandates, and standards.

Information Systems Security Standards - Section 2.6 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 2.2 through 2.5. Section 2.6 is structured to mirror the overall organization of the JTA so that readers can easily link security topics with the related JTA subject areas.

2.2 INFORMATION PROCESSING STANDARDS

2.2.1 Introduction

2.2.1.1 Purpose

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

2.2.1.2 Scope

This section applies to mission area, support application, and application platform service software. This section does not cover communications standards needed to transfer information between systems (defined in Section 2.3), nor standards relating to information modeling (process, data, and simulation), data elements, or military unique message set formats (defined in Section 2.4).

2.2.1.3 Background

Information Processing (IP) standards provide the data formats and instruction processing specifications required to represent and manipulate data to meet information technology (IT) mission needs. The standards in this section are drawn from widely accepted commercial standards that meet DoD requirements. Where necessary for interoperability, profiles of commercial standards are used. Military standards are mandated only when suitable commercial standards are not available.

2.2.2 Mandates

The following sections provide the applicable mandated standards that shall be used for the selection of commercial or government off-the-shelf (GOTS) software or in the development of government software. Appendix B contains a table that summarizes the mandated standards from this section, as well as providing information on how to obtain the standards.

2.2.2.1 Application Software Entity

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

Common support applications are those (e.g., e-mail and word processing) that can be standardized across individual or multiple mission areas. The services they provide can be used to develop mission-area-specific applications or can be made available to the user. The DoD Technical Reference Model (TRM) defines six support application categories: Multimedia, Communications, Business Processing, Environment Management, Database Utilities, and Engineering Support. The definitions of these categories are found in the TAFIM 3.0, Volume 2, DoD Technical Reference Model, 30 April 1996.

2.2.2.2 Application Platform Entity

The Application Platform Entity is the second layer of the DoD TRM, and includes the common, standard services upon which the required functionality is built. The Application Platform Entity is composed of service areas and cross-area services. The corresponding mandates are provided in the following subsections.

2.2.2.2.1 Service Areas

Seven primary service areas are defined within the Application Platform Entity: Software Engineering, User Interfaces, Data Management, Data Interchange, Graphics, Communications, and Operating System Services.

2.2.2.2.1.1 Software Engineering Services

The software engineering services provide system developers with the tools that are appropriate to the development and maintenance of applications. There are no mandated standards for this service area.

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

"Programming language selections should be made in the context of the system and software engineering factors that influence overall life-cycle costs, risks, and potential for interoperability."[1]

Computer languages should be used in such a way as to minimize changes when compilers, operating systems or hardware change. To maximize portability, the software should be structured where possible so it can be easily ported.

2.2.2.2.1.2 User Interface Services

User Interface Services control how a user interfaces with an information technology system. The Common Desktop Environment (CDE) provides a common set of desktop applications and management capabilities for environments similar to the Microsoft Windows desktop environment. CDE supports Open Software Foundation (OSF) Motif based application execution. Both CDE and Motif applications use the underlying X-Windows system. The Win32 Application Program Interface (API) set provides similar services for Microsoft Windows applications. Applications that require user interaction shall use either Motif/X-Window APIs and be capable of executing in the CDE or the applicable native windowing Win32 APIs. The following standards are mandated:

- C507, Window Management (X11R5): X-Window System Protocol, X/Open CAE Specification, April 1995.
- C508, Window Management (X11R5): Xlib - C Language Binding, X/Open CAE Specification, April 1995.
- C509, Window Management (X11R5): X Toolkit Intrinsics, X/Open CAE Specification, April 1995.
- C510, Window Management (X11R5): File Formats & Application Conventions, X/Open CAE Specification, April 1995.
- C320, Motif Toolkit API, X/Open CAE Specification, April 1995.
- X/Open C323, Common Desktop Environment (CDE) Version 1.0, April 1995.
- Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993 or later, Microsoft Press.

Refer to Section 2.5 for Human-Computer Interface (HCI) style guidance and standards.

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

2.2.2.2.1.3 Data Management Services

Central to most systems is the sharing of data between applications. The data management services provide for the independent management of data shared by multiple applications.

These services support the definition, storage, and retrieval of data elements from Database Management Systems (DBMSs). Application code using Relational Database Management System (RDBMS) resources and COTS RDBMSs shall conform to the requirements of Entry Level Structured Query Language (SQL). The following standards are mandated for any system using an RDBMS:

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

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

- Open Data-Base Connectivity, ODBC 2.0.

2.2.2.2.1.4 Data Interchange Services

The data interchange services provide specialized support for the exchange of data and information between applications and to and from the external environment. These services include document, graphics data, geospatial data, still imagery data, motion imagery data, multimedia data, product data, atmospheric data, oceanographic data, and time-of-day data.

2.2.2.2.1.4.1 Document Interchange

The Standard Generalized Markup Language (SGML) format supports the production of documents which are intended for long-term storage and electronic dissemination for viewing in multiple formats. SGML formalizes document mark-up, making the document independent of the production and/or publishing system. SGML is an architecture-independent and application-independent language for managing document structures. SGML is a meta-language, providing the rules for designing and applying a system of markup tags rather than the specific set of tags. The following standard is mandated:

- ISO 8879: 1986, Standard Generalized Markup Language (SGML) with Amendment 1, 1998.

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

- REC-html-971218, Hypertext Markup Language (HTML), Internet Version 4.0, Reference Specification, World Wide Web Consortium (W3C), 18 December 1997 - Interchange format used by the WWW for hypertext format and embedded navigational links.

Table 2.2-1 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 2.2-1 identifies conventions for file name extensions for documents of various types. The following file formats are mandated, but not the specific products mentioned:

- All applications acquired or developed for the production of documents shall be capable of generating at least one of the formats listed in Table 2.2-1 for the appropriate document type.
- All organizations shall at a minimum be capable of reading and printing all of the formats listed below for the appropriate document type.

Table 2.2-1 Common Document Interchange Formats

Document Type	Standard/Vendor Format	Recommended File Name Extension	Reference
Plain Text	ASCII Text	.txt	ISO/IEC 646:1991 IRV
Compound Document*	Adobe PDF 3.0	.pdf	Vendor
	HTML 4.0	.htm	W3C
	MS Word 6.0	.doc	Vendor
	Rich Text Format	.rtf	Vendor
	WordPerfect 5.2	.wp5	Vendor
Briefing - Graphic Presentation	Freelance Graphics 2.1	.pre	Vendor
	MS PowerPoint 4.0	.ppt	Vendor
Spreadsheet	Lotus 1-2-3 Release 3.x	.wk3	Vendor
	MS Excel 5.0	.xls	Vendor
Database	Dbase 4.0	.dbf	Vendor
Compression	GZIP file format	.gz	RFC 1952
	Zip file format	.zip	Vendor

Notes: * - Compound documents contain embedded graphics, tables, and formatted text. OLE linking complicates document interchange. IRV is International Reference Version. Note that some special fonts, formatting, or features supported in the native file format may not convert accurately.

2.2.2.2.1.4.2 Graphics Data Interchange

These services are supported by device-independent descriptions of the picture elements for vector and raster graphics. The ISO Joint Photographic Expert Group (JPEG) standard describes several alternative algorithms for the representation and compression of raster images, particularly for photographs. The standard does not specify an interchange format for JPEG images, which led to the development of the JPEG File Interchange Format (JFIF) format. Graphics Interchange Format (GIF) and JFIF are de facto standards for exchanging graphics and images over the internet. GIF supports lossless compressed images with up to 256 colors and short animation segments. GIF is mandated for use on an internet when such a format is needed. Note that Unisys owns a related patent, which requires a license for software that writes the GIF format. Readers of the GIF format have no royalty obligations. JFIF supports compressed images and is mandated for the interchange of lossy compressed, non-georeferenced photographic images over an internet (under Graphics Data Interchange). The following standards are mandated:

- ANSI/ISO/IEC 8632.1-4:1992 (R1997); ISO 8632:1992 with Amendment 1:1994 and Amendment 2:1995 as profiled by FIPS PUB 128-2: 17 April 1996, Computer Graphics Metafile (CGM)-Interchange format for vector graphics data.
- JPEG File Interchange Format (JFIF), Version 1.02, C-Cube Microsystems for raster graphics data encoded using the ISO/IEC 10918-1:1994, Joint Photographic Experts Group (JPEG) algorithm.
- Graphics Interchange Format (GIF), Version 89a, 31 July 1990, CompuServe Incorporated.

2.2.2.2.1.4.3 Geospatial Data Interchange

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

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

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

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

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

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

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

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

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

2.2.2.2.1.4.4 Still Imagery Data Interchange

The National Imagery Transmission Format Standard (NITFS) is a DoD and Federal Intelligence Community suite of standards for the exchange, storage, and transmission of digital imagery products and image related products. NITFS provides a package containing information about the image, the image itself, and optional overlay graphics. The Standard provides a 'package' containing an image(s), subimages, symbols, labels, and text as well as other information related to the image(s). NITF supports the dissemination of secondary digital imagery from overhead collection platforms. Guidance on applying the suite of standards composing NITFS can be found in MIL-HDBK-1300A. The following standards are mandated for imagery product dissemination:

- MIL-STD-2500A, National Imagery Transmission Format (Version 2.0) for the National Imagery Transmission Format Standard, 12 October 1994, Revised 7 February 1997.
- MIL-STD-188-196, Bi-Level Image Compression for the National Imagery Transmission Format Standard, 18 June 1993.
- MIL-STD-188-199, Vector Quantization Decompression for the National Imagery Transmission Format Standard, 27 June 1994.
- MIL-STD-2301A, Computer Graphics Metafile (CGM) Implementation Standard for the National Imagery Transmission Format Standard, 18 June 1993, with Notice of Change 1, 12 October 1994, profiled by ANSI/ISO 8632:1992 Computer Graphics Metafile (CGM) for the Storage and Transfer of Picture Description Information.
- ISO/IEC 10918-1: 1994, Joint Photographic Experts Group (JPEG) as profiled by MIL-STD-188-198A, Joint Photographic Experts Group (JPEG) Image Compression for the National Imagery Transmission Format Standard, 15 December 1993. Although the NITFS uses the same ISO JPEG algorithm as mandated in Section 2.2.2.2.1.4.2, the NITFS file format is not interchangeable with the JFIF file format.

Communication protocols for transmission of imagery over point-to-point tactical data links in high Bit Error Rate (BER), disadvantaged communications environments are specified in Section 2.3.2.1.4.

2.2.2.2.1.4.5 Motion Imagery Data Interchange

Motion Imagery is sequential or continuous streaming images at specified temporal rates (normally expressed as frames per second) at frame rates of 1 Hz (1 frame per second) or higher.

2.2.2.2.1.4.5.1 Video Systems

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

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

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

2.2.2.2.1.4.5.1.1 Video Imagery

The "DoD/IC/USIGS Video Imagery Standards Profile (VISP)," Version 1.21, 7 January 1998, describes the minimum set of standards and guidelines for the acquisition of systems that produce, use, or exchange Video Imagery information. The United States Imagery and Geospatial Information System (USIGS) is the federation of organizations within U.S. government that collectively or individually acquire, produce, or deliver imagery, imagery intelligence, and geospatial information and services. The VISP identifies commercial standards that support interoperability for USIGS environments. Digital video standards (as defined in the VISP) are for use in all new or upgraded DoD systems. Legacy video imagery systems that currently use analog formats may continue to use their existing analog components. The following standards, as profiled in VISP 1.21, 7 January 1998, are mandated for video imagery:

- ITU-R BT.601-4, Encoding Parameters of Digital Television for Studios, Component (4:2:2) Digital Video, 1994, shall be used for baseband (uncompressed) video signal waveforms.
- ANSI/SMPTE 259M-1993, Television - 10 bit 4:2:2 Component (Serial Digital Interface), 1993, using ITU-R BT.601-4 Component (4:2:2) digital video waveforms, shall be the uncompressed baseband signal transport and processing standard for digital video, audio and metadata origination, system interface, production/analysis center processing and manipulation.
- ISO/IEC 13818 - 1,2,4 "MPEG-2, 4:2:2 Profile @ Main Level" (4:2:2 P @ ML), 1996 shall be the compression profile for initial link origination, transmission, production, manipulation, and computer based archiving (disk based) where further image processing is anticipated.
- ISO/IEC 13818 – 1,2,4 "MPEG-2, 4:2:0 Main Profile @ Main Level" (MP @ ML), 1996 shall be the minimum quality compression profile for end-user video product distribution, including wide area transmissions, where limited additional image processing is anticipated and where bandwidth limitations preclude use of 4:2:2 P @ ML.
- ANSI/SMPTE 12M-1995, Television, Audio and Film - Time and Control Code, commonly known as Society and Motion Picture and Television Engineers (SMPTE) time code, shall be the standard for time annotation and embedded time references for video systems. Furthermore, within 12M, Vertical Interval Time Code (VITC), Drop Frame shall be used for 29.97 FPS systems, Non-Drop Frame Time Code shall be used for 24, 25, 30, 50, and 60 FPS systems. Note: Analog NTSC systems are based on 29.97 FPS.

The standards for Video Imagery section does not completely define an architecture for interoperability for low bandwidth (below 1.5 Mbits/s) real-time streaming applications. Standards for such low bandwidth applications are actively under development. Until such standards are available, users may use "MPEG-1" or "MPEG-2 4:2:0 MP@ML Adaptive Field Frame" standards for low bandwidth video applications. DoD users that adopt proprietary video compression systems for very low bandwidth applications are cautioned that such systems are generally not supported within DoD and that the interoperability of such systems is not assured.

2.2.2.2.1.4.5.1.2 Video Teleconference

Video Teleconferencing (VTC) standards are specified in Section 2.3.2.1.2.

2.2.2.2.1.4.5.1.3 Video Telemedicine

Video Telemedicine System interchange standards will be addressed in a later version of the JTA.

2.2.2.2.1.4.5.1.4 Video Support

MPEG-1 is an open international standard for video compression that has been optimized for single and double-speed CD-ROM data transfer rates. The standard defines a bit-stream representation for synchronized digital video and audio, compressed to fit into a bandwidth of 1.5 Mbits/s. This corresponds to the data retrieval speed from CD-ROM and Digital Audio Tape (DAT). With 30 frames per second video at a display resolution of 352 x 240 pixels, the quality of compressed and decompressed video at this data rate is often described as similar to 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 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s – Part 1: Systems, 1993.
- ISO/IEC 11172-1: 1993/Cor. 1:1995 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s – Part 1: Systems Technical Corrigendum 1; 1993/1995.
- ISO/IEC 11172-2: 1993 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s – Part 2 Video; 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 Mbits/s, where limited additional processing is anticipated, operating in either progressive or interlaced scan mode, optimally handling the resolution of the ITU-R 601 recommendation (that is, 720 x 480 pixels for the luminance signal and 360 x 480 pixels for the color space). The following video support standards for compressed video are mandated:

- ISO/IEC 13818-1: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 1: Systems (MPEG-2); 1996, with Amendment 1:1997. (The identical text is also published as ITU-T Rec. H.222.0.).
- ISO/IEC 13818-2: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 2: Video (MPEG-2); 1996, with Amendment 1:1997 and Amendment 2:1997. (The identical text is also published as ITU-T Rec. H.262).

The following video support applications will be addressed in a later version of the JTA:

– Moving Target Indication (MTI)

– Synthetic Aperature Radar (SAR)

– Infrared (IR)

2.2.2.2.1.4.6 Audio Data Interchange

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

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

2.2.2.2.1.4.6.1 Audio Associated with Video

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

1. Audio for Video Imagery Systems 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, Reconnaissance, and Surveillance (ISR) activities.
2. Audio for Video Teleconference Systems 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.
3. Audio for Video Telemedicine Systems provide real-time visual interchange between remote locations in support of biomedical applications including fiber optic and video teleconferencing.
4. Audio for Video Support Systems 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 which are not associated with DoD warfighting operations.

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

2.2.2.2.1.4.6.1.1 Audio for Video Imagery

For audio systems associated with Video Imagery applications, the audio sub-sections of the "USIGS Video Imagery Standards Profile (VISP)," Version 1.21, 7 January 1998 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). Used for digital audio signal interchange in uncompressed digital video.
- ISO/IEC 13818-3:1995, Information technology - Generic coding of moving pictures and associated audio information, with Amendment 1:1996. Used for compressed digital audio systems, MPEG-2 Part 3: Audio.

2.2.2.2.1.4.6.1.2 Audio for Video Teleconference

Video Teleconferencing (VTC) standards are specified in Section 2.3.2.1.2.

2.2.2.2.1.4.6.1.3 Audio for Video Telemedicine

Audio for Video Telemedicine system interchange standards will be addressed in a later version of the JTA.

2.2.2.2.1.4.6.1.4 Audio for Video Support

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

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

2.2.2.2.1.4.6.2 Audio Not Associated with Video Systems

Formats for the exchange of stand-alone audio will be addressed in a later version of the JTA.

2.2.2.2.1.4.7 Multimedia Data Interchange

Formats for the exchange of multimedia data will be addressed in a later version of the JTA.

2.2.2.2.1.4.8 Product Data Interchange

Formats for the exchange of product data are not addressed in the main body of the JTA.

2.2.2.2.1.4.9 Atmospheric Data Interchange

The following formats are established by the World Meteorological Organization (WMO) Commission for Basic Systems (CBS) for meteorological data. The WMO Format for the Storage of Weather Product Information and the Exchange of Weather Product Messages in Gridded Binary (GRIB) Form. GRIB was developed for the transfer of gridded data fields, including spectral model coefficients, and of satellite images. A GRIB record (message) contains values at grid points of an array, or a set of spectral coefficients, for a parameter at a single level or layer as a continuous bit stream. It is an efficient vehicle for transmitting large volumes of gridded data to automated centers over high speed telecommunication lines using modern protocols. It can serve as a data storage format. While GRIB can use predefined grids, provisions have been made for a grid to be defined within the message. The following standard is mandated:

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

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

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

2.2.2.2.1.4.10 Oceanographic Data Interchange

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

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

2.2.2.2.1.4.11 Time of Day Data Interchange

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

- ITU-R Recommendation TF.460-4, Standard-frequency and Time-signal Emissions, International Telecommunications Union, July 1986.

Note that the Global Positioning System (GPS) provides time of day information that is traceable to UTC(USNO). Also, note that leap seconds are inserted or deleted when necessary in UTC to keep the time of day system synchronized with the Earth's rotation.

2.2.2.2.1.5 Graphic Services

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

- ANSI/ISO/IEC 9636-1,2,3,4,5,6:1991 (R1997), Information Technology Computer Graphics Interfacing (CGI) Techniques for Dialogue with Graphics Devices.
- The OpenGL Graphics System: A Specification (Version 1.1) 25 June 1996 (for three-dimensional graphics).

2.2.2.2.1.6 Communications Services

These services support the distributed applications that require data access and applications interoperability in networked environments. The mandated standards are provided in Section 2.3.

2.2.2.2.1.7 Operating System Services

These core services are necessary to operate and administer a computer platform and to support the operation of application software. They include kernel operations, shell, and utilities. The kernel controls access to information and the underlying hardware. These services shall be accessed by applications through either the standard Portable Operating System Interface (POSIX) or WIN32 APIs. Not all operating system services are required to be implemented, but those that are used shall comply with the standards listed below.

The following standards are mandated:

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

- 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, as profiled by FIPS PUB 189: 1994, Information Technology - Portable Operating System Interface (POSIX) – Recommendations (Section 12) and Implementation Guidance (Section 13).
- IEEE 1003.2d: 1994, POSIX – Part 2: Shell and Utilities – Amendment: Batch Environment.
- IEEE 1003.5: 1992, IEEE Standard for Information Technology – POSIX Ada Language Interfaces – Part 1: Binding for System Application Program Interface (API) with Interpretations, March 1994.
- IEEE 1003.5b: 1996, IEEE Standard for Information Technology – POSIX Ada Language Interfaces – Part 1: Binding for System Application Program Interface (API) – Amendment 1: Real-time Extensions. (Incorporates IEEE 1003.5:1992).
- Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993 or later, Microsoft Press.

2.2.2.2.2 Application Platform Cross-Area Services

The DoD TRM defines four application platform cross-area services: Internationalization, Security, System Management, and Distributed Computing Services.

2.2.2.2.2.1 Internationalization Services

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

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

- ANSI/ISO 8859-1:1987, Information Processing – 8-Bit Single Byte Coded Character Sets, Part 1: Latin Alphabet No. 1.
- ISO/IEC 10646-1:1993, Information Technology - Universal Multiple-Octet Coded Character Set (UCS) – Part 1: Architecture and Basic Multilingual Plane with Technical Corrigendum 1:1996.

2.2.2.2.2.2 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 2.6.)

2.2.2.2.2.3 System Management Services

These services provide capabilities to manage an operating platform and its resources and users. System management services include configuration management, fault management, and performance management. Network Management mandated standards are provided in Section 2.3.2.4. There are no standards currently mandated for systems management. Emerging Network Management Standards can be found in Section 2.3.3.5.

2.2.2.2.2.4 Distributed Computing Services

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

2.2.2.2.2.4.1 Remote Procedure Computing

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

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

The C311 specification is included here to provide the complete definition of the DCE. Section 2.6, Information Systems Security Standards, specifies the other security requirements that must be met.

When used in conjunction with the POSIX Threads Extensions, the recommendations of the Open Group's Single UNIX Specification 1998 (UNIX 1998) is expected to integrate the DCE thread model with the POSIX thread model.

2.2.2.2.2.4.2 Distributed Object Computing

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

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

- The Common Object Request Broker: Architecture and Specification, Version 2.1, OMG document formal/1 September 1997.

When a CORBA Object Request Broker (ORB) is used, the following specifications are mandated:

- Naming Service, 7 December 1993, contained in CORBAservices: Common Object Services Specification, OMG Document formal/4 July 1997.
- Event Notification Service, 7 December 1993, contained in CORBAservices: Common Object Services Specification, OMG Document formal/24 February 1997.
- Object Transaction Service, 6 December 1994, contained in CORBAservices: Common Object Services Specification, OMG Document formal/24 February 1997.

2.2.3 Emerging Standards

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

2.2.3.1 User Interface

The Open Group released version 2.1 of the Common Desktop Environment (CDE) which integrates the Motif 2.1 graphical user interface, X Window System (X11R6), and CDE to standardize application presentations in distributed multi-platform environments. This framework provides not only mechanisms for graphical display of common objects, but also standard interprocess communication mechanisms and a set of commonly-used desktop tools (e.g., file manager and mail tool) that are relevant to many domains.

2.2.3.2 Data Management

Within Data Management Services, standards for both RDBMS and Object-Oriented Database Management Systems (OODBMSs) will continue to evolve and mature. In the RDBMS domain, SQL3 is being developed by the ANSI X3H2 committee. In the OODBMS domain, the Object Database Management Group (ODMG) is evolving from the ODMG-93 specification to the ODMG-9x standard. SQL3 and ODMG-9x are being developed in parallel to ensure as much commonality as possible.

2.2.3.3 Data Interchange

2.2.3.3.1 Document Interchange

The eXtensible Markup Language (XML), REC-xml-19980210, Extensible Markup Language, W3C Recommendation, 10 February 1998, is being defined by the World Wide Web Consortium (W3C) and is a metalanguage, based on SGML, for describing languages based on name-attribute tuples. XML allows domain specific markup languages and customized, application-specific markup languages to be defined through the use of application profiles using application-specific tagged data items. The resulting XML documents are conforming SGML documents that, while primarily intended for use in the exchange of metadata, support the embedding of URLs and style sheets. This allows XML tags to be used to represent concepts at multiple levels of abstraction, facilitate metadata searches, provide direct access to data described by the metadata, and provide information as to how to obtain data that is not available directly on-line. Finally, XML allows new capabilities to be defined and delivered dynamically.

2.2.3.3.2 Graphics Data Interchange

The Portable Network Graphics (PNG) format (IETF RFC-2083 PNG Specification Version 1.0, 16 January 1997) has been developed as a patent-free replacement for GIF. PNG is an extensible file format for the lossless, portable, well-compressed storage of raster images. Indexed-color, grayscale, and truecolor images are supported, plus an optional alpha channel for transparency. The Internet Media Type image/png was approved on 14 October 1996. The PNG specification was issued as a W3C Recommendation on 1 October 1996. Product support for PNG is growing, but is not yet sufficient to justify mandating the use of the format.

2.2.3.3.3 Virtual Reality Modeling Language

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

2.2.3.3.4 Geospatial Data Interchange

DIGEST (Digital Geographic Information Exchange Standard) 2.0, June 1997, has been developed by the DGI Working Group (DGIWG) to support the transfer of DGI between GISs in DoD, U.S., NATO, and co-producer countries. The DIGEST is evolving to supersede many of the MIL-STDs, such as MIL-STD-2411, Vector Product Format, that are currently maintained by the DoD.

Some Geospatial MIL-STDs are being reclassified as Interface Standards. Draft MIL-STD-2405, Datums, Coordinates, and Grids is being revised as an Interface Standard.

The NIMA Technical Report for the DoD World Geodetic System (WGS-84) 1984, NIMA TR8350.2, Third Edition, 4 July 1997, has been updated and approved. The report has been submitted for joint review and the development of an implementation plan. TR8350.2 is the technical implementation of MIL-STD-2401, DoD World Geodetic System (WGS84).

2.2.3.3.5 Still Imagery Data Interchange

MIL-STD-2500B, National Imagery Transmission Format (Version 2.1) for the National Imagery Transmission Format Standard has been approved, with an effective date of 1 October 1998. The NITFS is proposed for adoption as ISO standard (ISO 12087-5 BIIF).

Several NITFS (National Imagery Transmission Format Standard) Support Data Extensions (SDEs) have been developed to extend the functionality of the standard file format for imagery and imagery-related products. These SDEs provide support for using the NITFS with SAR, commercial satellite imagery and georeferenced imagery.

2.2.3.3.6 Motion Imagery Data Interchange

2.2.3.3.6.1 Video Systems

2.2.3.3.6.1.1 Video Imagery

The DoD/IC/USIGS Video Imagery Standards Profile (VISP), Version 1.21, 7 January 1998, Chapter 3 outlines emerging Standards, Profiles, and Recommended Practices for Video Imagery applications. VISP Chapter 3 emerging video imagery standards include profiles for High Definition Television Systems (HDTV); Advanced Television Systems (ATV); Video Metadata Systems, to include Intelligence Video Index, Content Description Metadata; Advanced Video Index; Ancillary Data; Advanced Video Index Encoding; Ancillary Data, Encoding into MPEG-2 Private Data Streams; Ancillary Data, Encoding into AES3 Data Streams; Time Code Embedding; Time Reference Synchronization; and completion of all levels of the Video Systems (Spatial and Temporal) Matrix (VSM).

It is also anticipated that MPEG-4 and MPEG-7 may be used for very low data rate video dissemination applications (such as VSM 1 and VSM 2).

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

2.2.3.3.6.1.2 Video Teleconference

Emerging standards for video teleconferencing are covered in the Information Transfer section of the JTA, Section 2.3.3.1.2.

2.2.3.3.7 Multimedia Data Interchange

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

2.2.3.4 Operating Systems

2.2.3.4.1 POSIX

The following POSIX standards are emerging:

- P1003.1d Real-Time System API Extensions.
- P1003.1g Protocol Independent Interfaces.
- P1003.1h Services for Reliable, Available, Serviceable Systems.
- P1003.1j Advanced Real-time System API Extensions.
- P1003.1m Checkpoint Restart.
- P1003.1q System API: The Trace Amendment.
- P1003.13 Standardized Application Environment Profile - POSIX Real-time Application Support.
- P1003.21 Real-Time Distributed Systems Communication.

2.2.3.4.2 UNIX

The X/Open Single UNIX Specification (SUS) Version 2 (T912) (previously referred to as Specification 1170, February 1997) has been updated to include POSIX real-time interfaces. Operating systems that conform to this specification and have received the UNIX brand from X/Open are on the market. For UNIX-based implementations, strong emphasis should be placed on acquiring systems that are SUS conformant over those that are not.

2.2.3.4.3 Virtual Machines

The Java Virtual Machine (JVM) and supporting libraries are an emerging standard. The JVM may be used to support applications executed through a web browser or to support development of portable applications. The Java Virtual Machine is defined in "The Java Virtual Machine Specification" by Tim Lindholm and Frank Yellin, Addison-Wesley, 1997. An overview of Java libraries and their status is available on the World Wide Web at:

http://java.sun.com/products/api-overview/index.html

2.2.3.5 Distributed Computing

- OSF-DCE Version 1.2.2 was issued to developers by the Open Group in November 1997.

Among the many emerging standards from the Object Management Group, there are three newly adopted specifications and one soon-to-be-adopted specification that bear particular consideration: the Unified Modeling Language (UML), the Meta-Object Facility (MOF), the COM/CORBA interworking specification, and the Mobile Agent Facility specification. In addition, there are a wide variety of specifications in various stages of development, including, but not limited to: real-time CORBA; a CORBA Scripting Language; a Messaging Service; a Negotiation Service and Electronic Payment Service for electronic commerce applications; a Healthcare Claims Facility; and much more.

2.3 INFORMATION TRANSFER STANDARDS

2.3.1 Introduction

2.3.1.1 Purpose

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

2.3.1.2 Scope

This section identifies the information transfer standards that are required for interoperability between DoD information technology systems. These standards support access for end-systems including host, VTC, facsimile, GPS, and secondary imagery dissemination. Networking and internetworking standards are identified. Transmission media standards for MILSATCOM, Synchronous Optical Network (SONET) and radio links as well as network and systems management standards for data communications and telecommunications are identified. Finally, emerging technologies that should be monitored for future extension of information transfer capabilities are identified. This section includes the Communications Services depicted in Figure 2.1-1, TAFIM DoD Technical Reference Model. Security standards are addressed in Section 2.6.2.3.

2.3.1.3 Background

The standards are drawn from widely accepted commercial standards that meet DoD requirements. Where necessary for interoperability, profiles of commercial standards are used. Military standards are mandated only when suitable commercial standards are not available. For example, the JTA makes use of the open-systems architecture used by the Internet and the Defense Information System Network (DISN). System components are categorized here as end-systems, networks and transmission media. End-systems (e.g., host computers, terminals) generally execute applications on behalf of users and share information with other end-systems via networks. Networks may be relatively simple (e.g., point-to-point links or subnetworks which are homogenous in protocol stacks) or have complex internal structures of diverse subnetworks. Routers interconnect two or more subnetworks and forward packets across subnetwork boundaries. Routers are distinct from hosts in that they are normally not the destination of data traffic. End-systems and networks are connected by transmission media.

2.3.2 Mandates

This subsection identifies the mandatory standards, profiles, and practices for information transfer. Each mandated standard or practice is clearly identified on a separate line, and includes a formal reference that can be included within Requests for Proposals (RFP) or Statements of Work (SOW). Appendix B contains a table that summarizes the mandated standards from this section, as well as providing information on how to obtain the standards.

2.3.2.1 End-system Standards

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

2.3.2.1.1 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. Standard-3 also adds additional discussion and guidance for implementers. The following standard is mandated:

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

2.3.2.1.1.1 Application Support Services

2.3.2.1.1.1.1 Electronic Mail

The standard for official organizational messaging traffic between DoD organizations is the Defense Message System's (DMS) X.400-based suite of military messaging standards defined in Allied Communication Publication (ACP) 123. The ACP 123 annexes contain standards profiles for the definition of the DMS "Business Class Messaging" (P772) capability and the Message Security Protocol (MSP). Organizational messaging is considered a high assurance messaging service that requires authentication, delivery confirmation, and encryption. See Section 2.6 for security standards. Since X.400 is not an internet standard, see Section 2.3.2.1.1.2.2 for operation over Internet Protocol (IP) based networks. The following standards are mandated:

- ACP 123, Common Messaging Strategy and Procedures, November 1994.
- ACP 123, U.S. Supplement No. 1, Common Messaging Strategy and Procedures, November 1995.

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

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

2.3.2.1.1.1.2 Directory Services

2.3.2.1.1.1.2.1 X.500 Directory Services

International Telecommunications Union (ITU) X.500 provides directory services that may be used by users or host applications to locate other users and resources on the network. 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 2.6 for security standards. Since X.500 is not an internet standard, see Section 2.3.2.1.1.2.2 for operation over IP based networks. The following standard is mandated:

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

2.3.2.1.1.1.2.2 Lightweight Directory Access Protocol (LDAP)

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

- IETF RFC-1777, LDAP, March 1995.

2.3.2.1.1.1.2.3 Domain Name System (DNS)

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 Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) as a transport service when used in conjunction with other services. The following standard is mandated:

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

2.3.2.1.1.1.3 File Transfer

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

- 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).

2.3.2.1.1.1.4 Remote Terminal

Basic remote terminal services shall be accomplished using Telecommunications Network (TELNET). TELNET provides a virtual terminal capability that allows a user to "log on" to a remote system as though the user's terminal was directly connected to the remote system. The following standard is mandated:

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

2.3.2.1.1.1.5 Network Time Synchronization

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

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

2.3.2.1.1.1.6 Bootstrap Protocol (BOOTP)

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

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

2.3.2.1.1.1.7 Configuration Information Transfer

The Dynamic Host Configuration Protocol (DHCP) provides an extension of BOOTP to support the passing of configuration information to Internet hosts. DHCP consists of two parts: a protocol for delivering host-specific configuration parameters from a DHCP server to a host, and a mechanism for automatically allocating IP addresses to hosts. The following standard is mandated:

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

2.3.2.1.1.1.8 World Wide Web (WWW) Services

2.3.2.1.1.1.8.1 Hypertext Transfer Protocol (HTTP)

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

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

2.3.2.1.1.1.8.2 Uniform Resource Locator (URL)

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

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

2.3.2.1.1.1.9 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 TCP/UDP as a transport service. The following standard is mandated:

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

2.3.2.1.1.2 Transport Services

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

2.3.2.1.1.2.1 Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) Over Internet Protocol (IP)

2.3.2.1.1.2.1.1 Transmission Control Protocol (TCP)

TCP provides a reliable connection-oriented transport service. The following standards are mandated:

- IETF Standard 7/RFC-793, Transmission Control Protocol, September 1981. In addition, TCP shall implement the PUSH flag and the Nagle Algorithm, as defined in IETF Standard 3, Host Requirements.
- IETF RFC-2001, TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms, 24 January 1997.

2.3.2.1.1.2.1.2 User Datagram Protocol (UDP)

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

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

2.3.2.1.1.2.1.3 Internet Protocol (IP)

IP is a basic connectionless datagram service. All protocols within the IP suite use the IP datagram as the basic data transport mechanism. Two other protocols are considered integral parts of IP: the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP). ICMP is used to provide error reporting, flow control, and route redirection. IGMP provides multicast extensions for hosts to report their group membership to multicast routers. The following standard is mandated:

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

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

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

2.3.2.1.1.2.2 Open Systems Interconnection (OSI) Transport Over IP-based Networks

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

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

2.3.2.1.2 Video Teleconferencing (VTC) Standards

VTC terminals and Multipoint Control Units operating at data rates of 56-1,920 kilobits per second (Kbits/s) shall comply with Appendix A of Federal Telecommunications Recommendation (FTR) 1080-97 Profile for Video Teleconferencing. The purpose of the profile is to provide interoperability between VTC terminal equipment, both in point-to-point and multipoint configurations for telephony applications. Additional ITU-T ratified standards, which supplement and/or displace the standards in Appendix A of FTR 1080-97, are mandated for those VTC systems implementing the multimedia applications. The key standard included in FTR 1080-97 is ITU-T H.320, Narrowband Visual Telephone Systems and Terminal Equipment, an umbrella standard of recommendations addressing audio, video, signaling, and control.

The following standards are mandated for VTC terminals operating at data rates of 56-1,920 Kbits/s:

- FTR 1080-97, Profile for Video Teleconferencing, Appendix A, 30 October 1997.
- ITU-T G.728 Coding of Speech at 16 kbps Using Low-Delay Code Excited Linear Prediction (LD-CELP), September 1992.

The following standards are mandated for VTC terminals requiring far-end camera control and operating at data rates of 56-1,920 Kbits/s:

- ITU-T H.224, A Real Time Control Protocol for Simplex Applications using H.221 LSD/HSD/MLP channels, November 1994.
- ITU-T H.281, A Far-End Camera Protocol for Videoconferencing Using H.224, November 1994.

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

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

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

- ITU-T T.120, Transmission Protocols for Multimedia Data, July 1996.
- ITU-T T.122, Multipoint Communications Service for Audiographic and Audio Visual Conferencing Service Definition, March 1993.
- ITU-T T.123, Protocol Stacks for Audiographic and Audiovisual Teleconferencing Applications, November 1994.
- ITU-T T.124, Generic Conference Control for Audiographic and Audiovisual Terminals and Multipoint Control Units, August 1995.
- ITU-T T.125, Multipoint Communications Service Protocol Specification, April 1994.
- ITU-T T.126, Multipoint Still Image and Annotation Conferencing Protocol Specification, August 1995.
- ITU-T T.127, Multipoint Binary File Transfer Protocol, August 1995.

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

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

2.3.2.1.3 Facsimile Standards

2.3.2.1.3.1 Analog Facsimile Standards

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

- TIA/EIA-465-A, Group 3 Facsimile Apparatus for Document Transmission, 21 March 1995.
- TIA/EIA-466-A, Procedures for Document Facsimile Transmission, 27 September 1996.

2.3.2.1.3.2 Digital Facsimile Standards

Digital facsimile terminals operating in tactical, high Bit Error Rate (BER) environments shall implement digital facsimile equipment standards for Type I and/or Type II modes. Also, facsimile transmissions requiring encryption, or interoperability with NATO countries, shall use the digital facsimile standard. The following standard is mandated:

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

2.3.2.1.4 Secondary 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 shall be used over point-to-point tactical data links in high BER disadvantaged communications environments. TACO2 is used to transfer secondary imagery and related products where JTA transfer protocols in Section 2.3.2.1.1.2 fail (e.g., TACO2 only applies to users having simplex and half duplex links as their only means of communications). MIL-HDBK-1300A, NITFS, provides guidance to implement various Technical Interface Specifications (TIS) to connect the TACO2 host to specific cryptographic equipment. The following standard is mandated:

- MIL-STD-2045-44500, National Imagery Transmission Format Standard (NITFS) Tactical Communications Protocol 2 (TACO2), 18 June 1993; with Notice of Change 1, 29 July 1994, and Notice of Change 2, 27 June 1996.

2.3.2.1.5 Global Positioning System (GPS)

GPS user equipment must employ Precise Position Service (PPS) user equipment incorporating both selective availability and anti-spoofing features to support combat operations. The GPS guidelines that are documented in ASD (C3I) Memorandum "Development, Procurement, and Employment of DoD Global Position System, User Equipment," 30 April 1992 must be followed.

2.3.2.2 Network Standards

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

2.3.2.2.1 Internetworking (Router) Standards

Routers are used to interconnect various subnetworks and end-systems. Protocols necessary to provide this service are specified below. RFC-1812 is an umbrella standard that references other documents and corrects errors in some of the referenced documents. In addition, some of the standards that were mandated for hosts in Section 2.3.2.1.1 also apply to routers. The following standards are mandated:

- IETF RFC-1812, Requirements for IP Version 4 Routers, 22 June 1995.
- IETF Standard 6/RFC-768, User Datagram Protocol, August 1980.
- IETF Standard 7/RFC-793, Transmission Control Protocol, September 1981.
- IETF Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983.
- IETF Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987.
- IETF RFC-951, Bootstrap Protocol, 1 September 1985.
- IETF RFC-1533, DHCP Options and BOOTP Vendor Extensions, 8 October 1993.
- IETF RFC-1541, DHCP, 27 October 1993.
- IETF RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, 27 October 1993.
- IETF Standard 33/RFC-1350, Trivial FTP (TFTP), July 1992, to be used for initialization only.

Security requirements are addressed in Section 2.6.

2.3.2.2.1.1 Internet Protocol (IP)

IP is a basic connectionless datagram service. All protocols within the IP suite use the IP datagram as the basic data transport mechanism. IP was designed to interconnect heterogeneous networks and operates over a wide variety of networks. Two other protocols are considered integral parts of IP, the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP). ICMP is used to provide error reporting, flow control, and route redirection. IGMP provides multicast extensions for hosts to report their group membership to multicast routers. The following standard is mandated:

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

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

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

2.3.2.2.1.2 IP Routing

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

2.3.2.2.1.2.1 Interior Routers

Routes within an autonomous system are considered local routes that are administered and advertised locally by means of an interior gateway protocol. Routers shall use the Open Shortest Path First (OSPF) V2 protocol for unicast interior gateway routing and Multicast OSPF (MOSPF) for multicast interior gateway routing. The following standards are mandated:

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

2.3.2.2.1.2.2 Exterior Routers

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

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

2.3.2.2.2 Subnetworks

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

2.3.2.2.2.1 Local Area Network (LAN) Access

While no specific LAN technology is mandated, the following is required for interoperability in a joint environment. This requires provision for a LAN interconnection. Ethernet, the common 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 Mbits/s and 100 Mbits/s. Platforms that must physically connect to a joint task force local area network shall support the 10BASE-T connection for Ethernet. When a higher speed interconnection is required, 100BASE-TX (two pairs of Category 5 unshielded twisted pair) may be employed. The 100BASE-TX Auto-Negotiation features are required when 100BASE-TX is deployed to permit interoperation with 10BASE-T. The following standards are mandated as the minimum LAN requirements for operation in a joint task force:

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

2.3.2.2.2.2 Point-to-Point Standards

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

- IETF Standard 51/RFC-1661/RFC-1662, Point-to-Point Protocol (PPP), July 1994.
- IETF RFC-1332, PPP Internet Protocol Control Protocol (IPCP), 26 May 1992.
- IETF RFC-1989, PPP Link Quality Monitoring (LQM), 16 August 1996.
- IETF RFC-1994, PPP Challenge Handshake Authentication Protocol (CHAP), 30 August 1996.
- IETF RFC-1570, PPP Link Control Protocol (LCP) Extensions, 11 January 1994.

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

- EIA/TIA-232-E, Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, July 1991.
- EIA/TIA-530-A, High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment, June 1992, Including Alternate 26-Position Connector, 1992. (This calls out EIA 422B and 423B).

2.3.2.2.2.3 Combat Net Radio (CNR) Networking

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

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

2.3.2.2.2.4 Integrated Services Digital Network (ISDN)

ISDN is an international standard used to support integrated voice and data over standard twisted-pair wire. ISDN defines a Basic Rate Interface (BRI) and Primary Rate Interface (PRI) to provide digital access to ISDN networks. These interfaces support both circuit-switched and packet-switched services. Note: It should be recognized that deployable systems might additionally be required to support other non-North American ISDN standards when accessing region-specific international infrastructure for ISDN services. The JTA recognizes that this is a critical area affecting interoperability but does not recommend specific solutions in this version. The following standards are mandated:

For BRI physical layer:

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

For PRI physical layer:

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

For the data link layer:

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

For signaling at the user-network interface:

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

Signaling at the user-network interface ANSI mandates shall be as profiled by the following National ISDN documents as adopted by the North American ISDN Users' Forum (NIUF):

- SR-3875, National ISDN 1995, 1996, and 1997, Bellcore.
- SR-3888, 1997 Version of National ISDN Basic Rate Interface Customer Premise Equipment Generic Guidelines, Bellcore.

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

For addressing:

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

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

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

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

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

2.3.2.2.2.5 Asynchronous Transfer Mode (ATM)

ATM is a high speed switched data transport technology that takes advantage of primarily low bit error rate transmission media to accommodate intelligent multiplexing of voice, data, video, imagery, and composite inputs over high-speed trunks and dedicated user links. ATM is a layered type of transfer protocol with the individual layers consisting of an ATM Adaptation Layer (AAL), the ATM layer, and the Physical Layer. The function of the AAL layer is to segment variable length data units into 48-octet cells, reassemble the data units, and perform error checking. The ATM Layer adds the necessary header information to allow for recovery of the data at the receiver end. The Physical Layer converts the cell information to the appropriate electrical/optical signals for the given transmission medium. AAL5 shall be used to support variable rate service. AAL1 shall be used to support constant bit rate service, which is sensitive to cell delay, but not cell loss. IP packets shall be transported over AAL5 in accordance with Lane 1.0. The ATM Forum's User-Network Interface (UNI) Specification shall be used as the set of Network Access Protocols for ATM Switches. The Private Network-Network Interface (PNNI) supports the distribution of topology information between switches and clusters of switches to allow paths to be computed through the network. PNNI also defines the signaling to establish point-to-point and point-to-multipoint connections across the ATM network. 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.

The following standards are mandated:

For Physical Layer:

- ATM Forum, af-phy-0040.000, Physical Interface Specification for 25.6 Mbp/s over twisted pair, November 1995.
- ATM Forum, af-uni-0010.002, ATM UNI Specification V 3.1, Section 2, September 1994.
- ATM Forum, af-phy-0016.000, DS1 Physical Layer Interface Specification, September 1994.
- ATM Forum, af-phy-0054.000, DS3 Physical Layer Interface Specification, January 1996.
- ATM Forum, af-phy-0046.000, 622.08 Mbp/s Physical Layer, January 1996.

For User to Network Interface (UNI):

- ATM Forum, af-uni-0010.002, ATM UNI Specification V 3.1, September 1994.

For ATM Adaptation Layer:

- ANSI T1.630, ATM Adaptation Layer for Constant Bit Rate (CBR) Services Functionality and Specification, 1993.
- ANSI T1.635, ATM Adaptation Layer Type 5 Common Part Functions and Specifications, 1994, which adopts ITU-T I.363, section 6.

For Private Network to Network Interfaces:

- ATM Forum, af-pnni-0055.000, PNNI Specification, Version 1.0, March 1996.
- ATM Forum, af-pnni-0066.000, PNNI Version 1.0 Addendum, September 1996.

For Local Area Network Emulation (LANE):

- ATM Forum, af-lane-0021.000, LANE over ATM, Version 1.0, January 1995.
- ATM Forum, af-lane-0050.000, LANE Version 1.0 Addendum, December 1995.
- ATM Forum, af-lane-0038.000, LANE Client Management Specification, September 1995.
- ATM Forum, af-lane-0057.000, LANE Servers Management Specification, March 1996.

For ATM Addressing Format:

- ATM Addressing Format specified as Notice of Change 1, 20 October 1997, to MIL-STD-188-176, Standardized Profile for ATM, 21 May 1996.

2.3.2.3 Transmission Media

2.3.2.3.1 Military Satellite Communications (MILSATCOM)

MILSATCOM systems include those systems owned or leased and operated by the DoD and those commercial SATCOM services used by the 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 of military or commercial satellite resources.

2.3.2.3.1.1 Ultra High Frequency (UHF) Satellite Terminal Standards

2.3.2.3.1.1.1 5-kHz and 25-kHz Service

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

- MIL-STD-188-181A, Interoperability Standard for Single Access 5-kHz and 25-kHz UHF Satellite Communications Channels, 31 March 1997.

2.3.2.3.1.1.2 5-kHz Demand Assigned Multiple Access (DAMA) Service

For 5-kHz Demand Assigned Multiple Access (DAMA) service, supporting the transmission of data at 75 - 2400 bits/s and digitized voice at 2400 bits/s, the following standard is mandated:

- MIL-STD-188-182A, Interoperability Standard for 5-kHz UHF DAMA Terminal Waveform, 31 March 1997.

2.3.2.3.1.1.3 25-kHz Time Division Multiple Access (TDMA)/Demand Assigned Multiple Access (DAMA) Service

For 25-kHz TDMA/DAMA service, supporting the transmission of voice at 2400, 4800, or 16,000 bits/s and data at rates of 75 - 16,000 bits/s, the following standard is mandated:

- MIL-STD-188-183, Interoperability Standard for 25-kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992; with Notice of Change 1, 2 December 1996.

2.3.2.3.1.1.4 Data Control Waveform

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

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

2.3.2.3.1.1.5 Demand Assigned Multiple Access (DAMA) Control System

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

- MIL-STD-188-185, DoD Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System, 29 May 1996.

2.3.2.3.1.2 Super High Frequency (SHF) Satellite Terminal Standards

2.3.2.3.1.2.1 Earth Terminals

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

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

2.3.2.3.1.2.2 Phase Shift Keying (PSK) Modems

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

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

2.3.2.3.1.3 Extremely High Frequency (EHF) Satellite Payload and Terminal Standards

2.3.2.3.1.3.1 Low Data Rate (LDR)

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

- MIL-STD-1582D, EHF LDR Uplinks and Downlinks, 30 September 1996; with Notice of Change 1, 14 February 1997.

2.3.2.3.1.3.2 Medium Data Rate (MDR)

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

- MIL-STD-188-136, EHF MDR Uplinks and Downlinks, 26 August 1995; with Notice of Change 1, 15 August 1996, and Notice of Change 2, 14 February 1997.

2.3.2.3.2 Radio Communications

2.3.2.3.2.1 Low Frequency (LF) and Very Low Frequency (VLF)

For radio subsystem requirements operating in the LF/VLF frequency bands, the following standard is mandated:

- MIL-STD-188-140A, Equipment Technical Design Standards for Common Long Haul/Tactical Radio Communications in the LF Band and Lower Frequency Bands, 1 May 1990.

2.3.2.3.2.2 High Frequency (HF)

2.3.2.3.2.2.1 HF and Automatic Link Establishment (ALE)

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

- MIL-STD-188-141A, Interoperability and Performance Standards for Medium and High Frequency Radio Equipment Standard, 15 September 1988; with Notice of Change 1, 17 June 1992, and Notice of Change 2, 10 September 1993.

2.3.2.3.2.2.2 Anti-jamming Capability

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

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

2.3.2.3.2.2.3 Data Modems

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

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

2.3.2.3.2.3 Very High Frequency (VHF)

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

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

2.3.2.3.2.4 Ultra High Frequency (UHF)

2.3.2.3.2.4.1 UHF Radio

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

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

2.3.2.3.2.4.2 Anti-jamming Capability

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

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

2.3.2.3.2.5 Super High Frequency (SHF)

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

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

2.3.2.3.2.6 Link 16 Transmission Standards

For communicating with the JTIDS/MIDS radios the following standard is mandated:

- STANAG 4175, Edition 1, Technical Characteristics of the Multifunctional Information Distribution System (MIDS), 29 August 1991.

2.3.2.3.3 Synchronous Optical Network (SONET) Transmission Facilities

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

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

The citation of applicable ANSI standards for SONET does not assure 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.

2.3.2.4 Network and Systems Management

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

2.3.2.4.1 Data Communications Management

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

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

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

- IETF Standard 16/RFC-1155/RFC-1212, Structure of Management Information, May 1990.
- IETF Standard 17/RFC-1213, Management Information Base, March 1991.
- IETF RFC-1514, Host Resources MIB, September 1993.
- IETF Standard 50/RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994.
- IETF RFC-1757, Remote Network Monitoring Management Information Base, (RMON Version 1), February 1995.
- IETF RFC-1850, Open Shortest Path First (OSPF) Version 2 Management Information Base, November 1995.

2.3.2.4.2 Telecommunications Management

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

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

2.3.3 Emerging Information Transfer Standards

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

2.3.3.1 End-system Standards

2.3.3.1.1 Internet Standards

IP Next Generation/Version 6 (IPv6). IPv6 is being designed to provide better internetworking capabilities than are currently available within IP (Version 4). IPv6 will include support for the following: expanded addressing and routing capabilities, authentication and privacy, autoconfiguration, and increased quality of service capabilities. IPv6 is described in the following proposed IETF standards: RFC-1883 (IPv6 Specification), RFC-1884 (IPv6 Addressing Architecture), RFC-1885 (ICMPv6 for IPv6), and RFC-1886 (DNS Extensions to Support IPv6).

Dynamic Domain Name System (DDNS). The DDNS protocol defines extensions to the DNS to enable DNS servers to accept requests to update the DNS database dynamically. DDNS is referenced in RFC 2136.

Lightweight Directory Access Protocol 3 (LDAPv3). The proposed standard for LDAPv3, IETF RFC 2251, supports standard based authentication, referrals, and all protocol elements of LDAP (IETF RFC 1777). Other features still under development include standards based access control, signed operations, replication, knowledge references, and paged results.

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

Integrated Services and Resource Reservation Protocol (RSVP). The IETF is currently developing an architecture for providing services over the internet beyond the current best-effort IP based service. This work is described in the Integrated Services Architecture (RFC 1633) which provides an informational overview of this work. This effort is extending the capabilities of the current, "stateless" IP protocol to incorporate "soft state" information. Network elements, which include end-systems and routers, will exchange Quality of Service (QoS) information in order to reserve resources for a particular information flow between a sender and receiver. Key components in the Integrated Services Architecture are: (1) Packet Scheduler for controlling when packets are forwarded; (2) Packet Classifier for determining whether a packet received relates to a particular flow; (3) Admission Control for determining whether a particular flow requested can be supported or not and (4) Reservation Setup Protocol which defines how network elements exchange flow information in order to set up a "soft state" which allows a particular QoS to be achieved. Currently the IETF is standardizing a Reservation Setup Protocol named ReSerVation Protocol (RSVP) and a number of protocols for running the Integrated Services over a variety of subnet types (including LANs, ATM, and low speed links). Two Integrated Services service types are being defined at this time for data flows involving guaranteed (bandwidth and latency) and controlled load data flows.

2.3.3.1.2 Video Teleconferencing (VTC) Standards

Federal Telecommunications Recommendation (FTR) 1080-1997 will be updated by a revision to its Appendix A. The updated document will include multimedia applications such as shared whiteboard and still image annotation, and additional security specifications. ITU-T H.321 and ITU-T H.323 are two emerging recommendations that support VTC over ATM and Ethernet networks, respectively. Also, ITU-T H.310, Broadband Audiovisual Communication Systems and Terminals, ratified November 1996, is an umbrella standard for VTC over high bandwidth (ATM) communication links. H.310 includes underlying standards for video (MPEG2), and audio (MPEG1, MPEG2). H.310 is used for high quality VTC requiring > 2 Mbits/s infrastructure. In the T.120 series of multimedia standards, T.128, Application Sharing, is a draft standard pending approval.

2.3.3.1.3 Space Communication Protocol Standards

The DoD has joined a cooperative effort with the National Aeronautics and Space Administration (NASA) and the National Security Agency (NSA) to develop the Space Communication Protocol Standards (SCPS), September 1997. The cognizant DoD office is SMC/AXE. The SCPS protocol suite will increase the reliability of data transfer, increase interoperability with both DoD and non-DoD assets, and decrease the cost of operating our space systems. The suite consists of a set of four protocols that operate at the network layer and above of the Open Systems Interconnect (OSI) model.

1. The File Handling Protocol (FP) is an application layer protocol (layer 7 in the OSI model) that was derived from the Internet file transfer protocol (FTP). FP is more capable than FTP in that individual records within a file can be updated in addition to the entire file. Another important feature of FP is that a file transfer can be automatically restarted after an interruption.
2. The Transport Protocol (TP) is a transport layer protocol (layer 4 in the OSI model) that was derived from the Internet transmission control protocol (TCP). TP can provide better end-to-end throughput in the space environment because it can respond to corruption in addition to congestion, it implements a TCP window scaling option, and it uses selective negative acknowledgments.
3. The Security Protocol (SP) is based on the security protocol at layer 3 (SP3) and the network layer security protocol (NLSP) with reduced overhead. SP does not have a corresponding layer in the OSI sense. It operates between the network and transport layers (layers 3 and 4).
4. The Network Protocol (NP) is a network layer protocol (layer 3 in the OSI model) that was developed to be a bit-efficient, scaleable protocol for a broad range of spacecraft environments. Among other things, NP provides for a selectable routing method, connectionless and managed connection operations, corruption and congestion signaling to TP, and handling of packet precedence.

Four MIL STDs have been developed and approved for the SCPS protocol suite. The MIL-STDs include:

1. MIL-STD-2045-44000: Department of Defense Interface Standard: Transport Protocol for High-Stress, Resource-Constrained Environments, 30 September 1997.
2. MIL-STD-2045-43000: Department of Defense Interface Standard: Network Protocol for High-Stress, Resource-Constrained Environments, 30 September 1997.
3. MIL-STD-2045-47000: Department of Defense Interface Standard: File and Record Transfer Protocol for Resource-Constrained Environments, 30 September 1997.

4. MIL-STD-2045-43001: Department of Defense Interface Standard: Network Security Protocol for Resource-Constrained Environments, 30 September 1997.

2.3.3.2 Network Standards

Wireless LAN. The IEEE 802.11 Wireless LAN protocol was finalized in June 1997 as IEEE 802.11-1997 Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. It provides a common set of operational rules for airwave interoperability of wireless LAN products from different vendors. It specifies both direct-sequence spread-spectrum and frequency-hopping spread-spectrum physical layers for wireless radio based LANs. Also, it includes infrared connectivity technologies. An Inter Access Point protocol is being developed to provide a standardized method for communications between wireless LAN access points.

ATM-related Standards. The ATM Forum has developed new Version 4.0 standards for UNI signaling (af-sig-0061.000), signaling ABR addendum (af-sig-0076.000), integrated local management (af-ilmi-0065.000), traffic management (af-tm-0056.000) and traffic management ABR addendum (af-tm-0077.000). Since ATM is essentially a packet rather than circuit oriented transmission technology, it must emulate circuit characteristics in order to provide support for CBR or "circuit" (voice and telephony) traffic over ATM. For voice and telephony, the following two ATM Forum standards were approved: Circuit Emulation Service Interoperability Specification, af-vtoa-0078.000, and ATM trunking using AAL1 for Narrowband Services Version 1.0, af-vtoa-0089.000.

LANE Version 2.0 LANE UNI (LUNI) specification and the MultiProtocol Over ATM (MPOA) Version 1.0 specification were recently approved by the ATM Forum. The LANE Version 2.0 LUNI, af-lane-0084.000, standardizes the interface between the LANE client (the LEC) and the LANE Server (the LES, LECS, and BUS). MPOA Version 1.0, af-mpoa-0087.000, provides for the support of multiple network layer protocols over ATM.

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

Personal Communications Services (PCS) and Mobile Cellular. PCS will support both terminal mobility and personal mobility. Terminal mobility is based on wireless access to the public switched telephone network (PSTN). Personal mobility allows users of telecommunication services to gain access to these services from any convenient terminal (either wireline or wireless). Mobile cellular radio can be regarded as an early form of 'personal communications service' allowing subscribers to place and receive telephone calls over the PSTN wherever cellular service is provided. The three predominant competing world-wide methods for digital PCS and Mobile Cellular access are: Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), and Global System for Mobile Communications (GSM). Of these three, CDMA offers the best technical advantages for military applications based on its utilization of Direct Sequence Spread Spectrum (DSSS) techniques for increased channel capacity, low probability of intercept (LPI), and protection against jamming. CDMA's low transmission power requirements should also reduce portable power consumption. The PCS standard for CDMA is J-STD-008. The Mobile Cellular standard for CDMA is IS-95-A. In North America, the standard signaling protocol for CDMA and TDMA mobile cellular is IS-41-C. It should be recognized that for Operations-Other-Than-War (OOTW), a user may require support of multiple protocols to access region-specific international digital PCS/Mobile Cellular infrastructures.

International Mobile Telecommunications - 2000 (IMT-2000). IMT-2000 defines third generation mobile systems which are scheduled to start service around the year 2000, subject to market conditions. Also known as Future Public Land Mobile Telecommunications Systems (FPLMTS), these systems will provide access by means of one or more radio links to a wide variety of telecommunication services supported by the fixed and mobile telecommunications networks (e.g. PSTN/ISDN), and to other services which may be unique to IMT-2000. A range of mobile terminal types, designed for mobile and fixed use, is envisaged linking to terrestrial and/or satellite-based networks. A goal for third generation mobile systems is to provide global coverage and to enable terminals to be capable of seamless roaming between multiple networks. The ability to coexist and work with pre-IMT-2000 systems is required.

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

2.3.3.3 Military Satellite Communications (MILSATCOM)

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

2.3.3.4 Radio Communications

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

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

2.3.3.5 Network Management

Network Management Systems for Data Communications. The following SNMP MIB modules are identified as emerging IETF standards for implementation within systems that manage data communications networks: (1) Asynchronous Transfer Mode (ATM) MIB, RFC 1695 - defines a set of standard objects for managing ATM switches. (2) Border Gateway Protocol version 4 (BGP-4) MIB, RFC 1657 - defines a set of standard objects for managing this internetwork routing protocol. (3) Domain Name Service (DNS) MIBs, RFCs 1611 and 1612 - define a set of standard objects for managing this name server and name resolver services. (4) Internetwork Protocol (IP) MIBs, RFCs 2006 and 2011 - define a set of standard objects for managing this traditional static IP and emerging mobile IP services. (5) Point-to-Point Protocol (PPP) MIBs, RFCs 1471 through 1474 - define a set of standard objects for managing PPP links, security, IP network level, and bridge level services. (6) Remote Network Management Monitoring Version 2 (RMON2) MIB, RFC 2021 - defines a set of standard objects for monitoring protocol communications services across a subnetwork across all seven layers of the OSI model. (7) Transmission Control Protocol (TCP) MIB, RFC 2012 - defines a set of standard objects for managing a system's TCP services. (8) User Datagram Protocol (UDP) MIB, RFC 2013 - defines a set of standard objects for managing a system's UDP services. (9) Directory Services MIB, RFC 1567 - currently defines a set of standard objects for monitoring X.500 directory services. and is being updated to add support for LDAP. (10) Network Services MIB, RFC 2248 – defines MIB that serves as a basis for application specific monitoring and management. (11) Mail Monitoring MIB, RFC 2249 – allows for the monitoring of Message Transfer Agents (MTAs).

This page intentionally left blank.

2.4 INFORMATION MODELING, METADATA, AND INFORMATION EXCHANGE STANDARDS

2.4.1 Introduction

2.4.1.1 Purpose

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

2.4.1.2 Scope

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

Security standards related to this section are in Section 2.6.2.4.

2.4.1.3 Background

An information model is a representation at one or more levels of abstraction of a set of real-world activities, products, and/or interfaces. Within the Information System (IS) domain, there are two basic types of models frequently created: activity and data.

Activity models are representations of mission area applications, composed of one or more related activities. Information required to support the mission area function is the primary product of each activity model. An activity model is also referred to as a function or process model.

Data models, developed from the information requirements documented in the activity model, define entities, their data elements and illustrate the interrelationships among the entities. The data model identifies the logical information requirements and metadata, which forms a basis for physical database schemata and standard data elements.

In order to provide an authoritative source for DoD data standards, the DoD created the Defense Data Dictionary System (DDDS). The DDDS, managed by DISA, is a DoD-wide central database that includes standard names and definitions for data entities and data elements (i.e., attributes). The DDDS server also provides password-protected access to DoD standard data models. The DDDS is used to collect individual data standards derived from the DoD data model (DDM) and to document content and format for data elements. A classified version of the DDDS, known as the Secure Intelligence Data Repository (SIDR), has been developed to support standardization of classified data elements and domains. System developers use these repositories as a primary source of data element standards.

Information exchange is accomplished for the most part by sending formatted messages. The definition and documentation of these exchange mechanisms are provided by various messaging standards. Each message standard provides a means to define message form and functions (i.e., transfer syntax), which includes the definition of the message elements that are contained in each message. The message fields, which are currently defined in the various message standards, are not necessarily mutually consistent, nor are they consistently based on any activity or data models either within a message system or across message systems. Newer techniques provide more direct exchange of data without the user following a rigid format. A model-based structure will eventually provide definitions which will be data element-based and will be compliant with the DoD data element standards established in accordance with the DoD Directive (DoDD) 8320.1, Data Administration, and associated DoD 8320.1 manuals.

Efficient execution of information exchange requirements (IERs) throughout the joint battlespace is key to evolving the DoD toward the ultimate goal of seamless information exchange. The primary component of this infrastructure is the Tactical Data Link (TDL), composed of message elements/messages and physical media. However, due to the diversity of Warfighter requirements, no single data link is applicable to every platform and weapon system.

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

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

2.4.2 Mandates

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

2.4.2.1 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 forms the basis for data model development or refinement. It is validated against the requirements and doctrine, and approved by the operational sponsor.

The mandated standard for activity modeling is:

- FIPS PUB 183, Integration Definition for Function Modeling (IDEF0), December 1993.

2.4.2.2 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, including message formats and schema for shared databases. The DoD Data Model (DDM) is a department-wide logical data model which provides the standard definition and use of specific data elements to the developers of all DoD systems. Command and control systems will incorporate applicable Command and Control (C2) Core Data Model (C2CDM) requirements. The C2CDM is a subset of the DDM.

Implementation of the DDM and C2CDM will be interpreted to mean that the DDM and C2CDM will serve as the logical database schema defining the names, representations, and relations of data within DoD systems. System developers comply by using this database schema as the basis of their own physical database schemas. Developers of new and existing systems will maintain traceability between their physical database schema and the DDM and C2CDM, as applicable, by registering the use of the data standards in the DDDS. Information regarding access to the DDM and C2CDM can be obtained from the DoD Data Administration World Wide Web home page at:

http://www-datadmn.itsi.disa.mil/

Adherence to the DDM will aid DoD agencies in becoming data interoperable among all information systems. The information requirements of a new or major system upgrade will be documented within a data model based on the DDM. New information requirements are submitted by DoD Components and approved by functional data stewards in accordance with DoD Manual 8320.1-M-1, DoD Data Standardization Procedures. These information requirements will be used to extend the DDM and C2CDM, as appropriate.

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

- DoD Manual 8320.1-M-1, DoD Data Standardization Procedures, April 1998 (which mandates the use of the DDM).
- FIPS PUB 184, Integration Definition For Information Modeling (IDEF1X), December 1993.

2.4.2.3 DoD Data Definitions

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

The mandated standards for DoD Data Definitions are:

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

2.4.2.3.1 DoD Date Standards

In order to ensure the unambiguous exchange of date data between systems before, during, and past the year 2000, database design and data modeling shall adhere to DoD date data standards. For external exchange of character dates between systems not using a standardized message or transaction format, the mandated standards are:

- Calendar Date: DDDS Counter ID # 195
  Format: YYYYMMDD (8-digit contiguous)

Where: YYYY = year; MM = month; DD = day
(Also referenced in ISO 8601, ANSI X3.30, and FIPS 4-1)

- Ordinal Date: DDDS Counter ID # 165
  Format: YYYYDDD (7-digit contiguous)
  Where: YYYY = year; DDD = ordinal day within year
  (Also referenced in ISO 8601)
- Year Date: DDDS Counter ID #166
  Format: YYYY (4-digit contiguous)
  Where: YYYY = year
  (Also referenced in ISO 8601)

2.4.2.4 Information Exchange Standards

2.4.2.4.1 Information Exchange Standards Applicability

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

A. The exchange of information among applications shall be based on the logical data models developed from identifying information requirements through activity models, where appropriate. The data model identifies the logical information requirements, which shall be developed into physical database schemata and standard data elements.

B. The standard data elements shall be exchanged using the data management, data interchange, and distributed computing services of application platforms. (Refer to Section 2.2 for further guidance on these services.) The goal is to exchange information directly between information systems, subject to security classification considerations.

For purposes of clarification, Information Exchange Standards refer to the system or application-independent ability of data to be shared, whereas Data Interchange is system or application-specific. Hence, this section discusses information exchange standards as the generic ability of a system or application to share data. Interchange standards help form the DII Common Operating Environment (COE) ensuring the use of system or application formats which can share data. Key references include Section 2.2.2.2.1.3, for SQL standards in Data Management Services and Section 2.2.2.2.1.4 for Data Interchange Services.

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

2.4.2.4.2 Tactical Information Exchange Standards

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

2.4.2.4.2.1 Bit-oriented Formatted Messages

The J-Series Family of TADILs allow information exchange using common data element structures and message formats which support time-critical information. They include Air Operations/Defense Maritime, Fire Support, and Maneuver Operations. These are the primary data links for exchange of bit-oriented information. The family consists of LINK 16, LINK 22, and the Joint Variable Message Format (VMF) and interoperability is achieved through use of J-Series family messages and data elements. The policy and management of this family is described in the Joint Tactical Data Link Management Plan (JTDLMP), dated 6 June 1996.

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

- MIL-STD-6016, Tactical Digital Information Link (TADIL) J Message Standard, 7 February 1997.
- STANAG 5516, Edition 1, Tactical Data Exchange - LINK 16, Ratified 15 January 1997.
- Joint Interoperability of Tactical Command and Control Systems Variable Message Format (VMF) Technical Interface Design Plan (Test Edition) Reissue 2, August 1996.

2.4.2.4.2.2 Character-based Formatted Messages

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

- MIL-STD-6040, United States Message Text Format (USMTF), 1 January 1997.

Note: MIL-STD-6040 is published every January with an implementation in the following January.

2.4.3 Emerging Standards

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

2.4.3.1 Activity Modeling

The emerging standard for activity modeling is IEEE P1320.1, IDEF0 Function Modeling, currently under development by a working group of the Software Engineering Standards Committee of the IEEE Computer Society. The standard extends FIPS PUB 183 by specifying detailed syntax and semantics for the IDEF0 language. The IDEF0 language deals with the constructs, semantics and syntax of the function modeling. The IDEF0 language is used to produce a function model which is a structured representation of the functions of a system or environment, and the information and objects which interrelate those functions. The intent of the IEEE standard is not to significantly change the notation described in FIPS PUB 183 but rather to improve the definition of it.

2.4.3.2 Data Modeling

The emerging standards for data modeling are IDEF1X97, Conceptual Schema Modeling and the Unified Modeling Language (UML). These standards accommodate object-oriented methods (OOM):

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

Unified Modeling Language (UML). UML (Rational Corp., Version 1.0, January 1997) is a language for specifying, constructing, visualizing, and documenting the artifacts of a software-intensive system. In an elaborative approach, developers develop models and increasingly add details until the model becomes the actual system being developed. The UML is being submitted to the Object Management Group (OMG) for adoption as an industry standard. Information may be obtained from the World Wide Web at:

http://www.rational.com.

2.4.3.3 DoD Data Definitions

DISA Joint Interoperability and Engineering Organization (JIEO), in coordination with the Standards Coordinating Committee (SCC) and the Change Control Board (CCB), will develop the strategy/policy for migration from many tactical data link (bit-oriented) and character-oriented joint message standards to a minimal family of DoD 8320.1-compliant information exchange standards. A normalized unified data/message element dictionary will be developed based on normalized Data Model and associated data element standards. The dictionary will support both character and bit-oriented representation of the standard data and their domain values. Message standards will then establish the syntax for standard data packaging to support mission requirements (e.g., character or bit-oriented, fixed or variable format, etc.). The unified data dictionary will ensure that multiple representations are minimized and transformation algorithms are standardized. The Data Model basis for the data elements will ensure the information is normalized.

2.4.3.4 Information Exchange Standards

The emerging standards for information exchange are:

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

2.5 HUMAN-COMPUTER INTERFACE STANDARDS

2.5.1 Introduction

2.5.1.1 Purpose

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

2.5.1.2 Scope

This section addresses the presentation and dialogue levels of the Human-Computer Interface. Section 2.2 addresses the application program interface (API) definitions and protocols. See Section 2.6.2.5 and Appendix A of the DoD HCI Style Guide, Security Presentation Guidelines, and other applicable portions of the DoD HCI Style Guide for HCI Security.

2.5.1.3 Background

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

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

2.5.2 Mandates

This subsection identifies the mandatory standards, profiles, and practices for human-computer interfaces. Each mandated standard or practice is clearly identified on a separate line, and includes a formal reference that can be included within Requests for Proposals (RFP) or Statements of Work (SOW). Appendix B contains a table that summarizes the mandated standards from this section, as well as providing information on how to obtain the standards.

2.5.2.1 General

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

2.5.2.1.1 Character-based Interfaces

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

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

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

2.5.2.1.2 Graphical User Interface

When developing DoD automated systems, the graphical user interface shall be based on one commercial user interface style guide consistent with Section 2.5.2.2.1. Hybrid GUIs that mix user interface styles (e.g., Motif with Microsoft Windows) shall not be created. A hybrid GUI is a GUI that is composed of toolkit components from more than one user interface style. When selecting commercial off-the-shelf (COTS)/government off-the-shelf (GOTS) applications for integration with developed DoD automated systems, maintaining consistency in the user interface style is highly recommended.

See Section 2.2.2.2.1.2 for mandated GUI standards.

2.5.2.2 Style Guides

An HCI style guide is a document that specifies design rules and guidelines for the look and behavior of the user interaction with a software application or a family of software applications. The goal of a style guide is to improve human performance and reduce 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 which define "how" the rules are implemented in the HCI application code.

Figure 2.5-1 illustrates the hierarchy of style guides that shall be followed to maintain consistency and good HCI design within the DoD. This hierarchy, when applied according to the process mandated in the DoD HCI Style Guide, provides a framework that supports iterative prototype-based HCI development. The process starts with top-level general guidance and uses prototyping activities to develop system-specific design rules.

The interface developer shall use the selected commercial GUI style guide, refinements provided in the DoD HCI Style Guide, and the appropriate domain-level style guide 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.

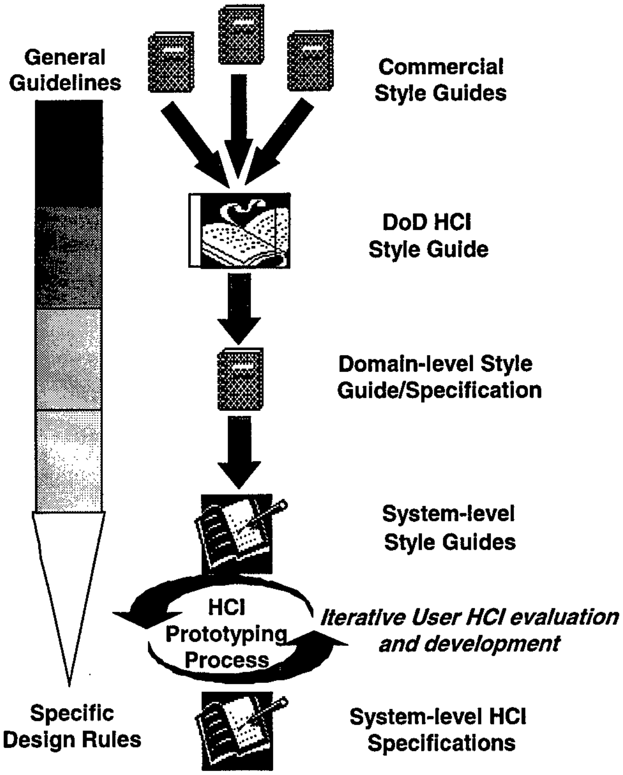

General Guidelines
Commercial Style Guides
DoD HCI Style Guide
Domain-level Style Guide/Specification
System-level Style Guides
HCI Prototyping Process
Iterative User HCI evaluation and development
Specific Design Rules
System-level HCI Specifications

Figure 2.5-1 HCI Development Guidance

2.5.2.2.1 Commercial Style Guides

A commercial GUI style shall be selected as the basis for user interface development. The GUI style selected is usually driven by the mandates specified in Section 2.2 (User Interface Services and Operating System Services).

2.5.2.2.1.1 X-Window Style Guides

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

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

For systems required to interface with the Defense Information Infrastructure (DII) Common Operating Environment (COE), the following specification is mandated:

- TriTeal Enterprise Desktop (TED) 4.0 Style Guide and Certification Checklist, Carlsbad, CA: TriTeal Corporation, 1995.

2.5.2.2.1.2 Windows Style Guide

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

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

2.5.2.2.2 DoD Human-Computer Interface (HCI) Style Guide

The DoD HCI Style Guide is a high level document which allows consistency across DoD systems without undue constraint on domain and system level implementation. The DoD HCI Style Guide (Volume 8 of the TAFIM Version 3.0) was developed as a guideline document presenting recommendations for good Human-Computer Interface design. This document focuses on Human-Computer behavior and concentrates on elements or functional areas that apply to DoD applications. These functional areas include such things as security classification display, mapping display and manipulation, decision aids, and embedded training. This style guide, while emphasizing commercial GUIs, contains guidance that can be used for all types of systems including those which employ character-based interfaces. Although the DoD HCI Style Guide is not intended to be strictly a compliance document, it does represent DoD policy.

The following guideline is mandated:

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

The general principles given in this document apply to all interfaces; some specialized areas, however, require separate consideration. Specialized interfaces, such as those used in hand-held devices, have interface requirements that are beyond the scope of the DoD HCI Style Guide. These systems shall comply with their domain-level style guide and follow the general principles and HCI design guidelines presented in the DoD HCI Style Guide.

2.5.2.2.3 Domain-level Style Guides

The JTA allows for the development of domain-level HCI style guides. These style guides will reflect the consensus on HCI appearance and behavior for a particular domain within the DoD. The domain-level style guide will be the compliance document and may be supplemented by a system-level style guide.

The following domain-level style guide is mandated for Motif-based systems.

- User Interface Specification for the Defense Information Infrastructure (DII), Version 2.0, June 1996.

2.5.2.2.4 System-level Style Guides

System-level style guides provide the special tailoring of commercial, DoD, and domain-level style guides. These documents include explicit design guidance and rules for the system, while maintaining the appearance and behavior provided in the domain-level style guide. If needed, the Motif-based system-level style guide will be created in accordance with the User Interface Specification for the DII.

2.5.2.3 Symbology

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

- MIL-STD-2525A, Common Warfighting Symbology, 15 December 1996.

2.5.3 Emerging Standards

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

Motif 2.1 Style Guide is published as part of the CDE 2.1 documentation, and is expected to be mandated.

Most Web-based interfaces use Hypertext Markup Language (HTML) to describe the structure of the information they contain. The next version of the DoD HCI Style Guide and the User Interface Specifications for the DII are expected to address HTML-based interfaces. The next version of the User Interface Specification for the DII addresses Win32-based interfaces.

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

Work to standardize data labeling for classified electronic and hardcopy documents is in progress. The results of this effort will replace the labeling standards currently appearing in Appendix A of the DoD HCI Style Guide, TAFIM, Version 3.0, Volume 8, 30 April 1996.

2.6 INFORMATION SYSTEMS SECURITY STANDARDS

2.6.1 Introduction

2.6.1.1 Purpose

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

2.6.1.2 Scope

The standards mandated in this section apply to all DoD information technology systems. This section provides the security standards applicable to information processing, transfer, modeling and standards, and Human-Computer Interfaces (HCI). This section also addresses standards for security audit and key management mechanisms. Subsection 2.6.2 addresses mandated security standards, and subsection 2.6.3 addresses emerging security standards.

2.6.1.3 Background

The Technical Architecture Framework for Information Management (TAFIM) provides a blueprint for the Defense Information Infrastructure (DII), capturing the evolving vision of a common, multipurpose, standards-based technical infrastructure. The DoD Goal Security Architecture (DGSA), Volume 6 of the DoD TAFIM, dated 30 April 1996, provides a comprehensive view of the architecture from the security perspective. The DGSA is a generic architectural framework for developing mission-specific security architectures; it includes security services for information systems (authentication, access control, data integrity, data confidentiality, non-repudiation, and availability). Although advancements in security theory and technology are needed to develop systems that are consistent with DGSA, the DGSA concepts and principles can be incorporated into current systems.

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

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

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

Security requirements and engineering should be determined in the initial phases of design. The determination of security services to be used and the strength of the mechanisms providing the services are primary aspects of developing the specific security architectures to support specific domains. Section 2.6 of the JTA is used after operational architectural decisions are made regarding the security services needed and the required strengths of protection of the mechanisms providing those services.

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

2.6.2 Mandates

This subsection identifies the mandatory standards, profiles, and practices for information systems security standards. Each mandated standard or practice is clearly identified on a separate line, and includes a formal reference that can be included within Requests for Proposals (RFP) or Statements of Work (SOW). Appendix B contains a table that summarizes the mandated standards from this section, as well as providing information on how to obtain the standards.

2.6.2.1 Introduction

This section contains the mandatory information systems security standards and protocols that shall be implemented in systems that have a need for the corresponding interoperability-related services. If a service is to be implemented, then it shall be implemented at the required level of protection using the associated security standards in this section. If a service is specified by more than one standard, the appropriate standard should be selected based on system requirements. Section 2.6.2 is structured to mirror the overall organization of the JTA so that readers can easily link security topics with the related subject area in the sections of the JTA (information processing; information transfer; information modeling, metadata, and information exchange; and human-computer interface) and their subsections.

2.6.2.2 Information Processing Security Standards

Technical evaluation criteria to support information system security policy, and evaluation and approval, disapproval, and accreditation responsibilities are promulgated by DoD Directive (DoDD) 5200.28. Based on the required level of trust, the following information processing security standards are mandated.

2.6.2.2.1 Application Software Entity Security Standards

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

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

If FORTEZZA services are used, the following are mandated:

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

2.6.2.2.2 Application Platform Entity Security Standards

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

2.6.2.2.2.1 Data Management Services

The following standard is mandated for data management services consistent with the required level of trust:

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

2.6.2.2.2.2 Operating System Services Security

For the application platform entity, the following standard is mandated for the acquisition of operating systems consistent with the required level of trust:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985.

2.6.2.2.2.2.1 Security Auditing and Alarms Standards

Security auditing is a review or examination of records and activities to test controls, ensure compliance with policies and procedures, detect breaches in security, and indicate changes in operation. Security alarm reporting is the capability to receive notifications of security-related events, alerts of any misoperations of security services and mechanisms, alerts of attacks on system security, and information as to the perceived severity of any misoperation, attack, or breach of security.

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

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985.

2.6.2.2.2.2.2 Authentication Security Standards

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

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

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

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

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

2.6.2.3 Information Transfer Security Standards

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

2.6.2.3.1 End-system Security Standards

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

2.6.2.3.1.1 Host Security Standards

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

For systems required to interface with Defense Message System, the following standard is mandated:

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

2.6.2.3.1.1.1 Security Algorithms

To achieve interoperability, products must support a common transport protocol. Transport protocols must agree on a common cryptographic message syntax, cryptographic algorithms, and modes of operations (e.g., cipher block chaining). Transport protocols support negotiation mechanisms for selecting common syntax, algorithms, and modes of operation.

The following paragraphs identify security standards that shall be used for the identified types of cryptographic algorithms.

Message digest or hash algorithms are one-way functions which create a "fingerprint" of a message. They provide data integrity when used in conjunction with other cryptographic functions. If message digest or hash algorithms are required, Key Recovery will be implemented in the certificate management hierarchy. The NSA developed encryption algorithm SKIPJACK is mandated:

- SKIPJACK, NSA, R21-TECH-044, 21 May 1991.

Digital signatures provide strong identification and authentication. Related standards include public key certificate standards (X.509) and directory service standards (X.500). If digital signature is required, the following standard is mandated:

- FIPS PUB 186, Digital Signature Standard, May 1994.

Encryption prevents unauthorized disclosure of information during transmission. Systems processing classified information must use a Type 1 NSA-approved encryption product, which can also be used to encrypt sensitive but unclassified information.

Key exchange algorithms allow two parties to exchange encryption keys without relying on out-of-band communications. In FORTEZZA applications, the following NSA-developed Type II key exchange algorithm is mandated:

- Key Exchange Algorithm, NSA, R21-TECH-23-94, 12 July 1994.

2.6.2.3.1.1.2 Security Protocols

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

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

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

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

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

- ACP-120, Allied Communications Publication 120, Common Security Protocol, CSP, 1997.

The following key management protocol is mandated:

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

2.6.2.3.1.1.3 Evaluation Criteria Security Standards

The following standards are mandated consistent with the required level of trust:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985.
- NCSC-TG-005, Version 1, Trusted Network Interpretation, July 1987.

2.6.2.3.2 Network Security Standards

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

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

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

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

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

2.6.2.3.3 Transmission Media Security Standards

There are currently no security standards mandated for transmission media.

2.6.2.4 Information Modeling, Metadata, and Information Security Standards

At this time, no information modeling, metadata, and information security standards are mandated. Process models and data models produced should be afforded the appropriate level of protection. (Ref: NCSC-TG-010, October 1992, A Guide to Understanding Security Modeling in Trusted Systems).

2.6.2.5 Human-Computer Interface Security Standards

DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria (TCSEC), December 1985, specifies the minimal security requirements associated with a required level of protection for DoD automated systems. HCI security-related requirements may include authentication, screen classification display, and management of access control workstation resources.

For systems employing graphical user interfaces, the following guideline is mandated:

- DoD Human-Computer Interface Style Guide, TAFIM Version 3.0, Volume 8, 30 April 1996.

2.6.3 Emerging Standards

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

2.6.3.1 Introduction

The emerging security standards described in this section are drawn from work being pursued by ISO, IEEE, IETF, Federal standards bodies, and consortia such as the Object Management Group (OMG). Section 2.6.3 is structured to mirror the overall organization of the JTA so that readers can easily link security topics with the related subject area in the sections of the JTA (information processing; information transfer; information modeling, metadata, and information exchange; and human-computer interface) and their subsections.

2.6.3.2 Information Processing Security Standards

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

2.6.3.2.1 Application Software Entity Security Standards

Emerging application software entity standards include evaluation criteria and World Wide Web (WWW) security-related standards.

2.6.3.2.1.1 Evaluation Criteria Security Standards

The Evaluation Criteria for Information Technology Security (Common Criteria) represents the outcome of efforts to develop criteria for evaluation of IT security that are widely useful within the international community. It is an alignment and development of a number of the existing European, US. and Canadian criteria (ITSEC, TCSEC and CTCPEC respectively). The Common Criteria resolves the conceptual and technical differences between the source criteria. It is a contribution to the development of an international standard, and opens the way to worldwide mutual recognition of evaluation results (ISO/IEC JTC1/SC27/WG3 N304, 23 April 1996).

2.6.3.2.1.2 World Wide Web Security Standards

"The Transport Layer Security (TLS) Protocol, Version 1.0," Tim Dierks (Consensus Development), Christopher Allen (Consensus Development), 21 May 1997, draft-ietf-tls-protocol-03.txt, which incorporates the Secure Sockets Layer (SSL) Protocol Version 3.0, 18 November 1996, is an Internet Engineering Task Force (IETF) Draft document supporting WWW security, and is being considered for standardization. The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. TLS runs above the transport layer.

2.6.3.2.2 Application Platform Entity Security Standards

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

2.6.3.2.2.1 Software Engineering Services Security

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

2.6.3.2.2.1.1 Generic Security Service (GSS)-Application Program Interface (API) Security

The GSS-API, as defined in RFC-1508, September 1993 (IETF), provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments. RFC-1508 defines GSS-API services and primitives at a level independent of underlying mechanism and programming language environment. RFC-2078, "GSS-API, Version 2.0," J. Linn, January 1997, revises RFC-1508, making specific, incremental changes in response to implementation experience and liaison requests.

The IETF Draft, "Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)," C. Adams, 25 March 1997, draft-ietf-cat-idup-gss-07.txt, extends the GSS-API (RFC-1508) for non-session protocols and applications requiring protection of a generic data unit (such as a file or message) in a way which is independent of the protection of any other data unit and independent of any concurrent contact with designated "receivers" of the data unit. An example application is secure electronic mail where data needs to be protected without any on-line connection with the intended recipient(s) of that data. Subsequent to being protected, the data unit can be transferred to the recipient(s) – or to an archive - perhaps to be processed as unprotected days or years later.

2.6.3.2.2.1.2 POSIX Security Standards

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

- IEEE P1003.1e, POSIX Part 1: System API - Protection, Audit, and Control Interfaces [C Language], Draft, 16 June 1997.
- IEEE P1003.2c, POSIX Part 2: Shell and Utilities - Protection and Control Interfaces, Draft, 16 June 1997.

These draft standards define security interfaces to open systems for access control lists, audit, privilege, mandatory access control, and information label mechanisms and are stated in terms of their C bindings.

2.6.3.2.2.2 Operating System Services Security

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

2.6.3.2.2.2.1 Evaluation Criteria Security Standards

See Section 2.6.3.2.1.1 for a description of the emerging Common Criteria. It is expected that the evolving Common Criteria Protection Profiles will replace those references to the Orange Book (e.g., Orange Book Class C2 would equate to a specific Common Criteria Protection Profile). More information on Common Criteria Protection Profiles is available on NIST's World Wide Web home page at:

http://csrc.nist.gov/nistpubs/cc

2.6.3.2.2.2 Authentication Security Standards

IETF RFC-1938, "A One-Time Password System," May 1996, provides authentication for system access (login), and other applications requiring authentication, that is secure against passive attacks based on replaying captured reusable passwords. The One-Time Password System evolved from the S/KEY One-Time Password System that was released by Bellcore.

When Remote Dial In Authentication is required, the following standard may be used:

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

2.6.3.2.2.3 Distributed Computing Services Security Standards

DCE Authentication and Security Specification (P315) 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.

2.6.3.3 Information Transfer Security Standards

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

2.6.3.3.1 End-system Security Standards

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

2.6.3.3.1.1 Host Security Standards

Security standards are emerging for host end systems in the security protocols and public key infrastructure areas discussed in the following subsections.

2.6.3.3.1.1.1 Security Protocols

In mid-1996, some significant improvements were proposed to the Secure/Multipurpose Internet Mail Extensions (S/MIME) messaging security protocol and the underlying encapsulation protocol, PKCS#7. With these improvements, S/MIME will provide a business quality security protocol for both the Internet and X.400 messaging environments. The improvements include: (1) algorithm independence; (2) support for digitally signed receipts; (3) support for mail lists; and (4) support for sensitivity labels in signed and unsigned/encrypted messages. This effectively merges S/MIME and Message Security Protocol (MSP) 4.0/ACP-120. In November 1997, the IETF formed the S/MIME security protocol working group to create Internet standards based on S/MIME and these improvements.

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

The following are emerging standards for Local Area Network (LAN) security: IEEE 802.10c/D13, Standard for Interoperable LAN Security-Part C: Key Management, and IEEE 802.10g/D7, Secure Data Exchange Label, 1995.

2.6.3.3.1.1.2 Public Key Infrastructure Security Standards

FIPS PUB 196, Entity Authentication Using Public Key Cryptography, 18 February 1997, is based on ISO/IEC 9798-3: 1993, Entity Authentication Using a Public Key System and will provide a standard for Public Key Cryptographic Entity Authentication Mechanisms for use in public key-based challenge-response and authentication systems at the application layer within computer and digital telecommunications systems.

2.6.3.3.2 Network Security Standards

Emerging network standards are listed in Section 2.6.3.3.2.1.

2.6.3.3.2.1 Internetworking Security Standards

RFC-1825, "Security Architecture for the Internet Protocol," R. Atkinson, August 1995, describes the security mechanisms for IP version 4 (IPv4) and IP version 6 (IPv6) and the services that they provide. Each security mechanism is specified in a separate document. RFC-1825 also describes key management requirements for systems implementing those security mechanisms. It is not an overall Security Architecture for the Internet, but focuses on IP-layer security.

The Internet Draft "IP Authentication Header (AH)," Stephen Kent (BBN Corp.), Randall Atkinson (@Home Network), 30 May 1997, draft-ietf-ipsec-auth-05.txt, describes a mechanism for providing cryptographic authentication for IPv4 and IPv6 datagrams. An AH is normally inserted after an IP header and before the other information being authenticated. The AH is a mechanism for providing strong integrity and authentication for IP datagrams. It might also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed.

The Internet Draft "IP Encapsulating Security Payload (ESP)," Stephen Kent (BBN Corp), Randall Atkinson (@Home Network), 30 May 1997, draft-ietf-ipsec-esp-04.txt, discusses a mechanism for providing integrity and confidentiality to IP datagrams. In some circumstances, depending on the encryption algorithm and mode used, it can also provide authentication to IP datagrams. Otherwise, the IP AH may be used in conjunction with ESP to provide authentication. The mechanism works with both IPv4 and IPv6.

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

RFC 1829, "The ESP DES-CBC Transform," P. Karn (Qualcomm), P. Metzger (Piermont), W. Simpson (Daydreamer), August 1995. The Encapsulating Security Payload (ESP) provides confidentiality for IP datagrams by encrypting the payload data to be protected. This specification describes the ESP use of the Cipher Block Chaining (CBC) mode of the US Data Encryption Standard (DES) algorithm (FIPS-46, FIPS-46-1, FIPS-74, FIPS-81). All implementations that claim conformance or compliance with the ESP specification must implement this DES-CBC transform.

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

The IETF Draft, "Internet Security Association and Key Management Protocol (ISAKMP)," Douglas Maughan, Mark Schertler, Mark Schneider, Jeff Turner, 21 February 1997, draft-ietf-ipsec-isakmp-07.txt, describes a protocol utilizing security concepts necessary for establishing Security Associations (SAs) and cryptographic keys in an Internet environment. It is expected that the IETF will adopt this protocol as the Internet standard for key and security association management for IPv6 security.

The IETF Draft, "The Resolution of ISAKMP with Oakley," D. Harkins, D. Carrel (Cisco Systems), February 1997, draft-ietf-ipsec-isakmp-oakley-03.txt, describes a proposal for using the Oakley Key Exchange Protocol in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec Domain of Interpretation (DOI). ISAKMP provides a framework for authentication and key exchange but does not define them. ISAKMP is designed to be key exchange independent; that is, it is designed to support many different key exchanges. Oakley describes a series of key exchanges – called "modes" – and details the services provided by each (e.g., perfect forward secrecy for keys, identity protection, and authentication).

The Internet Draft, "The Internet IP Security Domain of Interpretation for ISAKMP," Derrell Piper (Cisco Systems), 28 February 1997, draft-ietf-ipsec-ipsec-doi-02.txt, details the Internet IP Security DOI, which is defined to cover the IP security protocols that use ISAKMP to negotiate their security associations. The ISAKMP defines a framework for security association management and cryptographic key establishment for the Internet. This framework consists of defined exchanges and processing guidelines that occur within a given DOI.

Two IEEE LAN security standards are emerging: IEEE 802.10, IEEE Standards for Local and Metropolitan Area Networks (MANs): Interoperable LAN/MAN Security (SILS), 1992, discusses services, protocols, data formats and interfaces to allow IEEE 802 products to interoperate, and discusses authentication, access control, data integrity, and confidentiality; IEEE 802.10a, Standard for Interoperable LAN Security – The Model, Draft January 1989, shows the relationship of SILS to OSI and describes required interfaces. IEEE 802.10b, Secure Data Exchange, 1992, is incorporated in IEEE 802-10, and deals with secure data exchange at the data link layer.

2.6.3.4 Information Modeling, Metadata, and Information Security Standards

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

2.6.3.5 Human-Computer Interface Security Standards

Refer to Section 2.6.3.2.1.1 for information pertaining to the Common Criteria Protection Profiles emerging standard that is expected to replace DoD 5200.28-STD.

Refer to Section 2.6.3.3.1.1.2 for information pertaining to FIPS PUB 196, Entity Authentication Using Public Key Cryptography, 18 February 1997.

COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) DOMAIN ANNEX

C4ISR.1 DOMAIN OVERVIEW

C4ISR.1.1 PURPOSE

The C4ISR Domain Annex 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 Section 2 of the JTA core. These additions are common to the majority of C4ISR systems and support the functional requirements of C4ISR systems.

C4ISR.1.2 BACKGROUND

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

C4ISR.1.3 DOMAIN DESCRIPTION

The C4ISR domain consists of those integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications whose primary function is to:

- 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; or

– 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.

This annex 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 Combat Support systems include acquisition, finance, human resource, 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 Notional JTA Hierarchy is shown in Figure C4ISR-1.

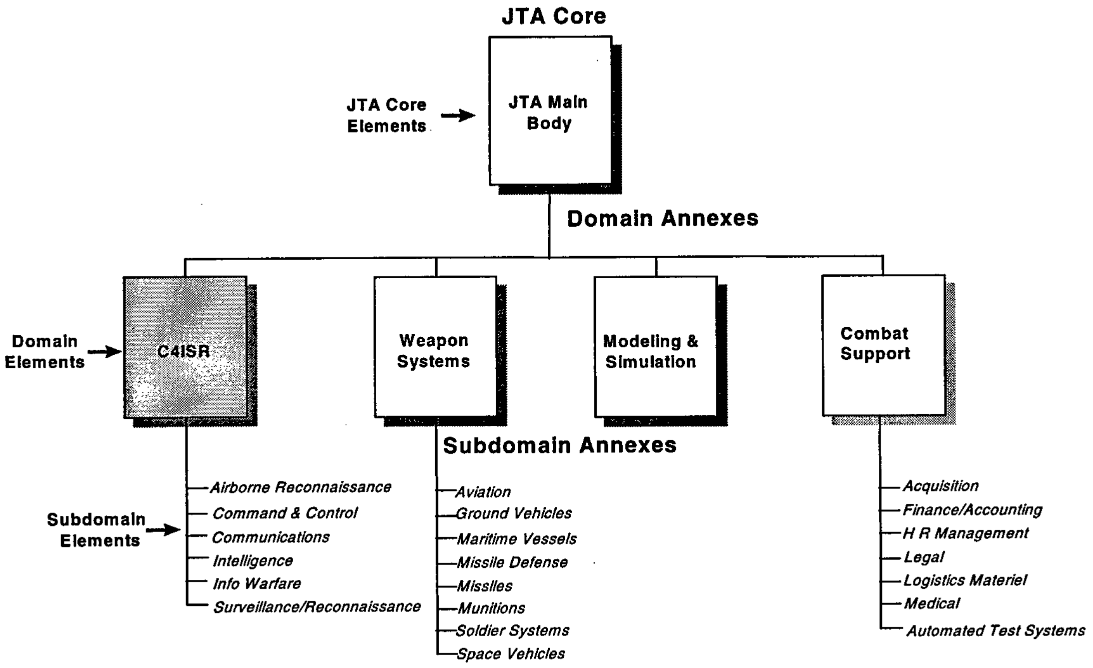


Figure C4ISR-1 Notional JTA Hierarchy

C4ISR.1.4 SCOPE AND APPLICABILITY

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

C4ISR.1.5 TECHNICAL REFERENCE MODEL

This domain uses the DoD Technical Reference Model cited in section 2.1.3. of the JTA as its framework. C4ISR Application Platform Entity service areas are addressed in Section C4ISR.2 as Additions to the JTA Core. Additional Application Software Entity service areas required to support C4ISR domain systems will be addressed in Section C4ISR.3, Domain Specific Service Areas.

C4ISR.1.6 ANNEX ORGANIZATION

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

C4ISR.2 ADDITIONS TO THE JTA CORE

C4ISR.2.1 INTRODUCTION

The C4ISR Domain Annex contains no additions to the elements mandated in the main body of the JTA unless otherwise cited in a specific C4ISR subdomain. The Airborne Reconnaissance (AR) Subdomain Annex does list additions to the C4ISR elements.

C4ISR.2.2 INFORMATION PROCESSING STANDARDS

C4ISR.2.2.1 Mandate Additions

There are currently no additions applicable to C4ISR with respect to Information Processing Standards as specified in Section 2.2 of the JTA. The Airborne Reconnaissance (AR) Subdomain Annex does list additions to the C4ISR elements.

C4ISR.2.2.2 Emerging Standards

There are currently no emerging standards identified in this section of the C4ISR domain.

C4ISR.2.3 INFORMATION TRANSFER STANDARDS

C4ISR.2.3.1 Mandate Additions

There are no additions applicable to C4ISR with respect to Information Transfer Standards as specified in Section 2.3 of the JTA. The Airborne Reconnaissance (AR) Subdomain Annex does list additions to the C4ISR elements.

C4ISR.2.4 INFORMATION MODELING, METADATA, AND INFORMATION EXCHANGE STANDARDS

C4ISR.2.4.1 Mandate Additions

There are no additions applicable to C4ISR with respect to Information Modeling, Metadata, and Information Exchange Standards as specified in Section 2.4 of the JTA.

C4ISR.2.5 HUMAN-COMPUTER INTERFACE STANDARDS

C4ISR.2.5.1 Mandate Additions

There are no additions applicable to C4ISR with respect to Human-Computer Interface Standards as specified in Section 2.5 of the JTA.

C4ISR.2.6 INFORMATION SYSTEMS SECURITY STANDARDS

C4ISR.2.6.1 Mandate Additions

There are no additions applicable to C4ISR with respect to Information Systems Security Standards as specified in Section 2.6 of the JTA.

C4ISR.3 DOMAIN SPECIFIC SERVICE AREAS

There are no C4ISR domain specific service areas identified. The Airborne Reconnaissance (AR) Subdomain Annex does list additional service areas.

AIRBORNE RECONNAISSANCE SUBDOMAIN ANNEX FOR THE C4ISR DOMAIN

C4ISR.AR.1 AR SUBDOMAIN ANNEX OVERVIEW

C4ISR.AR.1.1 PURPOSE

The Airborne Reconnaissance (AR) Subdomain Annex supports four mutually supporting objectives that provide the framework for meeting warfighter requirements. First, the AR Subdomain Annex provides the foundation for seamless flow of information and for interoperability among all airborne reconnaissance systems and associated ground/surface systems that produce, use, or exchange electronic information. Second, it establishes the minimum set of standards and technical guidelines for development and acquisition of new, upgraded, and demonstration systems to achieve interoperability; with reductions in costs and fielding times that would be unachievable without a technical architecture. Third, it ensures interoperability within the Defense Airborne Reconnaissance Programs (DARP) and enables development of new or alternative connectivities and operational plans for specific mission scenarios for AR systems. Finally, through coordination with other sections of the JTA, the AR Subdomain Annex takes the first step in ensuring interoperability between DARP and other DoD systems. Specifically, it provides the framework for attaining interoperability with space-based and other intelligence, surveillance, and reconnaissance systems.

C4ISR.AR.1.2 BACKGROUND

This AR Subdomain Annex to the Joint Technical Architecture (JTA) has been developed to provide standards to the DARP. These standards are mandated in order to aid in the development of new AR systems (or major upgrades of legacy systems). In addition, the standards are designed to facilitate the exchange and exploitation of AR data across the Department of Defense (DoD), and, in Operations Other Than War (OOTW), to users outside of the DoD. These standards have been determined to be unique to the DARP acquisition, communications, data processing, and user workstation systems. Standards that are not unique to the DARP have been transferred into the C4ISR Domain Annex or the core of the JTA.

The Airborne Reconnaissance Information Technical Architecture (ARITA) was the first attempt to consolidate all known airborne reconnaissance technical standards into a single document. The Airborne Reconnaissance Technical Architecture Working Group (ARTAWG) had representatives from the sensor, platform, communications, ground stations, and collection management/mission domains planning to consolidate AR standards. Based on the ARTAWG work, the Defense Airborne Reconnaissance Office (DARO) published the ARITA in September 1996. The DARO promoted the ARITA as a stand-alone reference that incorporated much of the work from the JTA, the Technical Architecture Framework for Information Management (TAFIM), and others that applied to airborne reconnaissance. In addition the ARITA contained many standards that were unique to AR. During this time, the proliferation of numerous architectures was addressed by both the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) and the Office of the Secretary of Defense for Acquisition and Technology (OSD(A&T)). The ARITA was recognized as unique because it addressed both Command, Control, Communications, Computers, and Intelligence (C4I), and the acquisition aspects of airborne reconnaissance systems. Therefore, the ARITA was deemed as a "pathfinder" for the larger architecture consolidation efforts within the DoD. As such, the Director of DARO elected to migrate the ARITA to the JTA and discontinue publication of the ARITA as a stand-alone document.

This version of the AR Subdomain Annex recognizes only standards that are mandated for AR systems in addition to those found in corresponding sections of the C4ISR Domain Annex or the JTA core. DARO is in the process of examining all DARP standards. As a result of this effort, future versions of the AR Subdomain Annex will address standards for the DARP that are not yet mature (under the rule set of the JTA), but are expected to develop into AR Subdomain Annex mandated standards. These standards will be placed in emerging standards sections of this annex.

C4ISR.AR.1.3 SUBDOMAIN DESCRIPTION

The AR Subdomain Annex to the JTA mandates the minimum set of standards and guidelines for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems relating to manned and unmanned AR systems. The annex provides the technical foundation for migrating AR systems towards the objective architecture identified in the Integrated Airborne Reconnaissance Strategy and in the various program plan documents of the DARO. Published DARO documents can be found on the World Wide Web at:

http://www.acq.osd.mil/daro

This AR Subdomain Annex adds the standards and guidance required for the airborne reconnaissance domain and is meant to complement both the C4ISR Domain Annex and the Defense Information Infrastructure Common Operating Environment (DII COE) as shown in Figure C4ISR.AR-1. The JTA (including the AR Subdomain Annex) and the DII COE supply the high level guidance to the two standards handbooks governing AR systems: the Joint Airborne Signals Intelligence (SIGINT) Architecture (JASA) Standards Handbook, and the Common Imagery Ground/Surface System (CIGSS) Acquisition Standards Handbook. These standards handbooks provide the most specific guidance for implementing the airborne efforts of the Imagery Intelligence (IMINT) and SIGINT communities and their corresponding umbrella programs. Airborne Measurement and Signature Intelligence (MASINT) standards will eventually be documented in the Joint Airborne MASINT Architecture (JAMA). An umbrella program, the Distributed Common Ground Systems (DCGS), has been proposed to eliminate potential duplication of IMINT, SIGINT, and MASINT ground station development. DCGS was chartered to develop a single ground system for these three intelligence areas under a common reference model.

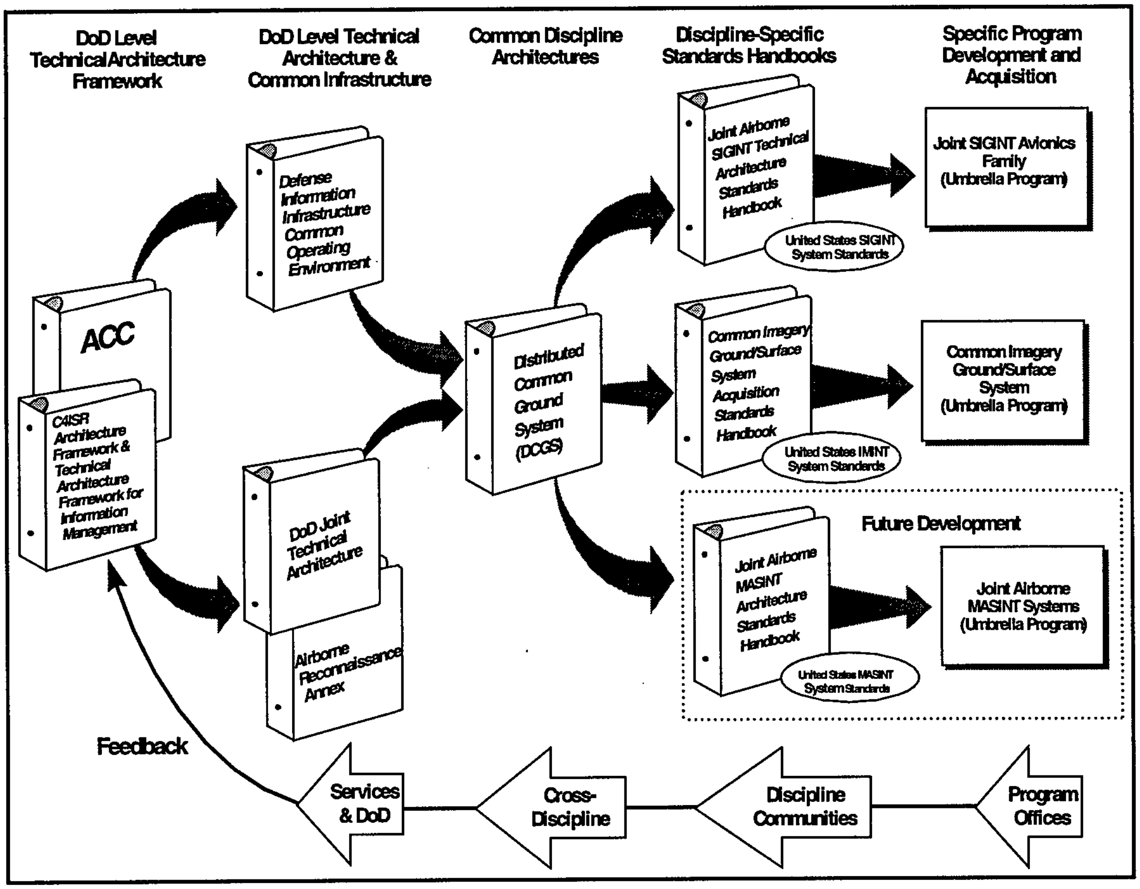

DoD Level Technical Architecture Framework
DoD Level Technical Architecture & Common Infrastructure
Common Discipline Architectures
Discipline-Specific Standards Handbooks
Specific Program Development and Acquisition
ACC
C4ISR Architecture Framework & Technical Architecture Framework for Information Management
Defense Information Infrastructure Common Operating Environment
DoD Joint Technical Architecture
Airborne Reconnaissance Annex
Distributed Common Ground System (DCGS)
Joint Airborne SIGINT Technical Architecture Standards Handbook
United States SIGINT System Standards
Common Imagery Ground/Surface System Acquisition Standards Handbook
United States IMINT System Standards
Future Development
Joint Airborne MASINT Architecture Standards Handbook
United States MASINT System Standards
Joint SIGINT Avionics Family (Umbrella Program)
Common Imagery Ground/Surface System (Umbrella Program)
Joint Airborne MASINT Systems (Umbrella Program)
Feedback
Services & DoD
Cross-Discipline
Discipline Communities
Program Offices

Figure C4ISR.AR-1 AR Annex Relationship to Other Standards Documents

The AR Subdomain Annex has been placed fully within the C4ISR Domain. It can be argued that elements of the AR Subdomain have better associations with the Weapon Systems or Combat Support domains. In the interest of readability and usability for the developer, it has been decided to place the entire annex in one domain (C4ISR) only.

The DoD JTA AR Subdomain Annex will be maintained by DARO through cooperation with the Architecture Coordination Council (ACC) and its associated steering groups and working groups. Questions or comments concerning technical details presented in this annex may be submitted to the ACC or directly to DARO.

C4ISR.AR.1.4 SCOPE AND APPLICABILITY

This part of the C4ISR Domain establishes the minimum set of rules governing information technology within airborne reconnaissance systems. The scope includes standards for information processing; information transfer; information modeling, metadata, and information standards; human-computer interface standards; information security; standards for the sensor-to-platform interface; and collection management, mission planning, and control.

The airborne reconnaissance domain constitutes *only a part* of the larger surveillance and reconnaissance part of C4ISR. As such, this annex does not cover technical architecture details for any part of the C4ISR spectrum other than the airborne reconnaissance portion. The annex has been derived from the ARITA, the most recent published DARO technical architecture document. This annex supersedes all draft and published versions of the ARITA. Future DARO technical architecture development and standards identification will merge within the greater C4ISR structure of the JTA. Because of the genesis of the AR

Subdomain Annex (from the ARITA), this version does not include many emerging standards. An ongoing effort by the DARO will identify emerging standards for future versions of the JTA.

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

Since airborne reconnaissance does cross domain boundaries, a certain degree of flexibility for citation of standards is necessary in order to meet the intent of the JTA. The AR Subdomain Annex references specific standards using the same rule set as the remainder of the JTA except for the following situation. In a few sections (e.g., Section C4ISR.AR.3.1.2.1.3.1 for Unattended MASINT Sensors), an Interface Control Document (ICD) has been mandated with a selected profile of Intelligence, Surveillance, and Reconnaissance (ISR) standards and tailored standards. This is necessary to meet the intent of the JTA to promote interoperability by acknowledging the dual C4ISR and Weapon Systems aspects of airborne reconnaissance. The JTA rules (Section 1) do allow "guidance" for interpretation of specific standards. The alternative, in this case, of specifying only a suite of standards instead of providing guidance through an ICD obscures the common ISR interfaces so vital to fully integrated, open systems. The selective application of ICDs, with corresponding standards profiles, will promote interoperability by combining standards with stable, open interfaces.

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

C4ISR.AR.1.5 TECHNICAL REFERENCE MODEL

As strictly defined by the *C4ISR Integrated Architecture Panel, C4ISR Architecture Framework*, "architectures" address multiple aspects crossing the boundaries of operational, technical, and system level architectures. The AR Subdomain Annex focuses on the technical architecture level and specifically identifies only those standards that have a direct bearing on airborne reconnaissance systems.

In order to achieve the desired focus, the AR Subdomain Annex uses a different reference model than the JTA technical reference model (TAFIM DoD TRM). This model variant is the AR Functional Reference Model (FRM). The complementary FRM and DoD TRM frameworks (or perspectives) are used to present and discuss the technology and information standards selected for virtually any C4ISR system. The DoD TRM, as derived from the TAFIM, is primarily a software-based model. It was originally developed for covering information technology within the DoD. Domain-specific standards, such as those required to cover all of airborne reconnaissance, do not fit fully within a software-based model. The FRM has therefore been adopted by DARO to encompass the airborne reconnaissance standards. It is used as a standards traceability matrix between the DARP architectures. The FRM depicts the generic, functional makeup of airborne reconnaissance systems, and shows how the various functions are interrelated. It is particularly well suited for showing which specific technology standards apply to each functional area.

C4ISR.AR.1.5.1 Background for the AR Functional Reference Model

The AR FRM provides a common framework for defining the scope and functional makeup of airborne reconnaissance systems. The FRM is critical for selecting standards and effectively depicting where they must be applied in the overall framework. Based on the functional model developed by the JASA working group and approved by the Defense Airborne Reconnaissance Steering Committee (DARSC), the FRM incorporates additional functions found in IMINT and MASINT systems, explicit mission planning and control functions, and expanded communications functions for integrating airborne reconnaissance with warfighter and other C4I systems (e.g., command and control systems, air tasking, and collection management). The AR FRM is shown in Figure C4ISR.AR-2.

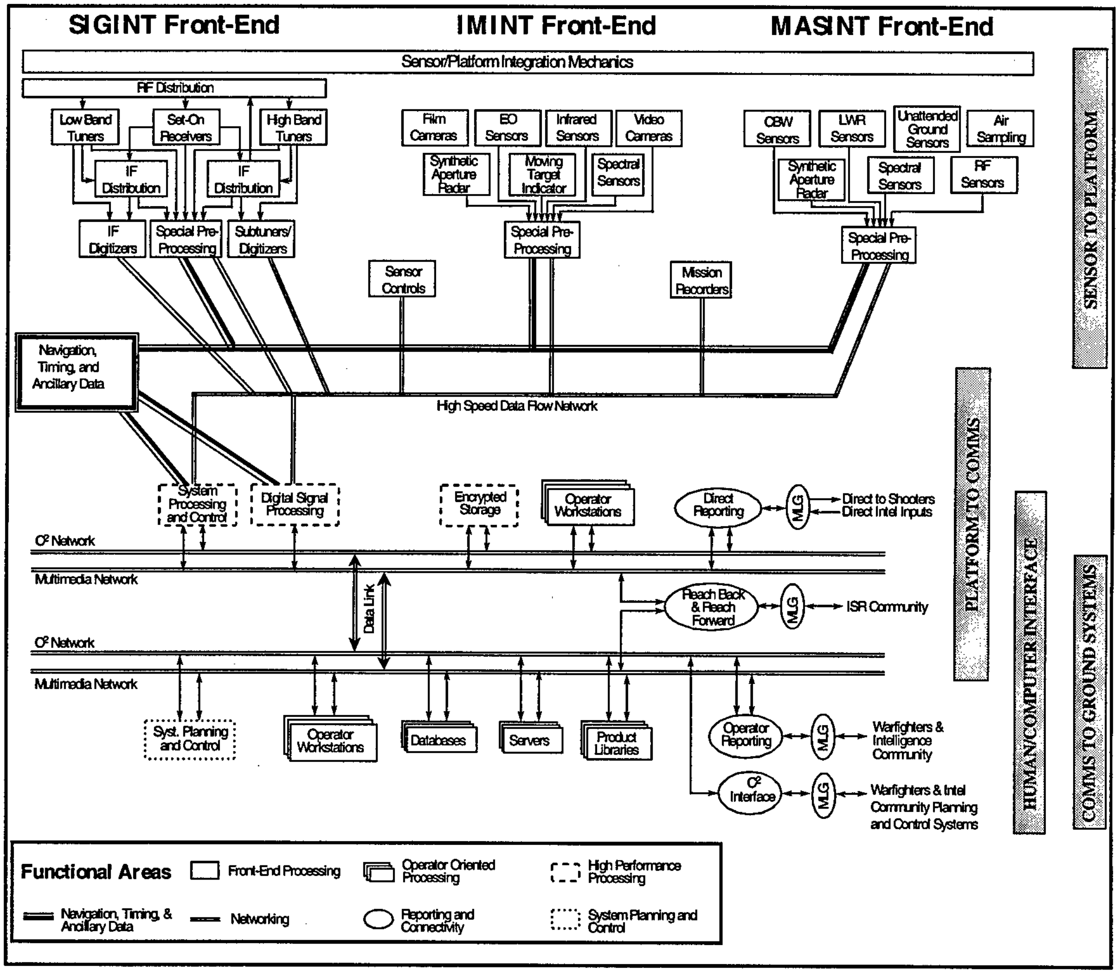


Figure C4ISR.AR-2 Airborne Reconnaissance Functional Reference Model

C4ISR.AR.1.5.2 AR FRM Traceability

In addition to this technical architecture, the DARO uses both operational and systems architectures to define and lead airborne reconnaissance systems. Both the operational and systems architectures will examine airborne reconnaissance using a functional flow approach. In each of these evolving architectures, there must be traceability back to standards as defined in this AR Subdomain Annex FRM. Where the operational functional flow or the system functional flow cannot be traced back to a set of standards (i.e., a "block" as shown in the FRM illustration), the FRM will require updating. Similarly, where the FRM blocks cannot be traced to both an operational component and a system component, the operational or system architecture model will require updating. Thus, the FRM model, as used in the airborne reconnaissance technical architecture described in this annex, will provide a cross-comparison capability with other DARO architecture models. Future versions of this annex will modify the FRM to more of a generic AR interface model, and will align the FRM more with the DARO Vision Architecture.

C4ISR.AR.1.5.3 AR FRM Defined

The AR FRM is a generic model intended to show only functional flow; it does not depict actual implementations of airborne reconnaissance systems. The generic model is intended to encompass all aspects of an airborne reconnaissance architecture that will meet the needs of manned aircraft and Unmanned Aerial Vehicles (UAVs) as well as their sensors and associated ground/surface systems. The AR FRM shown in Figure C4ISR.AR-2 breaks out the overall functional components into the seven distinct areas identified in Table C4ISR.AR-1.

Table C4ISR.AR-1 AR FRM Functional Components

Front-end processing functions
Navigation, timing, and ancillary data
Networking functions
High performance processing functions
Operator-oriented processing functions
Reporting and connectivity functions
System planning and control functions

The seven functional areas provide a convenient representation of the flow of information through airborne reconnaissance systems. At the top level, the three primary sources of AR data are shown (signal, imagery, and measurement & signature intelligence). Data from each of these types of front-end processors flow down through the system until the data can eventually be exploited at an analyst workstation. Each step of this flow-down process represents an interface where standards are required to ensure interoperability. In Figure C4ISR.AR-2, these interfaces are depicted wherever two of the separate functional areas connect. While useful for driving the interface requirements, dividing the mandated standards across the seven functional areas shown in Table C4ISR.AR-1 can cause confusion from an implementation viewpoint. For documentation and implementation, it is easier to list the resulting requirements by looking at the standards across a broader interface definition. The AR Subdomain Annex groups the seven functional areas logically into the four categories of Sensor-to-Platform Standards, Platform-to-Communications Standards, Communications-to-Ground Systems Standards, and Human-Computer Interface Standards. These four major groupings are shown in the gray rectangles placed vertically in Figure C4ISR.AR-2. This version of the AR Subdomain Annex identifies standards for three of these categories: Human-Computer Interface (Section 2.5 of this Subdomain Annex), Sensor-to-Platform (Section 3.1 of this Subdomain Annex) and Communications-to-Ground Systems. All of the identified Communication-to-Ground system standards fall within Collection Management, Mission Planning, and Control service areas (Section 3.2 of this Subdomain Annex). Future versions of this Subdomain Annex will add service areas for the Platform-to-Communications category.

C4ISR.AR.1.6 ANNEX ORGANIZATION

The organization of this annex is intended to mirror the organization of the C4ISR Domain Annex to the greatest extent possible. Each section of the annex, except for Part 1 (Overview), is divided into three subsections as follows. The first subsection, Introduction, is for information only. It defines the purpose and scope of the subsection and provides background descriptions and definitions that are unique to the section. The second subsection contains a minimum set of mandated standards for the identified service area. The subsection also identifies mandatory standards profiles and practices that are applicable to the AR subdomain. Each mandated standard or practice is identified as a bulleted item on a separate line and includes a formal reference citation that can be included within Requests for Proposals (RFP) or Statements of Work (SOW). The third subsection, Emerging Standards, provides an abbreviated description of candidates that are expected to move into the mandated subsection within a short period. As defined within the core of the JTA, this transition should occur within three years of publication of the standard in the emerging subsection.

The AR Subdomain Annex contains three parts. Part 1 is the Overview. Part 2 contains the standards for the DARP corresponding to the JTA core (and C4ISR Domain) service areas that contain AR available standards mandates as described above. Part 2 also contains emerging standards for the AR Subdomain Annex. Part 3 contains the Standards for the DARP for service areas that are not included in the JTA core or C4ISR Domain Annex. The acronym list for the AR Subdomain Annex has been incorporated into the larger JTA list (Appendix A). Similarly, a summary of AR mandated standards for each service area has been incorporated into Appendix B of the JTA. Table C4ISR.AR-2 identifies the service areas for this Subdomain Annex. This table also indicates whether the AR Subdomain Annex service area has a corresponding service area in the C4ISR Domain Annex of the JTA or whether the service area is unique to the DARP. Table C4ISR.AR-2 also identifies whether this version of the AR Subdomain Annex includes any service-unique items for the DARP or whether the paragraph is merely a placeholder for this version of the document.

Table C4ISR.AR-2 AR Annex Sections

C4ISR Section	Service Area	Corresponding JTA Service Area	DARP-Unique Service Area	Annex Mandates Identified
2.2	Information Processing	*		*
2.3	Information Transfer	*		*
2.4	Information Modeling, Metadata, and Information Exchange	*		
2.5	Human-Computer Interfaces	*		*
2.6	Information Systems Security	*		
3.1	Sensor Platform Interface		*	*
3.2	Collection Management, Mission Planning and Control		*	*

C4ISR.AR.2 ADDITIONS TO C4ISR DOMAIN SERVICE AREAS

C4ISR.AR.2.1 INTRODUCTION

This Airborne Reconnaissance Subdomain Annex, in conjunction with the JTA core and the C4ISR Annex, provides the technical foundation for migrating airborne reconnaissance systems towards the objective architecture identified in the various program plan documents of the Defense Airborne Reconnaissance Office. DARO's high-level vision of the migration plans and major thrusts to achieve the capabilities, connectivities, and interoperability required of airborne reconnaissance systems has now moved forward by merging ISR systems within the C4I structure described in the C4ISR Domain Annex of the JTA. This merger is made with the full knowledge that ISR systems are not, as of today, a simple extension of the JTA but rather, a broad expansion of the concept of C4I interoperability. The migration from today's stove-piped systems to achieving the concepts promulgated by *C4I For The Warrior*, other DoD technical architectures, and Service/Agency operational architectures requires DARO and the ISR community to take this step. This part of the AR Subdomain Annex establishes the minimum set of rules governing information technology within airborne reconnaissance systems. The scope includes standards for information processing; information transfer; information modeling, metadata, and information exchange standards; human-computer interface standards; and information security standards. This part of the AR

Subdomain Annex does not contain rules for the physical, mechanical, or electrical components of systems, even when these are related to information technology.

C4ISR.AR.2.2 INFORMATION PROCESSING STANDARDS

C4ISR.AR.2.2.1 Introduction

This annex expands the concept of *information* within a C4I system to include the information processing of ISR sensor systems. Much of this processing is embedded within the sensor systems themselves and the avionics on-board reconnaissance assets. It is important to note that ISR systems encompass both real-time and non-real-time architectures. The sensor, platform, telemetry, and data link systems within ISR are all real-time, 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. The DoD TRM, adopted for use by the JTA, does not accommodate real-time and embedded systems. On the other hand, once raw data is delivered to the ground, non-real-time processing and dissemination systems follow the current JTA/TRM model.

It is not the intent of the AR Subdomain Annex to force DII COE compliance on those AR systems where the DII COE cannot presently provide a reasonable solution (e.g., real-time systems or multi-level security systems). These situations must be evaluated on a case-by-case basis. The JTA waiver process is designed to allow flexibility in implementation details when there are overriding technical or economic concerns. This annex does endorse compliance with the DII COE I&RTS (as defined in the JTA core) in the absence of a submitted waiver.

As intelligence time lines continue to shrink to weapon systems (shooter) time lines, speed will become even more critical for operational systems. Much of this architecture is based on real-time processing and does not follow the Technical Reference Model described in the JTA. Real time systems may be closer to the Society of Automotive Engineers (SAE) Generic Open Architecture (GOA). The DII COE is also working towards a DoD-wide real-time architecture model. Ongoing work by the TRM Working Group will resolve this disconnect in a manner that, if possible, accommodates both weapon systems and C4I systems.

User requirements for specific ISR missions define information processing within the three intelligence disciplines (IMINT, SIGINT and MASINT) as defined below. These standards encompass all software in associated ground/surface systems as well as software embedded in airborne reconnaissance systems.

C4ISR.AR.2.2.2 AR Information Processing Mandates

C4ISR.AR.2.2.2.1 Image Processing

This AR Subdomain Annex defines image processing as the conversion of raw data into a product that can be exploited. Imagery is defined as any Electro Optical (EO), Infrared (IR), or Synthetic Aperture Radar (SAR) data stream collected by an imaging sensor that can be visualized on an exploitation terminal. The sequence of steps needed to extract information and prepare an exploitation product depends upon the required external environment interface (EEI), the shapes of the objects in the scene, illumination and shadows, and military and physical contexts.

C4ISR.AR.2.2.2.1.1 Imagery Archives

The primary function for product libraries is to maintain a complete set of all reconnaissance products produced (in a given system) and make them available to all potential users on a query or browse basis. Although the products may include conventional formatted message reports, product libraries are most useful for disseminating newer "specialized" products such as video and audio clips, imagery, graphics, multi-media, and hypertext products like those available on the Internet. Dissemination of these products and access to the product libraries will be through the Internet protocol router networks such as NIPRNET, SIPRNET, and JWICS. Although there are no mandated standards for this area, compatibility with the NIMA Library Program (NLP) [formerly Image Product Archive (IPA) and Image Product Library (IPL)] is required. The NLP is described in the US Imagery and Geospatial Information System (USIGS) Architecture.

C4ISR.AR.2.2.2.1.2 Common Imagery Ground/Surface System (CIGSS)

The Common Imagery Ground/Surface System (CIGSS) concept, which is now a segment of the DCGS described in Part 1, has been approved by the Joint Requirements Oversight Council (JROC) and is fully supported by the DoD Services. It is not a system in the traditional sense; instead, CIGSS is an umbrella program that defines interoperability, performance, and commonality requirements and standards for DoD ground/surface based imagery processing and exploitation systems. It consolidates the systems listed in Table C4ISR.AR-3 into a single DARP project.

Table C4ISR.AR-3 CIGSS Component Programs

Joint Service Image Processing System (JSIPS) program – including Navy, Air Force, and Marine Corps
Army's Enhanced Tactical Radar Correlator (ETRAC)
Army's Modernized Imagery Exploitation System (MIES)
Imagery parts of the Air Force's Contingency Airborne Reconnaissance System (CARS)
Marine Corps' Tactical Exploitation Group (TEG) programs
Korean Combined Operational Intelligence Center (KCOIC) imagery systems
Pacific Air Forces Interim National Exploitation System (PINES)
Mobile Intelligence Processing Element (MIPE)
Integrated Deployable Processing System (IPDS)
Processing/exploitation capability for the U-2R SENIOR YEAR Electro-Optical (E/O) sensor (SENIOR BLADE)

CIGSS-compliant (mandated) systems are designed to receive, process, exploit and disseminate imagery products derived from satellites, commercial or foreign satellite sensors, UAV, U-2 reconnaissance aircraft and tactical aircraft such as the F/A-18. CIGSS will be afforded increased flexibility and capability in satisfying multiple time-sensitive user needs. Once compliant with common community processing, storage, retrieval, and dissemination standards, CIGSS modularity will enable the theater, JTF and components to employ interactive CIGSS elements for small regional contingencies and major regional conflicts from a variety of sources to meet the anticipated intelligence demand. This annex mandates the standards identified in the most current approved handbook for airborne IMINT:

- Common Imagery Ground/Surface System (CIGSS) Acquisition Standards Handbook, Version 1, 19 July 1995.

C4ISR.AR.2.2.2.2 SIGINT Information Processing

The Joint Airborne SIGINT Architecture (JASA) is the DoD's plan for meeting the warfighter's 2010 and beyond airborne SIGINT requirements. The fundamental philosophy behind JASA is to leverage commercial digital signal processor technology to address the ever growing population of varied radio frequency (RF) signals, modulation schemes and signal multiplexing structures. By digitizing the signal early in the sensor system, common hardware processing can be used that is independent of signal type, reducing the need for signal specific specialized hardware. This approach to signal processing increases the flexibility and overall capacity of the SIGINT system, which must rapidly respond to the explosion of digital signals in the environment.

Version 2.0 of the *JASA Standards Handbook*, developed by the JASA Standards Working Group, was published in October 1997. This AR Subdomain Annex mandates the standards identified in the handbook for airborne SIGINT systems:

- Joint Airborne SIGINT Architecture Standards Handbook, Version 2.0, 30 October 1997.

C4ISR.AR.2.2.2.3 MASINT Information Processing

The Central MASINT Office (CMO) is currently developing a MASINT architecture under the umbrella of the US MASINT System (USMS) program. The airborne portion of the USMS is called the Joint Airborne MASINT Architecture (JAMA). As a part of JAMA, a MASINT Standards Handbook will be developed. Upon publication, it will be evaluated for incorporation into this AR Subdomain Annex. There are presently no MASINT-specific information processing mandates identified.

C4ISR.AR.2.2.2.4 Data Management

Airborne Reconnaissance data management supports the definition, storage, retrieval, and distribution of data elements (e.g., imagery and support data) derived from data collected by airborne sensors and shared by multiple applications/systems.

C4ISR.AR.2.2.2.4.1 Target/Threat Data Management

The National Target/Threat Signature Data System (NTSDS) has been designated as a migration system, in accordance with guidance from ASD(C3I) and by the Intelligence Systems Board (ISB). NTSDS provides the DoD signature data community (ISR, MASINT, & Armament) 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. There are no AR Annex mandates for target/threat data management. However, compatibility with the National Target/Threat Signature Database System is required.

C4ISR.AR.2.2.2.4.2 Data Management Services

These services support the definition, storage, and retrieval of data elements from monolithic and distributed relational Database Management Systems (DBMSs). These services also support platform-independent file management (e.g., the creation, access, and destruction of files and directories). This annex follows the JTA core that mandates conformance to entry level ANSI Structured Query Language (SQL) standards and adds Ada interfaces. There are presently no additional AR Annex Data Management Service standards beyond those listed elsewhere in the JTA.

C4ISR.AR.2.2.3 Emerging Standards

This version of the AR Annex does not identify any emerging standards for information processing. An ongoing effort by the DARO will identify emerging standards for future versions of the JTA.

C4ISR.AR.2.3 INFORMATION TRANSFER STANDARDS

C4ISR.AR.2.3.1 Introduction

Near-real-time dissemination of Joint Service tactical intelligence information hinges on information transfer standards. To ensure continued battlespace awareness and to satisfy the requirement for secure, high-speed, multi-media transmission services, an integration of several intelligence broadcasts into one standard system is probable.

Information transfer standards and profiles described in this section cover dissemination and data link mandates for ISR systems. This section identifies systems and the interface standards that are required for interoperability between and among ISR systems and are in addition to the systems described in the JTA core and the C4ISR Domain Annex. This section does not cover standards for platform internal information transfer. These standards will be covered in the Sensor-to-Platform service areas of this Subdomain Annex.

C4ISR.AR.2.3.2 AR Information Transfer Mandates

C4ISR.AR.2.3.2.1 Dissemination Systems

This section focuses on standards supporting near-real-time battlefield dissemination of intelligence and surveillance products from both airborne platforms and ground surface systems. Broadcasts give tactical users a "picture of the battlefield." Depending on the system, displays or messages can include data derived from SIGINT, IMINT, or MASINT systems as well as support for targeting, situation awareness, battle management, survivability, and mission planning. Together these standards reflect the diverse needs addressed by Joint users. There are no additional dissemination system standards mandated in this annex. However, compatibility with the systems identified in Table C4ISR.AR-4 are required.

Table C4ISR.AR-4 Airborne Reconnaissance Dissemination Systems

Joint/Global Broadcast Service (JBS/GBS)
Tactical Information Broadcast Service (TIBS)
Tactical Receive Equipment and Related Applications (TRAP) Data Dissemination System (TDDS)
Tactical Reconnaissance Intelligence Exchange System (TRIXS)

C4ISR.AR.2.3.2.2 Data Link Standards

The Common Data Link (CDL) is a flexible, multi-purpose radiolink based digital communication system that was developed by the Government for use in imagery and signals intelligence collection systems. It provides standard waveforms that follow a line-of-sight microwave path (link) and allows both full-duplex and simplex communications between airborne/spaceborne platforms and surface based terminals. The link consists of an uplink that operates at 200 Kbits/s and a downlink that operates at 10.71 Mbits/s, 137 Mbits/s and 274 Mbits/s. All links use the C, X and K frequency bands. The uplink is secure and jam resistant. Currently, the downlink is secure only for the 10.71 Mbits/s rate. New platforms are coming online that will require a secure downlink for the 137/274 Mbits/s rates. The CDL system supports air-to-land/sea surface, and air-to-satellite (relay/beyond line-of-sight) communications modes.

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

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

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

C4ISR.AR.2.3.3 Emerging Standards

The airborne reconnaissance dissemination systems listed in Table C4ISR.AR-4 are to be replaced by the Integrated Broadcast Service (IBS) over the next five years. The IBS IOC is expected in 2002.

C4ISR.AR.2.4 INFORMATION MODELING, METADATA, AND INFORMATION EXCHANGE STANDARDS

C4ISR.AR.2.4.1 Introduction

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

C4ISR.AR.2.4.2 AR Information Modeling and Information Mandates

This version of the AR Subdomain Annex does not specify any additional standards for information modeling and information.

C4ISR.AR.2.4.3 Emerging Standards

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

C4ISR.AR.2.5 HUMAN-COMPUTER INTERFACE STANDARDS

C4ISR.AR.2.5.1 Introduction

This subsection identifies the mandatory standards, profiles, and practices for human-computer interfaces. The human-computer interface is an extremely important AR function. It is an area that is evolving quickly due in large part to rapid advances in commercial video technologies. These commercial interfaces have been released to the public only to be replaced in a very short time by the next generation of products. This rapid pace has produced few standards. However, the speed of technology advance is expected to produce several breakthroughs for information/understanding transfer to reconnaissance operations.

C4ISR.AR.2.5.2 AR Human-Computer Interface Mandates

Currently, the ISR community has no additional standards, beyond those in the core of the JTA, for imagery display systems.

C4ISR.AR.2.5.3 Emerging Standards

The Tactical Control System (TCS) is being designed and developed to provide a common set of Human-Computer Interfaces for interoperability with the family of Tactical UAVs. TCS HCI design requirements are contained within the TCS Block 0 Software Requirements Specification, (TCS Document Control Number: TCS-103), and the TCS Human-Computer Interface Requirements Specification, (TCS Document Control Number: TCS-108). These documents will be adopted as formal emerging standards following their official release.

C4ISR.AR.2.6 INFORMATION SYSTEMS SECURITY STANDARDS

C4ISR.AR.2.6.1 Introduction

Information systems security standards protect information and the processing platform resources. They must often be combined with security procedures, which are beyond the scope of the information technology service areas, to fully meet operational security requirements. Security services include security policy, accountability, assurance, user authentication, access control, data integrity and confidentiality, non-repudiation, and system availability control. The mandated and emerging standards identified in Section 2.6 of the JTA apply to the AR subdomain. ISR reporting includes dissemination of formatted message traffic, imagery, imagery products, database transaction updates, and graphical situation display data. In general, these products are widely disseminated through the DoD communications infrastructure.

C4ISR.AR.2.6.2 AR Information Security Mandates

Intelligence information can be disseminated from Unclassified to TS/SCI. For the AR Subdomain, there are presently no additions to the information security mandates listed in the JTA core.

C4ISR.AR.2.6.3 Emerging Standards

This version of the AR Subdomain Annex does not identify any emerging standards for information security. An ongoing effort by the DARO will identify emerging standards for future versions of the JTA.

C4ISR.AR.3 SUBDOMAIN SPECIFIC SERVICE AREAS

C4ISR.AR.3.1 SENSOR-TO-PLATFORM INTERFACE

C4ISR.AR.3.1.1 Introduction

This section identifies the minimum standards for airborne sensors and the interface to the airborne sensor platforms. These interfaces allow sensor data, both raw and pre-processed, to transfer through airborne communications/telemetry systems and to mission recording equipment. Conversely, aircraft data such as navigation, timing, or telemetry inputs to control on-board sensors (e.g., optics, SAR spot coverage) must pass through this interface as well. Eventually, the interfaces will become more platform independent and sensor system independent as these standards evolve towards open systems.

Airborne reconnaissance sensors are the source of all ISR information. Their output, combined with on-board flight information such as position and altitude, produces a raw data set that is normally not considered useful information until it is processed and disseminated to the warfighter consumer. Much of this processing is done on board within real-time systems and these must interface seamlessly within the host aircraft. This section lists standards that apply to that interface.

This section addresses the critical components of the interface between the sensor system and the host aircraft. This interface includes: sensor to external environment; sensor control; data recording; aircraft power; navigation/flight data information to the sensor system; timing; internal communications; avionics busses and back planes; telemetry; and sensor preprocessing. Sensor systems have been divided into imagery, signals, and MASINT.

C4ISR.AR.3.1.2 AR Sensor-to-Platform Mandates

C4ISR.AR.3.1.2.1 Sensor Mandates

All airborne reconnaissance systems begin with a platform-integrated SIGINT, IMINT, or MASINT sensor. The specific functions of the front-end sensors are completely different and are discussed separately within the following subsections.

C4ISR.AR.3.1.2.1.1 IMINT

IMINT front-end functions are divided into ten major areas: seven image acquisition sensors, sensor control functions, special pre-processing functions, and mission recorders. The following subsections describe IMINT sensors and the specific standards that apply.

C4ISR.AR.3.1.2.1.1.1 Video Cameras

Legacy AR video systems currently use analog components. For analog systems, the base video standard is the National Television Standards Committee (NTSC) signal provided in RS-170 format. Commercial industry is currently migrating away from analog video components to all-digital systems. Airborne reconnaissance systems will leverage advances in commercial television technology that provide the standards for interoperability for commercial broadcast and military video systems. AR systems should provide a clear migration path toward an all-digital system, conforming to the mandated standards of the JTA core. There are no additional video camera standards mandated for the AR community.

C4ISR.AR.3.1.2.1.1.2 Image Quality Standards

Image quality is the single most critical factor determining the utility of the image for data exploitation. Image quality is dependent upon physical features of the collection system (e.g., focal length, lens quality, number and spread of multispectral sensors, and density of the sensor array), the geometric relationships at the time of imaging (e.g., distance and angle between the sensor and the target), target and transmission media features (e.g., acquisition angle and degree of illumination, image degradation from cloud cover and smoke), and errors introduced in the processing stream (e.g., data dropouts and “noisy” communication paths). The user communities for panchromatic, multispectral and radar imagery have developed a series of scales to rate the quality of the received imagery. These scales condense the many factors influencing the image into a single rating that defines the overall usability of the image. Common rating scales include the National Imagery Interpretability Rating Scale (NIIRS) for optical imagery, National Radar Imagery Interpretation Standard (NRIIS) for Synthetic Aperture Radar, and Multispectral Imagery Interpretability Rating Scale (MSIIRS) for spectral imagery.

For video imagery systems, the Department of Defense/Intelligence Community/United States Imagery and Geospatial System (DoD/IC/USIGS) Video Working Group Video Imagery Standards Profile (VISP), Version 1.21, 7 January 1998, defines a "Video Systems (Spatial and Temporal) Matrix" (VSM). This Recommended Practice gives user communities an easy to use, common shorthand reference language to describe the fundamental technical capabilities of DoD/IC video imagery systems. The "Video Systems Matrix" includes tables of Technical Specifications and related Notes.

There are no AR community mandated standards for image quality beyond those referenced in the JTA core.

C4ISR.AR.3.1.2.1.1.3 Synthetic Aperture Radar

Synthetic Aperture Radar (SAR) is the most commonly used type of radar for imagery reconnaissance applications. The systems are called synthetic aperture because the combination of the individual radar returns effectively creates one large antenna with an effective aperture size equivalent to the flight path-length traversed during the signal integration. The formation of this large synthetic aperture is what enables these radars to produce images with fine in-track (for azimuthal) resolution. The high bandwidth and pulse repetition interval enables the SAR’s fine cross track (or range) resolution. The image can be produced with ground resolutions less than one foot, when operating in “spot” mode, and approach photographic appearance and interpretability. In search modes, ground sample distance (more correctly radar impulse response) is often ten feet or more. It is common practice to smooth the navigation and timing data for SAR using Kalman filtering techniques. The following standard practice is therefore mandated for the AR community:

- Kalman filtering for navigation and timing, as originally defined in Kalman, R.E., A new approach to linear filtering and prediction problems, Trans. ASME, Series D, J. Basic Eng., V. 82, March 1960.

C4ISR.AR.3.1.2.1.2 SIGINT

SIGINT front-end standards are concerned primarily with on-board systems that receive and process radio frequency (RF) from low frequency (LF), 30 KHz to 300 KHz, through extra high frequency (EHF), 30 GHz to 300 GHz, received by the platform antenna/antenna arrays. These RF antenna/antenna array types may be omni-directional, directional, beam-steered, steered dish, interferometric, or spinning dish. In addition, the SIGINT front-end functional elements include the RF distribution, low and high band tuners, set-on receivers, IF distribution IF digitizers, and sub-band tuners/digitizers, and channelizers. SIGINT sensor/platform interface standards are identified in the following reference:

- Joint Airborne SIGINT Architecture Standards Handbook, Version 2.0, 30 October 1997.

C4ISR.AR.3.1.2.1.3 MASINT

Two important distinctions between MASINT and other intelligence systems are the maturity and diversity of the component systems. MASINT technologies are both immature and diverse. The MASINT discipline encompasses the seven technological areas of remote sensing identified in Table C4ISR.AR-5. Within each of the seven areas there are numerous implementations, many of which are still in the research and development phase, which makes the creation of standards a much more difficult task. Where possible, standards for MASINT systems will be specified in this document. This version of the AR annex only identifies a single standard for unattended MASINT sensors.

Table C4ISR.AR-5 MASINT Technology Areas

Chemical and Biological Weapons (CBW)
LASINT/Laser Warning Receivers (LWR)
Unattended Ground Sensors (UGS)
Spectral (Non-literal)
Air Sampling
Radio Frequency (RF)
Synthetic Aperture Radar Phase History (SAR PH)

The Joint Airborne MASINT Architecture (JAMA) is a much needed effort to define the overall architecture for airborne MASINT systems and the corresponding standards. The JAMA, when initiated, will be fully integrated with JASA where RF MASINT and SIGINT systems overlap. Similarly, the SAR PH and spectral MASINT airborne areas will be fully coordinated with CIGSS to maximize intelligence assets.

C4ISR.AR.3.1.2.1.3.1 Unattended MASINT Sensors

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

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

C4ISR.AR.3.1.2.2 Airborne Platform Mandates

This AR Annex does not cover the technical architecture details for the airborne platform except for those details that directly affect the on-board reconnaissance sensors and the processing of the collected data stream. Power, timing, and navigation standards are critical for the operation of the sensors, the transmission of data, and the exploitation of the gathered information.

C4ISR.AR.3.1.2.2.1 Timing

Timing is critical for airborne sensor systems and directly affects the overall quality of the finished airborne reconnaissance product. All processing and exploitation functions use timing data in some way when processing the sensor data. The following timing standards are mandated for AR systems:

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

C4ISR.AR.3.1.2.2.2 Navigation, Geospatial

Navigation service provides information about the position and attitude (roll, pitch and yaw) of the collection platform. Navigation and geospatial data are parts of the metadata associated with sensor data, and are critical to sensor data exploitation. The following navigation and geospatial standards are mandated for AR systems:

- SNU-84-1, Revision D Specification for USAF Standard Form, Fit, and Function (F3) Medium Accuracy Inertial Navigation Unit (INS), 21 September 1992.
- ICD-GPS-200, Interface Control Document GPS (200), 1 July 1992.

C4ISR.AR.3.1.2.3 Airborne Platform-Internal Communications

Internal communications for on-board networks are used to apply real-time commands to control on-board sensors, distribution of raw/pre-processed digital sensor data between processing components, and metadata tagged to the sensor data. The numerous standards referenced below must be selected based on the platform. Their selection depends on whether the end platform is an unmanned aerial vehicle or manned vehicle. For example, most UAVs will not require a LAN capacity needed for a Rivet Joint or AWACS. Depending upon the application environment, one of more of the following mandated standards shall be selected for AR systems:

- MIL-STD-1553B, Notice 4, Department of Defense Interface Standard for Digital Time Division Command/Response Multiplex Data Bus, 15 January 1996.
- ANSI X3.184, Information Systems - Fiber Distributed Data Interface (FDDI) Single-Mode Fiber Physical Layer Medium Dependent (SMF-PMD) (100 Mb/s dual counter rotating ring), 1 January 1993.
- ANSI X3.230, Information Technology - Fiber Channel - Physical and Signaling Interface (FC-PH), (800 Mb/s), 1 January 1996.

C4ISR.AR.3.1.2.4 Air Vehicle/Sensor Telemetry Mandates

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

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

C4ISR.AR.3.1.2.5 Mission Recorder Mandates

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

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

To support digital recording activities, the following mission recorder standards are mandated for use in AR systems:

- Compatibility with the published "AMPEX Digital Instrumentation Recorder DCRSi 240 User Manual."
- ANSI X3.175, 19-mm Type ID-1 Recorded Instrumentation - Digital Cassette Tape Form, 1990, ID 1.

To support analog recording activities, the following mission recorder standard is mandated for use in AR systems:

- Instrumentation Group (IRIG) B format as defined in IRIG Document 104-70, August 1970.

C4ISR.AR.3.1.3 Emerging Standards

This version of the AR Annex does not identify any emerging standards for the sensor platform interface. An ongoing effort by the DARO will identify emerging standards for future versions of the JTA.

C4ISR.AR.3.2 COLLECTION MANAGEMENT, MISSION PLANNING, AND CONTROL

C4ISR.AR.3.2.1 Introduction

This annex defines standards for collection management, mission planning and mission control which are integral parts of airborne reconnaissance systems. Collection management is a process that is performed by a Collection Management Authority (CMA) which uses a specific collection management system. Mission planning is a process that may be performed within an airborne reconnaissance system or it may be performed externally. Mission control is a process that deals with execution of specific reconnaissance missions.

C4ISR.AR.3.2.2 AR Collection Management, Mission Planning, and Control Mandates

C4ISR.AR.3.2.2.1 Collection Management Mandates

Collection requirements are generated by warfighters and then allocated to the Collection Management Authority (CMA). The CMA uses the Joint Collection Management Tool (JCMT) to provide an overview of the requirements database. JCMT assists the CMA in determining the appropriate collection platform or mix of assets required to perform the mission. The CMA's collection management system provides the reconnaissance feedback to the warfighters who originated the requests for information. JCMT is the migration system designated by the DoD to be used for all-source management functions (i.e., legacy systems will be phased out as JCMT supersedes them). As such, it will combine IMINT, SIGINT, MASINT, and HUMINT tasking.

On 28 October 1994, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) approved the recommendations from the Intelligence Systems Board Migration Panel that: 1) JCMT become the DoD Intelligence Information Systems (DODIIS) migration system for all-source collection management, and 2) the Army's Collection Management Support Tools (CMST) become the initial baseline for JCMT. According to ASD (C3I) direction, migration systems are to replace all legacy systems in FY97. Besides CMST, the legacy systems which JCMT will replace include DIA's Collection Requirements Management Application (CRMA), USAF National Air Intelligence Center's (NAIC) Collection Requirements Management System (CRMS), Operational Support Office's (OSO) UNIX-based National Exercise Support Terminal (UNEST), and SOUTHCOM's Intelligence Support Processing Tool (ISPT).

For the AR domain, compatibility with the Joint Collection Management Tool (JCMT) is a requirement. In addition, the following standard for country codes is mandated for collection management functions:

- FIPS PUB 10-4: April 1995, Countries, Dependencies, Areas of Special Sovereignty, Municipal Divisions.

C4ISR.AR.3.2.2.2 Mission Planning Mandates

A multitude of mission planning systems exist today. Many of these are special applications that were designed for specific aircraft and operate on specific hardware suites. There are formal, programmatic efforts underway to consolidate these into several generic systems. Two of these were picked as representative systems for purposes of developing this annex: the U.S. Navy's Tactical Aviation Mission Planning System (TAMPS) and the USAF Air Force Mission Support System (AFMSS). Note that other specific mission planning systems have been consolidated into these two programs. TAMPS consists of a core and a number of mission planning modules for specific Navy, Marine Corps, and Coast Guard aircraft and weapons. AFMSS contains a core and a number of Avionics/Weapons/Electronics (AWE) modules for specific Air Force, Army, and US Special Operations Command aircraft and weapons. Long-term plans call for combining these into one DoD-wide mission planning system.

While both the TAMPS and AFMSS programs show plans to provide mission planning capabilities for reconnaissance platforms (such as the U-2, UAVs, RC-135, EP-3, F/A-18 and others), the plans are generally for platform and navigation planning only (e.g., flight path, threat avoidance, take-off and landing calculations, or fuel consumption). Mission planning modules for the reconnaissance sensor system payloads and communications system planning are currently not in the baseline.

The interfaces required for mission planning functions vary depending on specific system operational requirements and mission needs. For example, systems operated by the USAF will receive intelligence data from the unit-level Combat Information System (CIS), whereas the Army will generally rely on their All Source Analysis System (ASAS). Regardless of the source of the data, it will generally be received in airborne reconnaissance systems through the command and control interfaces or via bulk digital media such as magnetic tape and CD-ROM. There are no mandated mission planning standards for the AR domain. However, depending upon the service supported by the reconnaissance asset, compatibility with the Air Force Mission Support System (AFMSS), the Tactical Aviation Mission Planning System (TAMPS), the USAF Combat Intelligence System (CIS), the Joint Maritime Combat Intelligence System (JMCIS), or the USA All Source Analysis System (ASAS) is essential.

The Tactical Control System (TCS) Tactical UAV Route and Payload Planner (RPP) is being designed and developed to provide a common route and payload planner for the family of Tactical UAVs. Air vehicle route planning, modular mission payload planning, plan verification, plan uplink, plan monitoring, and plan display are provided by the TCS RPP. These two standards are mandated for tactical UAVs:

- TCS RPP design requirements are contained within the TCS RPP Software Requirements Specification Version 1.0, 14 November 1997 (TCS Document Control Number: TCS-303).
- The Tactical Control System (TCS) Flight Route Plan to Tactical Control System, Version 1.0 Interface Design Description (IDD), (TCS Document Control Number: TCS-244, 1 October 1997,

provides the standard Flight Route and Payload Plan file format to be used for compatibility with the TCS RPP and TCS Core Software.

C4ISR.AR.3.2.2.3 Mission Control Mandates

Mission control functions provide for real-time and near-real-time control of the platform, sensor suite, and communications subsystems during the execution of reconnaissance missions. These control functions are implemented in ground/surface subsystems and consist of three types: remote piloting functions and telemetry data, remote sensor control functions, and dynamic retasking functions.

Currently, there are no standards in this annex for manned aircraft. However, for remotely piloted UAVs, telemetry data are transmitted to the ground/surface system and piloting commands are transmitted to the vehicle via the data link in real-time. For UAVs, the Mission Planning and Control Station (MPCS) consists of the equipment necessary to perform mission planning, mission control, communications and data exploitation for one or more UAVs. Mission control includes the capability to hand over or take control of another UAV to/from another MPCS and prepare or process all the data which must be transmitted to the air vehicle to conduct the mission. The telemetry data essentially provides the same data that would otherwise be displayed to a cockpit pilot, but it is processed and displayed on ground-based equipment. As an aid to the ground-based "pilot," telemetry data also includes real-time video (e.g., in the visible part of the spectrum). The remote piloting functions are also used to facilitate take-off and landing for UAVs that may otherwise operate autonomously by executing programmed flight and sensor operations plans.

Remote sensor control functions serve to extend real-time, direct control of the collection equipment to operators stationed in ground/surface systems. Remote commands may include, for example, turning receivers, aiming directional antenna, changing sensor modes, pointing cameras, adjusting focal length and exposure, setting on-board processing parameters, and a host of other operator-controlled functions. The MPCS is capable of receiving, storing, displaying, and exploiting Modular Mission Payloads (MMP) data received from the Air Vehicle (AV), reformatting the data and transmitting that data to appropriate internal and external users. The MPCS manages the data link and controls the data link operating parameters.

Dynamic retasking functions enable reconnaissance operations to be changed in near-real-time by designated users/operators. Changes may affect the platform, such as navigating to a new track (flight path), or they may affect the sensor suites, such as switching SAR modes or switching from SIGINT to imagery collection.

For all current and future Tactical UAVs, the Tactical Control System has been identified as the system that will provide for real-time and near-real time control of the platform, sensor suite, and communications subsystems, as well as payload product and tactical data dissemination to identified C4I systems during the execution of Tactical UAV missions.

The Tactical Control System (TCS) provides an open architecture system that supports interoperability with all Tactical UAVs. The TCS architecture consists of real-time and non-real time core components and air vehicle specific components integrated using standardized interfaces, networking and data server technologies, and software applications that support distributive processing, functional scaleability, modularity, and portability across service standard computing platforms. The TCS software and hardware architectures have been developed in compliance with the requirements of the JTA and the DII COE. TCS provides the necessary physical components, human-computer interface, Tactical UAV route and payload planner, air vehicle monitoring and control applications, tactical message communications processing, and the connectivity necessary to receive tasking, operate Tactical UAVs and sensors, and support payload product and tactical data dissemination to identified C4I systems.

The following standards are mandated for use in AR systems for any mission planning and control system that is interoperable with Tactical UAVs:

- TCS SDD 117, Tactical Control System (TCS) Software Design Description (SDD), Version 1.0, 31 March 1997 (TCS Document Control Number: TCS-117).

- TCS JII 2, Tactical Control System Joint Interoperability Interface 2 (JII 2) - Tactical Control System to Service Command, Control, Communications, Computers and Intelligence (C4I) Systems, Version 1.0, 9 May 1997 (TCS Document Control Number: TCS-233).
- TCS IDD 229, Tactical Control System Segment to Air Vehicle Standard Segment Interface (TCS AVSI) Interface Design Description (IDD), Version 1.2, 29 August 1997 (TCS Document Control Number: TCS-229).

C4ISR.AR.3.2.3 Emerging Standards

This version of the AR Subdomain Annex does not identify any emerging standards for collection management, mission planning, and control. An ongoing effort by the DARO will identify emerging standards for future versions of the JTA.

This page intentionally left blank.

COMBAT SUPPORT DOMAIN ANNEX

CS.1 DOMAIN OVERVIEW

CS.1.1 PURPOSE

The Combat Support Domain Annex was developed to help Combat Support Elements migrate toward a common technical architecture. This technical architecture will enable the entire DoD community to understand the nuances of the Combat Support community. The goal is to have the rest of DoD community communicate with the Combat Support Elements and either adopt their practices or work to eliminate the differences.

CS.1.2 BACKGROUND

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

CS.1.3 DOMAIN DESCRIPTION

The Combat Support domain addresses those specific elements necessary for the production, use, or exchange of information within and among systems supporting personnel, logistics, and other functions required to maintain operations or combat (see Figure CS-1). 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.

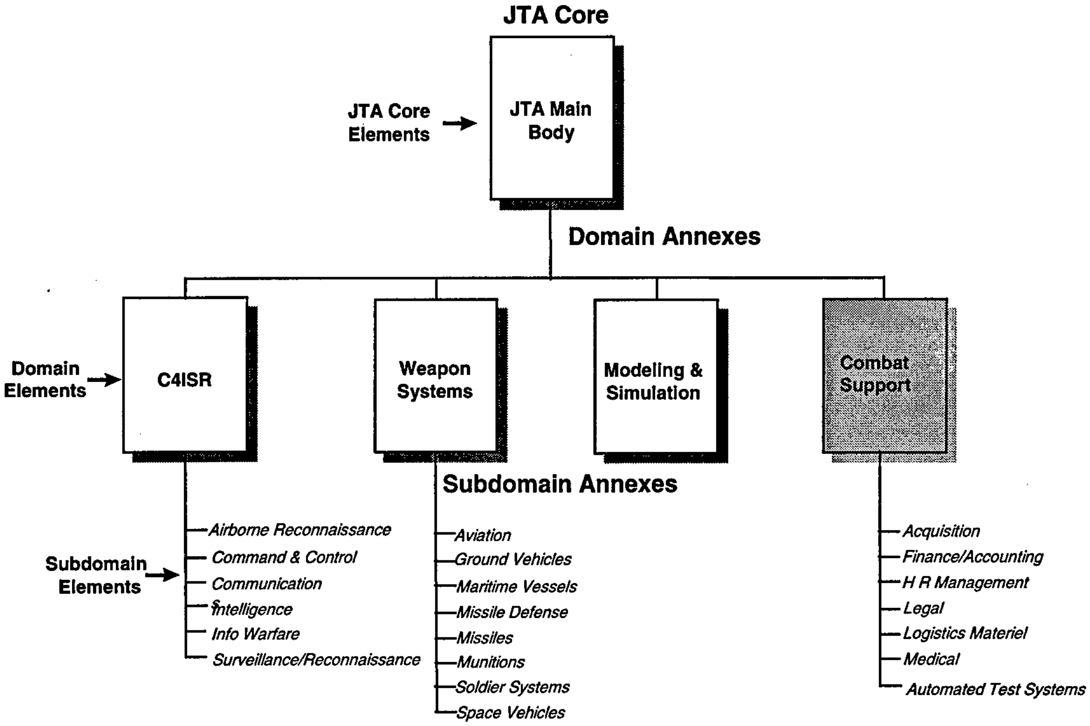


Figure CS-1 Notional JTA Hierarchy

CS.1.4 SCOPE AND APPLICABILITY

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

CS.1.5 TECHNICAL REFERENCE MODEL

This domain uses the Technical Reference Model (DoD TRM) cited in Section 2.1.3. of the JTA as its framework. Combat Support Application Platform Entity service areas are addressed in Section CS.2 as Additions to the JTA Core. Additional Application Software Entity service areas required to support Combat Support domain systems are addressed in Section CS.3 as Domain Specific Service Areas.

CS.1.6 ANNEX ORGANIZATION

The Combat Support Domain Annex consists of three sections. Section CS.1 contains the overview, Section CS.2 contains those information technology standards that are additions to the standards contained in the core, and Section CS.3 is reserved for those mandates for combat support that are domain specific because they do not map directly to the core service areas.

CS.2 ADDITIONS TO JTA CORE

CS.2.1 INTRODUCTION

The Combat Support domain embraces the principles established in Section 2 of the JTA. Only those paragraphs from the core that have additions are included below.

CS.2.2 INFORMATION PROCESSING STANDARDS

CS.2.2.1 Document Interchange

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

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

CS.2.2.2 Graphics Data Interchange

CALS has developed a metadata standard which profiles the ISO CGM standard (8632). The latest FIPS 128-2 also profiles the CGM ISO standard and incorporates CALS CGM (see 2.2.2.2.1.4.2). There is also a CALS Raster Standard that puts raster graphics in a binary format. The mandated standards for the CALS Graphics Data Interchange BSA are:

- ISO 8632 as profiled by MIL-PRF-28003A.
- MIL-PRF-28002C, Requirements for Raster Graphics Representation in Binary Format, 30 September 1997.

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

- NEMA/ACR DICOM V3.0, parts 1-12, Digital Imaging and Communication in Medicine, 1993.

CS.2.2.3 Product Data Interchange

CALS has developed a standard that profiles the IGES standard for Engineering Drawings. IGES is used for CAD/CAM applications. The latest FIPS also profiles IGES and incorporates CALS IGES. CALS STEP is an international standard, which depicts products in three dimensions. MIL-STD-2549 was developed to replace MIL-STD-973, Configuration Management. The AITI (MIL-STD-1840C) also has formats for product data archiving. The Bar Code used by DoD is documented in AIM BC1 "Uniform Symbology specification Code 39." Users are cautioned to evaluate this document for their particular application before citing it as a replacement document of MIL-STD-1189B. The mandatory standards for the Product Data Interchange BSA are:

- FIPS PUB 177-1, IGES, adopts CALS IGES and ANSI/US PRO-100-1993, V5.2, 23 April 1996.
- MIL-PRF-28000A w/AMD 1, Digital Representation for Communications of Product Data: IGES Application Subsets and IGES Application Protocols, 14 December 1992.
- ISO/IEC 10303-1:1994 Standards for the Exchange of Product Model Data (STEP), Part 1: Overview and Principles.
- MIL-STD-2549, Configuration Management Data Interface, 30 June 1997.
- MIL-STD-1840C, Automated Interchange of Technical Information, 26 June 1997.

CS.2.2.4 Electronic Data Interchange

Electronic Data Interchange (EDI) is a new Base Service Area specializing in the computer-to-computer exchange of business information using a public standard. EDI is a central part of Electronic Commerce (EC). EC is the paperless exchange of business information. The 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 World Wide Web at:

http:// www.antd.nist.gov/fededi/l.

The DoD EDI Standards Management Committee (EDISMC) was established for the purpose of coordinating EDI standardization activities within the 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). The DoD FWGs have been established in the following areas: Logistics, Finance, Healthcare, Transportation, Procurement, Communications, Command and Control. EDISMC approved implementation conventions are submitted to the FESMCC for approval as Federal implementation conventions. DoD approved implementation conventions may be viewed on the World Wide Web at:

http://www-edi.itsi.disa.mil.

FIPS PUB 161-2, 22 May 1996, Electronic Data Interchange (EDI) adopts, with specific conditions, ANSI ASC X12, UN/EDIFACT and ANSI HL7.

The following standards are mandated as profiled by FIPS PUB 161-2:

- ANSI ASC X12 Electronic Data Interchange (ASC X12S 97-372 is latest edition).
- ANSI HL7 Version 2.3 (is the latest edition).
- ISO UN/EDIFACT.

CS.2.3 INFORMATION TRANSFER STANDARDS

CS.2.3.1 Additions

There are no additions for the Information Transfer Standards section

CS.2.3.2 Emerging Standards

The following standard is not mandated in this version of the JTA, but is an emerging standard for the next version of the JTA:

– IEEE 1073, Protocol for Medical Device Communications, 1996.

CS.2.4 INFORMATION MODELING, METADATA, AND INFORMATION EXCHANGE STANDARDS

There are no additions or emerging standards for the Combat Support Information Modeling, Metadata, and Information Exchange Standards section.

CS.2.5 HUMAN-COMPUTER INTERFACE STANDARDS

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

CS.2.6 INFORMATION SYSTEMS SECURITY STANDARDS

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

CS.3 DOMAIN SPECIFIC SERVICE AREAS

There are no domain specific service areas for the Combat Support Domain.

This page intentionally left blank.

AUTOMATIC TEST SYSTEMS SUBDOMAIN ANNEX FOR THE COMBAT SUPPORT DOMAIN

CS.ATS.1 SUBDOMAIN OVERVIEW

CS.ATS.1.1 PURPOSE

The Automatic Test Systems (ATS) Subdomain Annex identifies additions to the Combat Support Domain Annex core elements (i.e., standards, interfaces, and service areas) listed in Section 2 of this document. These additions are common to the majority of ATS and support the functional requirements of these systems.

The purpose of the ATS Subdomain Annex is:

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

CS.ATS.1.2 BACKGROUND

From 1980 to 1992, the US DoD investment in depot and factory ATS 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 the DoD appear to be a variety of separate customers. To address this problem, the DoD enacted policy changes that require 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) (ARI) sponsored the Critical Interfaces (CI) Working Group, which recommended interfaces and standards that should be mandated for DoD ATS acquisitions. The CI report became the basis for this document which is an annex to the Joint Technical Architecture (JTA). The ATS Subdomain Annex will aid in satisfying the requirements of DoD Regulation 5000.2-R to migrate DoD designated tester families towards a common architecture.

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

- DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information System Acquisition Programs", March 15, 1996[1], 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).
- Secretary of Defense Memorandum on Specifications and Standards - 29 June 1994, directs that DoD procurements will 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 ATS has been projected to provide the following five benefits.[2]

- 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 Test Program Sets (TPSs).
- Decrease the use of custom hardware from approximately 70% today to 30%.
- Reduce engineering costs 70%.
- Reduce TPS integration time and cost 50-75%.
- Provide an iterative improvement in the quality of test by the reuse and refinement of libraries.

CS.ATS.1.3 SUBDOMAIN DESCRIPTION

A high level overview of a typical ATS is shown in Figure CS.ATS-1. An ATS has three major components: Automated Test Equipment (ATE), TPSs, and the Test Environment. The ATE consists of test and measurement instruments, a host computer, switching, communication busses, 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 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, and a standard format for describing UUT design requirements and test strategy information that allows TPS software to be produced at a lower cost. The ATS architecture shown in Figure CS.ATS-1 is expanded into more detail in the hardware and software technical reference models introduced in Section CS.ATS.1.4. Each interface in the technical reference models is discussed in more detail in Sections CS.ATS.2 and CS.ATS.3.

[1] DoD Regulation 5000.2-R, paragraph 4.3.3.4, 15 March 1996. *"DoD Automated Test System (ATS) families or COTS components that meet defined ATS capabilities shall be used to meet all acquisition needs for automatic test equipment hardware and software. ATS capabilities shall be defined through critical hardware and software elements. The introduction of unique types of ATS into the DoD field, depot, and manufacturing operations shall be minimized."*

[2] Institute for Defense Analysis (IDA) *Investment Strategy Study* 1993

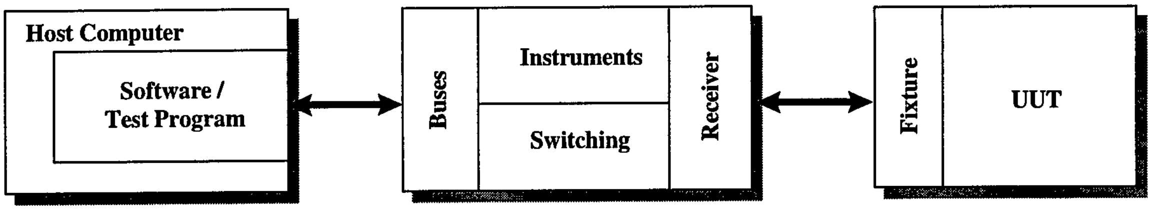


Figure CS.ATS-1 Generic ATS Architecture

CS.ATS.1.4 SCOPE AND APPLICABILITY

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

- 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 Annex are mandated for depot and intermediate level ATS only. The standards may be mandated for operational/organizational level use in the future.

The standards selected for inclusion in the ATS Subdomain Annex were found to be key for the generic open system architecture for ATS. 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 Annex 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 their own sets of standards (e.g., technical architectures). The ATS Subdomain Annex is envisioned as a single generic open system architecture for ATS for the DoD. The ATS Subdomain Annex shall be used by anyone involved in the management, development, or acquisition of new or improved ATS within DoD. System developers shall use the ATS Subdomain Annex to ensure that new and upgraded ATS, 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 Annex in developing requirements and functional descriptions. ATS is a subdomain of the Combat Support domain of the JTA.

CS.ATS.1.5 TECHNICAL REFERENCE MODEL

CS.ATS.1.5.1 Hardware

The hardware interfaces in a typical ATS are shown in Figure CS.ATS-2. Mandates were only made for interfaces that have an impact on the interoperability and life-cycle costs of ATS across the DoD and for which widely accepted commercial standards exist. Mandates were not made for interfaces that are not supported by commercial standards, nor were they made for interfaces that do not affect the interoperability and life-cycle costs of DoD ATS. Unsupported interfaces that impact the interoperability and life-cycle costs of DoD ATS are identified in the section on emerging standards.

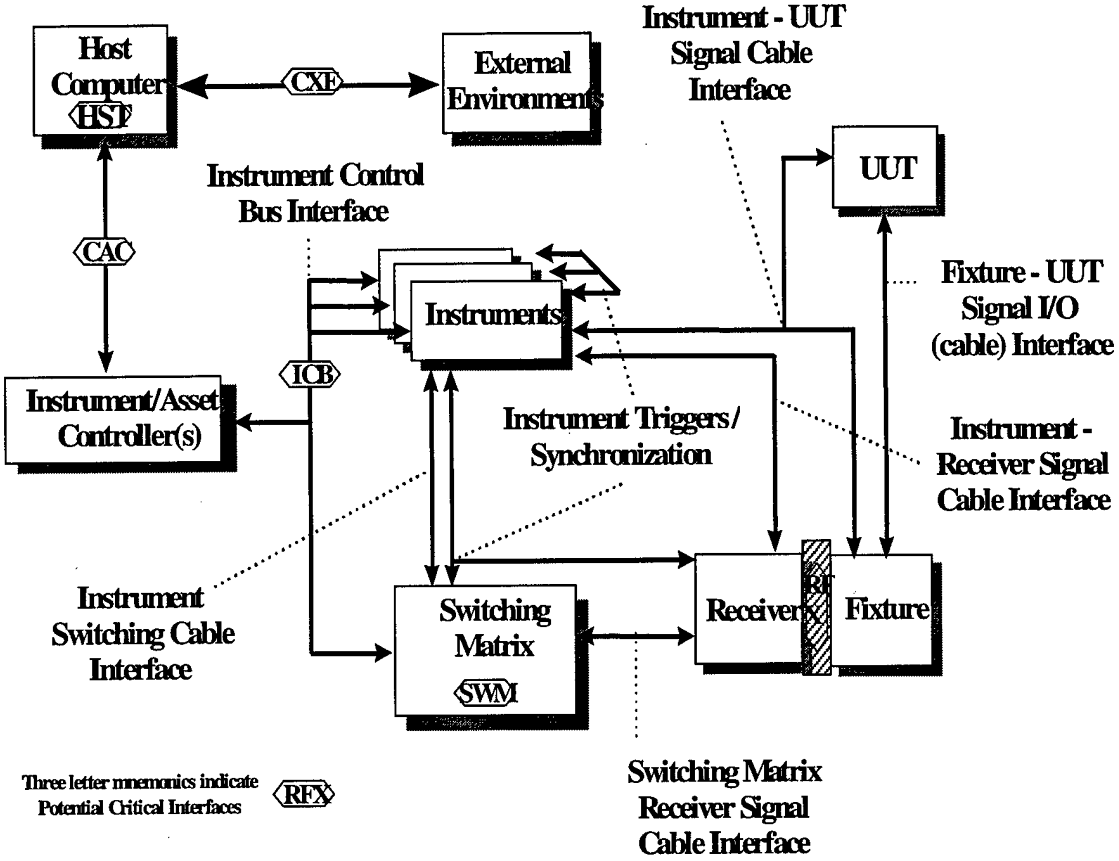

Host Computer
HST
CXE
External Environments
Instrument - UUT Signal Cable Interface
UUT
Instrument Control Bus Interface
CAC
Instruments
Fixture - UUT Signal I/O (cable) Interface
ICB
Instrument/Asset Controller(s)
Instrument Triggers / Synchronization
Instrument - Receiver Signal Cable Interface
Instrument Switching Cable Interface
Switching Matrix
SWM
Receiver
RFX
Fixture
Three letter mnemonics indicate Potential Critical Interfaces
RFX
Switching Matrix Receiver Signal Cable Interface

Figure CS.ATS-2 Hardware Interfaces

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

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

- **Switching Matrix Interface (SWM)** describes switch paths that connect ATS test and measurement instruments to pins on the RFX.

CS.ATS.1.5.2 Software

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

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

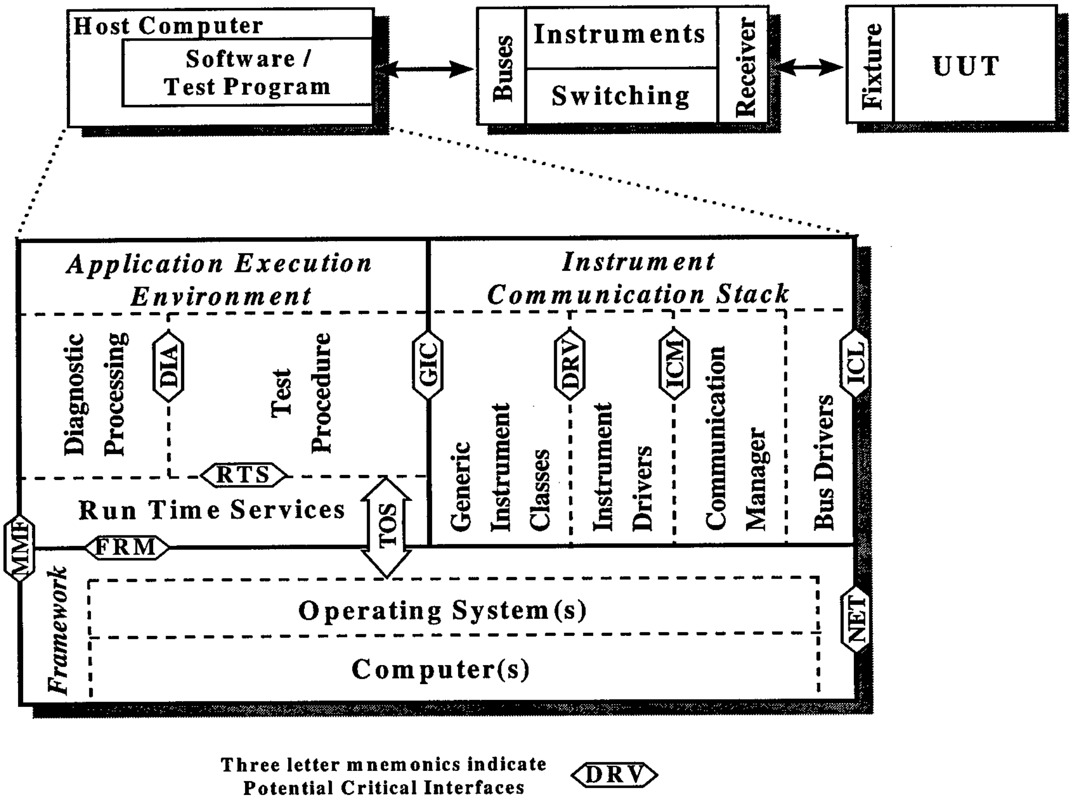


Figure CS.ATS-3 TPS Run Time Interfaces

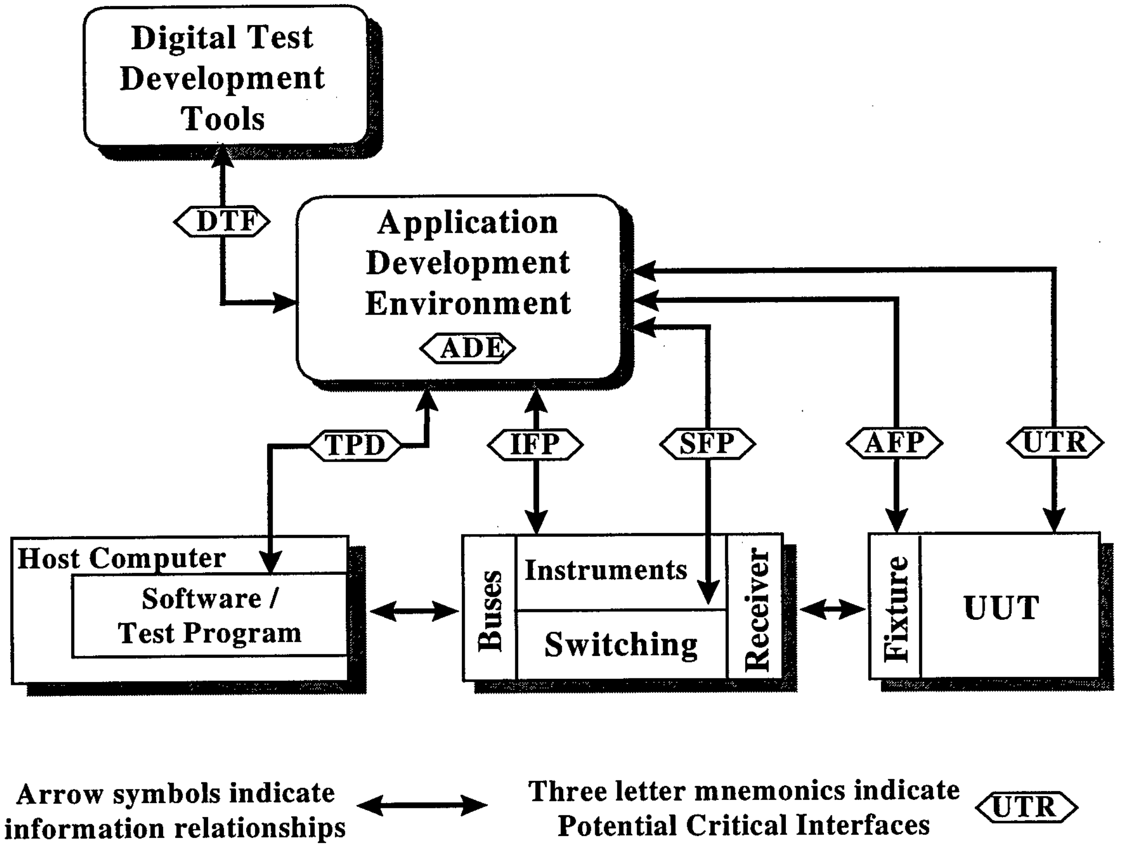

Digital Test Development Tools
DTF
Application Development Environment
ADE
TPD
IFP
SFP
AFP
UTR
Host Computer
Software / Test Program
Buses
Instruments
Switching
Receiver
Fixture
UUT
Arrow symbols indicate information relationships
Three letter mnemonics indicate Potential Critical Interfaces
UTR

Figure CS.ATS-4 TPS Development Interfaces

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

- **Diagnostic Processing (DIA)** is the interface protocol linking execution of a test with software diagnostic processes that analyze the significance of the test results and suggest conclusions or additional actions required.
- **Instrument Driver API (DRV)** is the Application Programming Interface (API) through which instrument drivers accept commands from and return results to Generic Instrument Classes.
- **Framework (FRM)** is a collection of system requirements, software protocols, and business rules (e.g., software installation) affecting the operation of test software with its host computer and Operating System (OS).
- **Generic Instrument Classes (GIC)** is the interface through which instrument drivers accept commands from and return results to test procedures or run time services serving the Test Program.
- **Instrument Command Language (ICL)** is the language in which instrument commands and results are expressed as they enter or leave the instrument.
- **Instrument Communication Manager (ICM)** is the interface between the instrument drivers and the Communication Manager that supports communication with instruments independent of the bus or other protocol used (e.g., VXI, IEEE-488.2, RS-232).
- **Multimedia Formats (MMF)** denotes the formats used to convey hyperlink text, audio, video and three-dimensional physical model information from multimedia authoring tools to the Application Development Environment (ADE), Application Execution Environment, and host framework.
- **Network Protocol (NET)** is the protocol used to communicate with external environments, possibly over a Local or Wide Area Network. The software protocol used on the CXE hardware interface is represented by the NET software interface.

- **Run Time Services (RTS)** denotes the services needed by a TPS not handled by the services supplied by the DRV, FRM, GIC, and NET, (e.g., error reporting, data logging).
- **Test Program to Operating System (TOS)** denotes system calls to the host OS made directly from the TPS.

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

- **Application Development Environments (ADE)** is the interface by which the test engineer creates and maintains a TPS, whether captured in the form of a text or graphical language.
- **Adapter Function and Parametric Data (AFP)** is the information and formats used to define to the ADE the capabilities of the test fixture, how the capabilities are accessed, and the associated performance parameters.
- **Instrument Function and Parametric Data (IFP)** is the information and formats used to define to the ADE the load, sense, and drive capabilities of the instruments, how these capabilities are accessed, and the associated performance parameters.
- **Switch Function and Parametric Data (SFP)** is the information and formats used to define to the ADE the interconnect capabilities of the switch matrix, how these capabilities are accessed, and associated performance parameters.
- **Test Program Documentation (TPD)** is human-understandable representations of information about the TPS for use by the TPS maintainer.
- **UUT Test Requirements (UTR)** is the information and formats used to define to the ADE the load, sense, and drive capabilities that must be applied to the UUT to test it, including the minimum performance required for a successful test.

CS.ATS.1.6 ANNEX ORGANIZATION

The ATS Subdomain Annex consists of three main sections. Section one contains the overview, section two contains the additions to the JTA core service areas for ATS, and section three contains the domain specific service areas for ATS. A list of sources is provided in Appendix B. In cases where the ATS Subdomain Annex does not address an interface to be used in an ATS, the JTA takes precedence. In cases where the JTA and ATS Subdomain Annex specify different standards for the same interface, the ATS Subdomain Annex takes precedence.

CS.ATS.1.7 CONFIGURATION MANAGEMENT

Configuration management of the ATS Subdomain Annex will be the responsibility of the joint service ARI. All changes will be approved by the ATS EAO with coordination from the ATS Management Board (AMB).

CS.ATS.2 ADDITIONS TO THE JTA CORE

CS.ATS.2.1 INTRODUCTION

The standards in the ATS Subdomain Annex apply in addition to the standards in the Combat Support Domain and the JTA core.

CS.ATS.2.2 INFORMATION PROCESSING STANDARDS

CS.ATS.2.2.1 Mandate Additions

CS.ATS.2.2.1.1 Instrument Driver API Standards

The DRV is the interface between the generic instrument class serving the test procedure and the instrument driver. The calls made available at this interface include calls oriented to software housekeeping, such as initializing the driver itself, and calls that cause the instrument to perform a function, such as arm and measure commands. The service requests crossing this interface are communications between generic ATS assets (e.g., digital multimeter) and specific ATS assets (e.g., vendor XYZ model 123 digital multimeter). The instruments are ATS assets, but the calls to the driver are either direct or close-to-direct consequences of action requests in the Test Procedure which is a TPS asset. Some instrument functions are available from a variety of instruments. However, the driver calls to access these functions vary from instrument to instrument. This interferes with TPS portability. Historically, cross-platform incompatibilities in the way drivers for the same instrument implement the same function have been a recurring ATS integration problem. In common commercial practice, the driver is acquired with the instrument from the instrument's original equipment manufacturer. The DRV API interface allows software developed by different organizations to work together. No standards are mandated in this version of the JTA, but an emerging standard is given in Section CS.ATS.2.2.2.1.

CS.ATS.2.2.1.2 Digital Test Data Formats

Digital Test Data Formats (DTF) 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 that are used for the fault dictionary. In addition, certain diagnostic data may exist that are closely associated with the digital test data. This interface is intended to be used for capturing the output of digital automatic test pattern generators. No standards are mandated in this version of the JTA, but an emerging standard is given in section CS.ATS.2.2.2.2.

CS.ATS.2.2.2 Emerging Standards

CS.ATS.2.2.2.1 Instrument Driver API Standards

The following standard may be mandated in a future version of the JTA:

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

CS.ATS.2.2.2.2 Digital Test Data Formats

A standard for describing DTF, known as LSRTAP, has become a de facto industry standard. The LSRTAP standard was submitted to the IEEE for formal standardization and is currently being voted on. The following standard may be mandated in a future version of the JTA:

- NAWCADLKE-MISC-05-PD-003, Navy Standard Digital Simulation Data Format (SDF), January 1998.

Note: The Navy specification for LSRTAP will be replaced with the IEEE standard (IEEE P1445) upon final approval from the IEEE.

CS.ATS.2.2.2.3 Generic Instrument Class Standards

The Generic Instrument Class (GIC) is the interface between the generic instrument classes serving the test procedure or run time services and the instrument driver. The service requests crossing this interface are communications between the TPS requirements (e.g., measure voltage of a sine wave) and generic ATS assets (e.g., digital multimeters, waveform generators, and power supplies). Industry has indicated an interest in pursuing a standard in this area. Some examples are the IEEE 1226 ABBET standard and the VXI*plug&play* Systems Alliance.

CS.ATS.2.2.2.4 Diagnostic Processing Standards

The diagnostic processing interface resides between the test procedure or run time 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 Fault Isolation System, and 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. Industry has indicated an interest in pursuing a standard in this area. One example is IEEE 1232.1: 1997, *Artificial Intelligence Exchange and Services Tie to All Test Environments* (AI-ESTATE).

CS.ATS.2.2.2.5 Adapter Function and Parametric Data Standards

This information defines the electrical behavior of the fixture which connects the UUT to the ATS. Functional descriptions are included to allow for the case of active fixtures. Describing the function of the fixture begins with a statement of the wirelist association between receiver terminals and UUT terminals. Performance parameters are required to complete the characterization of the path between the instrument and the UUT, so as to be able to construct a model of the effective instrument applied to the UUT signals (characterized with reference to the UUT interface). Industry has indicated an interest in pursuing a standard in this area. One example of this is the IEEE P1226.11 ABBET *Test Resource Information Model* (TRIM).

CS.ATS.2.2.2.6 ATS Instrument Function and Parametric Data Standards

This interface defines the capabilities of the ATS stimulus and measurement devices, how they are controlled, and how they are connected within the ATS. It includes:

- **Instrument Capabilities** - This defines what the instrument can measure, stimulate, and/or load the circuits to which it is attached. It includes identifying the function, such as measure volts, and quantitative performance characteristics including the range over which a voltage can be measured and the resolution and accuracy (as a function of choice of range) to be expected from the measured value.
- **Instrument Control** - The command vocabulary by which the instrument can be controlled to apply these behaviors.
- **Instrument Limits** - Limits are associated both with the safety of the instrument and surety of resolution performance. For example: *"Do not expose this instrument to more than 1 KV across the sensing terminals"* or *"Accuracy of voltage stimulus guaranteed with the instrument sourcing up to 100 mA."*

Industry has indicated an interest in pursuing a standard in this area. One example of this is the IEEE P1226.11 ABBET TRIM.

CS.ATS.2.2.2.7 ATS Switching Function and Parametric Data Standards

This interface defines the capabilities of the ATS switching devices, how they are controlled, and how they are interconnected with other ATS devices. It includes the possible states of the separately-setable switch elements, the connectivity through the switch in each such state, and electrical performance characteristics of the paths connected as a result of the switch state. The parametric information includes as-installed electrical path performance from the point to which the instrument characteristics are referenced out to the receiver/fixture disconnect surface. Industry has indicated an interest in pursuing a standard in this area. One example of this is the IEEE P1226.11 ABBET TRIM.

CS.ATS.2.2.2.8 UUT Test Requirements Data Standards

High re-host costs in the past have been associated with the failure to record or preserve the signal-oriented action capabilities *as required* as opposed to *as used.* This problem is most visible in the allocation phase of TPS development. When a TPS is transported or re-hosted, the resources requested by the TPS must be allocated to assets in the target ATS. This task would be simplified if UUT test requirements in the form of load specifications, measurement requirements, and stimuli requirements that must appear at the UUT interface were available. Industry has indicated an interest in pursuing a standard in this area. Some examples of this are the IEEE P1029.3 Test Requirements Specification Language (TRSL) and the Electronics Industry Association's Electronic Design Interchange Format (EDIF).

CS.ATS.2.2.2.9 TPS Documentation Standards

The TPS Documentation interface consists of the supporting documentation, provided by the TPS developer, whose purpose is to convey an understanding of the design philosophies incorporated into the various elements of the TPS hardware and software, along with detailed instructions for selected processes such as how to regenerate the executable program from the source libraries provided. These documents may include the Test Strategy Report (TSR), Diagnostic Flow Charts (DFC), Test Requirements Document (TRD), Test Diagrams, Test Program Instruction (TPI), and Automatic Test Program Generator (ATPG) support data. These data are bundled together in the Test Program Documentation (TPD) interface. The following Data Item Descriptions are being considered for mandates:

- DI-ATTS-80284A, Test Program Set Document.
- DI-ATTS-80285A, Engineering Support Data.

CS.ATS.2.3 INFORMATION TRANSFER STANDARDS

CS.ATS.2.3.1 Mandate Additions

CS.ATS.2.3.1.1 Data Networking Standards

In an ATS that has either internal (controller to controller) or external (controller to external host) networking, standardizing on a networking protocol should reduce the amount of time spent re-hosting a TPS between two organizations. This problem becomes more serious if the ADE that is controlling the ATS has built-in applications that are network objects (either clients, servers, routers, or other). In these instances, porting the ADE between platforms becomes more difficult since it may support different network protocols and different operating environments. Also important is the transfer of test result data for logistics and maintenance engineering purposes, i.e., tracking of UUT, failure modes, and test results analysis. By defining a specific protocol as the choice for data communications, these problems will be significantly reduced. Networking accelerates the distribution of updates for TPSs that are operational on a large number of widely distributed ATSs. No data networking standards are mandated in this version of the JTA, but an emerging standard is given in section CS.ATS.2.3.2.1.

CS.ATS.2.3.1.2 Instrument Communication Manager Standards

The ICM interface includes bus-specific options for communicating from the instrument driver to a supporting Input/Output (I/O) library. Until recently, vendors of IEEE-488 and VXI bus hardware provided software drivers for their buses that were different according to the hardware bus protocol or Operating System (OS) used. This situation interfered with the plug and play capabilities that users thought they were going to get from buying different instruments that all communicated by common hardware protocols. The same functions of the same instruments were not accessed through software in the same way across buses and host platforms. Different manufacturers of IEEE-488 cards had proprietary and unique software calls. Furthermore, Hewlett-Packard and National Instruments, the two leading vendors of VXI slot0 cards and embedded controllers, used different I/O calls to access instruments. This impeded the transporting of instrument drivers, ADEs, and test programs from one set of hardware to another. Without a standard ICM interface, vendors cannot provide interoperable or portable instrument drivers because different vendors would use different I/O drivers at the very lowest layer of the software. This forces instrument drivers to be tailored to specific I/O calls for each test station and lowers the likelihood that instrument drivers will be commercially available for each configuration. In addition, standard I/O software allows one to place parameters such as bus addresses.and instrument addresses in the instrument driver instead of the test program. No instrument communication manager standards are mandated in this version of the JTA, but an emerging standard is given in Section CS.ATS.2.3.2.2.

CS.ATS.2.3.2 Emerging Standards

CS.ATS.2.3.2.1 Data Networking Standards

ATS and development systems that are elements of ATS must maintain networking capabilities that conform with current Internet standards. Current Internet standards are identified in the Internet Official Protocol Standards Index as released by the Internet Architecture Board (IAB), which may be mandated in a future version of the JTA:

- Any hardware that has support for the software protocol standards specified in JTA Section 2.3.2.1.1.2.1.1, Transmission Control Protocol (TCP) and JTA Section 2.3.2.1.1.2.1.3, Internet Protocol (IP) may be used; however TCP and IP are mandated by the JTA core document. Unacknowledged, connectionless, datagram transport services will not be used in ATS.

CS.ATS.2.3.2.2 Instrument Communication Manager Standards

A standard ICM interface enables higher level software to be interoperable and portable between vendors and across different platforms. This improves the interoperability of test software and the ability to re-host test software from one test system to another. The following specification may be mandated in a future version of the JTA:

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

CS.ATS.2.4 INFORMATION MODELING, METADATA, AND INFORMATION EXCHANGE STANDARDS

CS.ATS.2.4.1 Mandate Additions

There are currently no additions applicable to ATS with respect to Information Modeling, Metadata, and Information Transfer Standards as specified in Section 2.4 of the JTA.

CS.ATS.2.4.2 Emerging Standards

There are currently no emerging standards identified in this section of the ATS Subdomain Annex.

CS.ATS.2.5 HUMAN-COMPUTER INTERFACE STANDARDS

CS.ATS.2.5.1 Mandate Additions

There are currently no additions applicable to ATS with respect to Human-Computer Interface Standards as specified in Section 2.5 of the JTA.

CS.ATS.2.5.2 Emerging Standards

There are currently no emerging standards identified in this section of the ATS Subdomain Annex.

CS.ATS.2.6 INFORMATION SYSTEMS SECURITY STANDARDS

CS.ATS.2.6.1 Mandate Additions

There are currently no additions applicable to ATS with respect to Information Systems Security as specified in Section 2.6 of the JTA.

CS.ATS.2.6.2 Emerging Standards

There are currently no emerging standards identified in this section of the ATS Subdomain Annex.

CS.ATS.3 SUBDOMAIN SPECIFIC SERVICE AREAS

CS.ATS.3.1 SOFTWARE ENGINEERING SERVICES

CS.ATS.3.1.1 Mandates

CS.ATS.3.1.1.1 Test Program to Operating System Calls

The TOS interface defines calls to host OS functions from the TPS. Some TPSs are highly dependent upon system calls unique to the initial TPS development system OS. A common use of calls to the OS in a TPS is in the area of file I/O. At the time of re-host, the OS calls may not be supported on the target ATS. OS calls are a chronic cause of non-portability in software. The best measure that will alleviate the transportability and re-hostability problems associated with OS calls is to ban them entirely. This also ensures that the TPS is developed with an ADE that provides enough encapsulated run time services to preclude the need for direct calls to the OS. The problems associated with calling OS utilities from within a TPS can be generalized to problems that occur if the next interface in the process is bypassed. For example, interoperability will be reduced if an instrument driver bypasses the ICM interface and calls a function outside of the VISA (VPP-4.x) library or if functions that are supported by VISA are embedded in an instrument driver and implemented in a non-standard manner. No test program to operating system call standards are mandated in this version of the JTA, but a rule which may be mandated in a future version of the JTA is given in Section CS.ATS.3.1.2.1.

CS.ATS.3.1.2 Emerging Standards

CS.ATS.3.1.2.1 Test Program to Operating System Calls

The following rule may be mandated in a future version of the JTA.

- Any element of the technical architecture that is implemented shall not be bypassed by a direct communication to another interface or layer further on in the process.

CS.ATS.3.2 DATA/INFORMATION SERVICES

CS.ATS.3.2.1 Mandates

This version of the ATS Subdomain Annex does not contain any domain-specific mandated standards in the area of data/information services.

CS.ATS.3.2.2 Emerging Standards

CS.ATS.3.2.2.1 Run Time Services

The RTS interface encompasses data logging services, operator I/O, timing and tasking control, and resource allocation performed at execution. This interface defines the means by which run time services are called during TPS execution. Although standards do not exist, various implementations do. Standardization in this area would allow the use of various test executives with any language that they support. Proprietary implementations of the interface between the TPS and Test Executive exist. However, the means by which various run time services are called depends upon the implementation. Direct transportability of a TPS across platforms will be compromised if the TPS requires run time services that are not supported on both systems or if the calling method differs between the host and target platforms.

Industry has indicated an interest in pursuing a standard in this area. Some examples are IEEE P1226.10, Microsoft's COM/OLE *(Component Object Model/Object Linking and Embedding)*, and Object Management Group's CORBA *(Common Object Request Broker Architecture).*

CS.ATS.3.3 PLATFORM/ENVIRONMENT SERVICES

CS.ATS.3.3.1 Mandates

CS.ATS.3.3.1.1 Computer to External Environments

The Computer to External Environments (CXE) interface describes the communication methods between a host ATS and remote systems. This includes paths between the target ATS host computer and other ATS systems as well as TPS development stations which are part of the Test Environment. This interface supports transporting TPS software and supporting documentation between organizations. Examples of this interface include Ethernet, RS-232, and IEEE-488.

Any hardware that has support for the software protocol standards specified in JTA Sections 2.3.2.1.1.2.1.1 and 2.3.2.1.1.2.1.3, Transmission Control Protocol (TCP) over Internet Protocol (IP), may be used.

CS.ATS.3.3.1.2 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. No system framework standards are mandated in this version of the JTA, but a standard which may be mandated in a future version of the JTA is given in Section CS.ATS.3.3.2.1.

CS.ATS.3.3.2 Emerging Standards

CS.ATS.3.3.2.1 System Framework Standards

The following standard may be mandated in a future version of the JTA.

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

CS.ATS.3.3.2.2 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 ATS. 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. Industry has indicated an interest in pursuing a standard in this area. One example of this is the Receiver Fixture Interface (RFI) Alliance.

CS.ATS.3.3.2.3 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 increase interoperability by ensuring that ATS instruments needed to test a UUT can be switched to pins required by the fixture.

CS.ATS.3.3.3 Other Standards

The interfaces described in this section are provided for completeness of the ATS Subdomain Annex and to make readers aware that these interfaces have been addressed. Standards for these interfaces are not mandated because they were not found to be key for the generic open system architecture for ATS.

CS.ATS.3.3.3.1 Computer Asset Controller Interface

The Computer Asset Controller (CAC) interface describes the communication paths between the host computer and instrument controllers in a distributed system. These interfaces may be internal or external to the host computer. Examples of internal interfaces are Industry Standard Architecture (ISA) and Peripheral Component Interface (PCI). Examples of external interfaces are IEEE-488, RS-232, Ethernet, Multisystem Extension Interface, and Modular System Interface Bus.

CS.ATS.3.3.3.2 Host Computer Interface

The Host Computer (HST) interface describes the processing architecture of the primary control computer where the TPS is executed and through which the operator interfaces. Portions of the HST interface affect the interoperability of ATS. These requirements are included in the Frameworks software interface.

CS.ATS.3.3.3.3 Instrument Control Bus Interface

The Instrument Control Bus (ICB) interface describes the connection between the host computer or instrument controller and the test and measurement instruments in the ATS. Examples of these interfaces are IEEE-488, VME, and VME Extensions for Instrumentation (VXI).

CS.ATS.3.3.3.4 Instrument Command Language

The Instrument Command Language (ICL) interface describes how instrument commands and results are expressed as they enter or leave test and measurement instruments. The requirements for this interface are satisfied by the DRV and GIC interfaces.

CS.ATS.3.3.3.5 Application Development Environments

The Application Development Environment (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.

MODELING AND SIMULATION DOMAIN ANNEX

The Defense Modeling and Simulation Office (DMSO) manages this annex.

M&S.1 DOMAIN OVERVIEW

M&S.1.1 PURPOSE

The Modeling and Simulation (M&S) Domain Annex identifies additions to the JTA core elements (standards, interfaces, and service areas) listed in Section 2 of the JTA. These additional standards are key to the interoperability of M&S within DoD among themselves and real-world systems.

M&S.1.2 BACKGROUND

In 1992 DoD established a vision for modeling and simulation, as stated in the DoD M&S Master Plan. "Defense modeling and simulation will provide readily available, operationally valid environments for use by the DoD Components:

- To train jointly, develop doctrine and tactics, formulate operational plans, and assess warfighting situations.
- To support technology assessment, system upgrade, prototype and full-scale development, and force structuring.

Common use of these environments will promote a closer interaction between the operations and acquisition communities in carrying out their respective responsibilities. To allow maximum utility and flexibility, these modeling and simulation environments will be constructed from affordable, reusable components interoperating through an open systems architecture." (Executive Council for Modeling & Simulation).

Department of Defense Directive 5000.59, DoD Modeling and Simulation (M&S) Management, January 4, 1994, and DoD 5000.59-P, DoD Modeling and Simulation (M&S) Master Plan (MSMP), October 1995, outline DoD policies, organizational responsibilities and management procedures for M&S and provide a comprehensive strategic plan to achieve DoD's vision of readily available, authoritative, interoperable and reusable simulations.

Objective 1 of the DoD MSMP states "Provide a common technical framework for M&S" and includes, under sub-objective 1-1, the establishment of "a common high level simulation architecture to facilitate the interoperability of all types of simulations among themselves and with C4I systems, as well as to facilitate the reuse of M&S components." The efficient and effective use of models and simulations across the Department of Defense and supporting industries requires a common technical framework for M&S to facilitate interoperability and reuse. This common technical framework consists of: (1) a high level architecture (HLA) to which simulations must conform; (2) conceptual models of the mission space (CMMS) to provide a basis for the development of consistent and authoritative M&S representation; (3) 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 which have been developed and used successfully for specific classes of simulation. These include Distributed Interactive Simulation (DIS) protocol standards which support networked, real-time, platform-level virtual simulation and the Aggregate Level Simulation Protocol (ALSP) which is used to support distributed, logical-time, constructive simulations. The HLA provides a common architecture for all classes of simulation and, consequently, the HLA supersedes both the DIS and ALSP standards. Transition of simulations from use of other standards is underway in accordance with DoD M&S policy.

M&S.1.3 DOMAIN DESCRIPTION

This annex 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 the Department and supporting industries are integrating and operating a mix of computer simulations, actual warfighting systems, weapons simulators and instrumented ranges to support a diversity of applications including training, mission rehearsal, operational course of action analysis, investment analysis, and many aspects of acquisition support throughout all phases of the system lifecycle. Figure M&S-1 shows the position of the M&S domain in the Notional JTA Hierarchy.

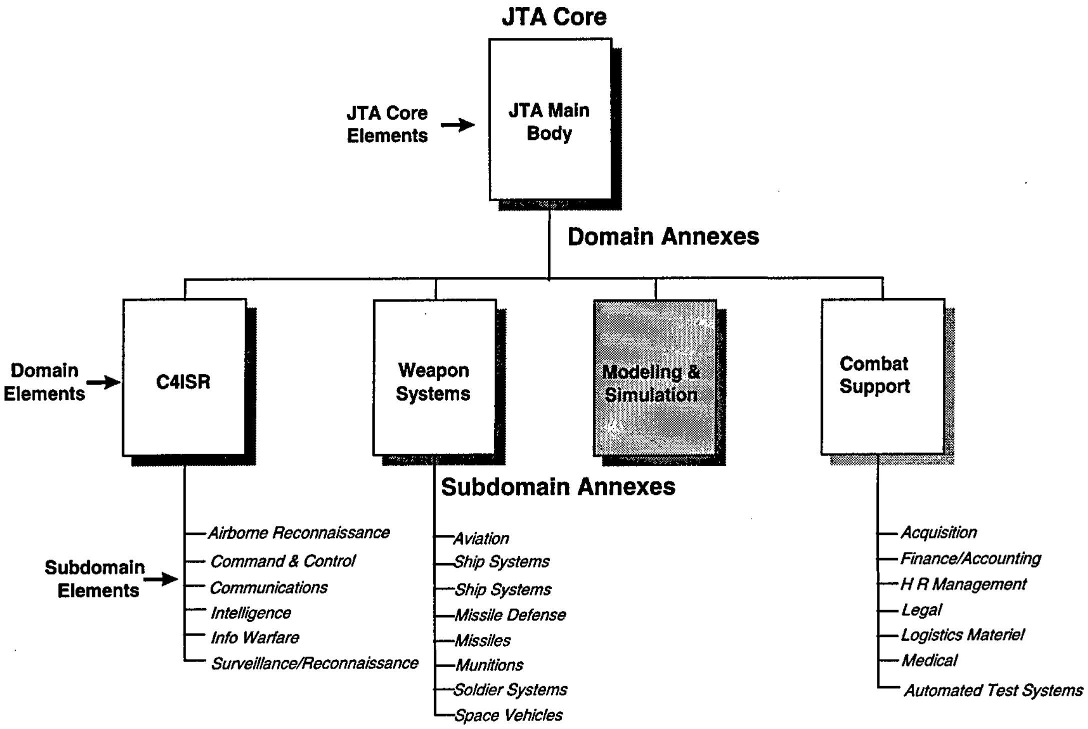


Figure M&S-1 Notional JTA Hierarchy

M&S.1.4 SCOPE AND APPLICABILITY

The Under Secretary of Defense for Acquisition and Technology (USD(A&T)) in 1996 designated the HLA as the standard technical architecture for all DoD simulations. The HLA is a technical architecture that applies to all classes of simulations, including virtual simulations, constructive simulations, and interfaces to live systems. The virtual simulation class comprises human-in-the-loop simulators. The constructive simulation class includes wargames and other automated simulations which represent actions of people and systems in the simulation. The live simulation class includes C4I systems, weapon systems/platforms, and instrumented ranges.

The High Level Architecture 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 annex provide the framework within which specific systems, targeted against precise requirements, can be developed. While many of these systems will operate in computational environments that are considered standard and fall within the spectrum of the other JTA standards, some may require massively-parallel processing or other unique, laboratory configurations, bringing with them their own set of requirements. Simulation developers should follow those standards required for the environment in which the simulation is implemented.

Mandates listed in this domain annex are in addition to those listed in Section 2 of the JTA core.

M&S.1.5 TECHNICAL REFERENCE MODEL

There is no separate Technical Reference Model established for the M&S Domain.

M&S.1.6 ANNEX ORGANIZATION

The Modeling and Simulation Domain Annex consists of three sections. Section M&S.1 contains the overview, Section M&S.2 contains those Information Technology standards that are additions to the standards contained in the core, and Section M&S.3 is reserved for those mandates for modeling and simulation that are domain specific because they do not map directly to the core service areas.

M&S.2 ADDITIONS TO THE JTA CORE

M&S.2.1 INTRODUCTION

The following standards apply in addition to those found in the core of the JTA. On September 10, 1996 the Under Secretary of Defense for Acquisition and Technology (USD(A&T)) designated the High Level Architecture (HLA) as the standard technical architecture for all DoD simulations. The HLA, as mandated, is defined by the HLA Rules, the HLA Interface Specification and the HLA Object Model Template Specification. Compliance criteria have been set forth in the compliance checklist, which was developed as part of the HLA, along with the HLA test procedures. These form the technical basis for HLA compliance. The following additional standards are mandated, current versions of which are listed and available at the Defense Modeling and Simulation Office World Wide Web site at:

http://www.dmso.mil

M&S.2.2 INFORMATION PROCESSING STANDARDS

M&S.2.2.1 Introduction

In addition to those mandates for Information Processing Standards described in Section 2.2 of the JTA, the following are unique mandates applicable to the Modeling and Simulation Domain.

M&S.2.2.2 Mandates

M&S.2.2.2.1 HLA Rules

HLA Rules: These 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.

- High Level Architecture Rules, Version 1.3, February 1998.

M&S.2.2.2.2 HLA Interface Specification

HLA Interface Specification: HLA federates interact with an RTI (analogous to a special-purpose distributed operating system) to establish and maintain a federation and to support efficient information exchange among simulations and other federates. The HLA interface specification defines the nature of these interactions, which are arranged into sets of basic RTI services.

- High Level Architecture Interface Specification, Version 1.3, February 1998.

M&S.2.2.2.3 HLA Object Model Template Specification

HLA Object Model Template: The HLA requires simulations (and other federates) and federations to each have an object model describing the entities represented in the simulations and the data to be exchanged across the federation. The HLA Object Model Template prescribes the method for recording the information in the object models, to include 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.

- High Level Architecture Object Model Template, Version 1.3, February 1998.

M&S.2.3 INFORMATION TRANSFER STANDARDS

There are no additional Information Transfer Standards applicable to modeling and simulation beyond those specified in Section 2.3 of the JTA.

M&S.2.4 INFORMATION MODELING, METADATA, AND INFORMATION EXCHANGE STANDARDS

M&S.2.4.1 Introduction

In addition to those mandates for Information Modeling, Metadata, and Information Exchange Standards described in Section 2.4 of the JTA, the following mandates are applicable to the Modeling and Simulation Domain.

M&S.2.4.2 Mandates

M&S.2.4.2.1 Federation Execution Details Data Interchange Format (FED DIF)

This DIF is the input/output vehicle for sharing HLA initialization data. It contains data from the Federation Object Model as well as additional initialization data needed by the HLA Runtime Infrastructure (RTI) and other HLA initialization tools. The content of the FED DIF is compliant with the HLA Interface Specification referenced above.

- Federation Execution Details Data Interchange Format, Version 1.3, February 1998.

M&S.2.4.2.2 Object Model Template Data Interchange Format

A data interchange format has been adopted as an input/output vehicle for sharing HLA object models presented in the standard Object Model Template (OMT) among object model developers and users.

- Object Model Template Data Interchange Format (OMT DIF), Version 1.3, February 1998.

M&S.2.4.2.3 Standard Simulator Database Interchange Format (SIF)

A DoD data exchange standard (MIL-STD-1821) has been adopted as an input/output vehicle for sharing externally created visual terrain simulator databases among the operational system training and mission rehearsal communities.

- MIL-STD-1821, Standard Simulator Data Base (SSDB) Interchange Format (SIF) Design Standard, 17 June 1993, with Notice of Change 1, 17 April 1994, and Notice of Change 2, 17 February 1996.

M&S.2.4.3 Emerging Standards

M&S.2.4.3.1 Synthetic Environment Data Representation and Interchange Specification (SEDRIS)

No standard currently exists for comprehensively describing and interchanging environmental data in all domains (terrain, ocean, atmosphere, and space) among M&S applications supporting the broad range of acquisition, analysis, and training requirements. SIF will be replaced by SEDRIS. SEDRIS establishes a uniform and effective interchange specification for the pre-runtime distribution of source data and integrated databases. The specification encompasses a robust data model, data dictionary, and interchange format supported by read and write application program interfaces (APIs), data viewers, a data model browser, and analytical verification and validation data model compliance tools. While designed to meet M&S community requirements, the interchange specification has the potential for also being used for natural environment data in DoD operational systems.

M&S.2.4.3.2 Object Model Data Dictionary

The Object Model Data Dictionary is being developed to support the development and reuse of Federation Object Models (FOMs) and Simulation Object Models (SOMs). This will greatly reduce the time needed to develop new HLA applications and transition legacy systems to the HLA. Initially, content standards are being developed based on the requirements of several programs, which are early adopters of the HLA standards. The early adopter programs cover a broad range of simulation applications from engineering to analysis and multiple levels of aggregation from platform-level (previously addressed by the IEEE 1278.1 Protocol Data Unit standards) to aggregate unit simulations (previously addressed by the Aggregate Level Simulation Protocol). The object model requirements of these programs are being consolidated into a common set of data elements, specifying both semantics and syntax. Where existing DoD standards do not exist, they will be developed through the HLA Object Model Data Dictionary process.

M&S.2.5 HUMAN-COMPUTER INTERFACE STANDARDS

There are no additional Human-Computer Interface standards applicable to modeling and simulation beyond those specified in Section 2.5 of the JTA.

M&S.2.6 INFORMATION SYSTEMS SECURITY STANDARDS

There are no additional Information Systems Security standards applicable to modeling and simulation beyond those specified in Section 2.6 of the JTA.

M&S.3 DOMAIN SPECIFIC SERVICE AREAS

There are no domain specific service areas for the Modeling and Simulation Domain.

WEAPON SYSTEMS DOMAIN ANNEX

WS.1 DOMAIN OVERVIEW

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

WS.1.1 PURPOSE

This annex identifies standards for the Weapon Systems domain to include information standards and analogous standards applicable to weapon systems.

WS.1.2 BACKGROUND

This Domain Annex 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 Annex consists of three sections including: Domain Overview, Mandates, and Emerging Standards.

Weapon Systems mandates 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 JTA for which no additions have been mandated in the Weapon Systems Domain Annex or by one or more Subdomain Annexes. However, due to their hard real-time and embedded system requirements, the Weapon Systems subdomains are evaluating the available real-time standards for possible mandate as additions to each section of the JTA, where appropriate.

WS.1.3 DOMAIN DESCRIPTION

Weapon Systems have special attributes (examples: timeliness, embedded nature, space and weight limitation), adverse environmental conditions, and critical requirements (e.g., survivability, low power/weight, and dependable hard real-time processing) that drive system architectures and make system hardware and software highly interdependent and interrelated. The position of the Weapons Systems domain in the Notional JTA Hierarchy is shown in Figure WS-1.

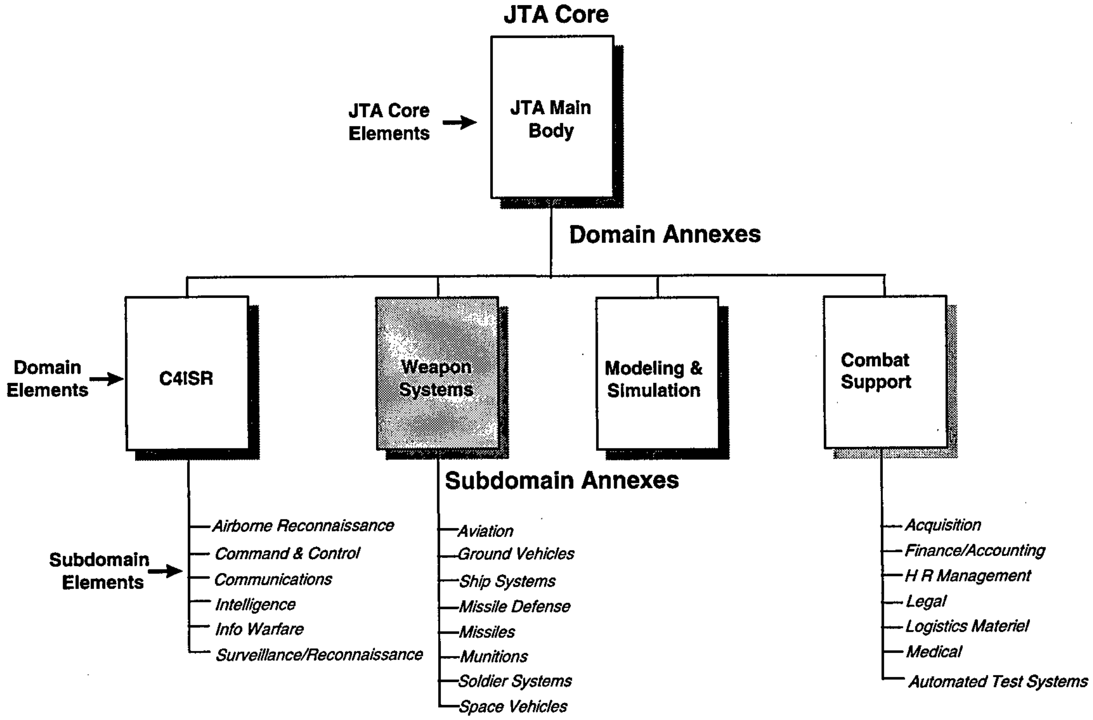


Figure WS-1 Notional JTA Hierarchy

WS.1.4 SCOPE AND APPLICABILITY

A domain is defined as a distinct functional area that can be supported by a family of systems with similar requirements and capabilities. The Weapon Systems Domain Annex, 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 (Joint Pub 1-02). The Weapon Systems domain encompasses a subset of the JTA, and the specific supporting standards profile. For the purposes of the JTA, the Weapons System Domain is that domain whose systems' primary function is that of supporting attack and/or defense against an adversary, and that are intentionally designed to interoperate with other weapons systems and/or with systems external to the Weapon Systems domain.

The Weapon Systems Domain annex is applicable to all weapons systems as defined in Joint Pub 1-02.

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 Weapons System Domain is based upon the Domain participants' agreement to include or exclude a candidate. It is important to note that some weapons systems incorporate features/functions associated with more than one subdomain and therefore must consider the applicable standards from the pertinent subdomains. The current weapon systems subdomains are:

Ground Vehicle subdomain
Includes all DoD weapons systems on moving ground platforms, except missiles, both wheeled and tracked, manned and unmanned.

Aviation subdomain
Includes all DoD weapons systems on aeronautical platforms, except missiles, both manned and unmanned, fixed wing and rotorcraft.

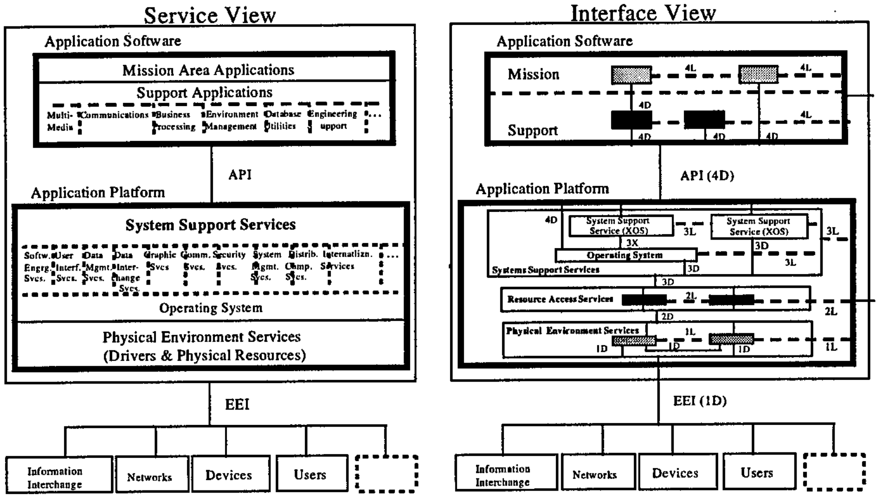
Missile Defense subdomain
Includes any system or subsystem (including associated BM/C4I systems) with a mission to detect, classify, identify, intercept, and destroy or negate the effectiveness of enemy aircraft or missiles before launch or while in flight so as to protect US and coalition forces, people, and geopolitical assets.

WS.1.5 TECHNICAL REFERENCE MODEL

WS.1.5.1 DoD TRM Views

The Weapon Systems domain and subdomains use both the DoD TRM Service View and the Interface View, as described in Section 2. The Interface View is more applicable to real-time systems. Services are best described by the DoD 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 WS-2 depicts the DoD TRM Service View and Interface View. The Interface View is based on the GOA framework. Both views were developed using the POSIX model as a baseline. The POSIX Applications Software Layer is analogous to the Application Software Interface View, while the Service View extends the POSIX model by categorizing Application Software into mission area applications and several support application areas.



Integrated DoD Technical Reference Model

Figure WS-2 DOD TRM Service View and Interface View

The Interface View expanded the Application Platform entity within the POSIX model to include the three other layers: Systems Support Services, Resource Access Services, and Physical Environment Services. The Interface View includes the 4L, 3L, and 2L, for peer-to-peer logical interfaces, and the 3X, 3D, and 2D direct interfaces. The Application Programmers Interface (API) is synonymous with the 4D interface. The External Environment Interface (EEI) is synonymous with the 1L and 1D interfaces treated as a pair. Thus the Interface View extends the Service View by including language describing application-to-application logical interfaces, expanding the Application Platform, and by including language to discuss Application Platform-to-Application Platform logical interface (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 run-time and pre-run-time services. The Service View addresses only 4D API interfaces and 1D/1L EEI interfaces. The Service View does not address 2L, 3L, or 4L peer-to-peer logical interfaces, 3X, 3D, or 2D direct interfaces, nor does it address Resource Access Services.

The Interface View contains two types of interfaces: logical and direct. A logical interface defines requirements for peer-to-peer interchange of data. It identifies senders, receivers, data types, frequency of exchange, and formats. A direct interface identifies the characteristics of the information transfer medium. Simply stated, logical interfaces define what information is transferred, the direct interfaces define how the information is transferred. Logical interfaces are implemented with direct interfaces.

Section WS.2 uses the Service View and identifies additions to the JTA core standards. WS.2 also includes emerging standards representing current standards work within the Weapon Systems domain.
The DoD TRM Interface View is based on the SAE GOA framework, and provides a framework to identify interface classes for applying open system interface standards to the design of hardware/software systems. As a result, the following architecture standard is used to define the interfaces:

- SAE AS 4893. Generic Open Architecture (GOA) Framework, 1 January 1996.

WS.1.5.1.1 Performance Environment

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

WS.1.5.1.2 Application Hardware Environment

Within weapon systems, embedded computing hardware and software components are highly interdependent in order to satisfy very demanding requirements. The DoD TRM Service View often does not fit a general purpose computing model very well. Therefore the DoD TRM Interface View is used to capture such features as interconnect and open systems hardware standards.

WS.1.5.2 Hierarchy of TRM Views

In order to capture the diversity found in weapon subsystem design, a hierarchical approach to TRM Views is being established. From the DoD TRM Service View in Figure WS-2, the DoD TRM Interface View in Figure 2.1-2 will extend downward into the Weapon Systems domain and subdomains to provide the basis for standards identification and traceability.

WS.1.6 ANNEX ORGANIZATION

This annex is divided into three sections: the Overview in Section WS.1, the Additions to the JTA Core Service Areas in Section WS.2, and the Domain Specific Services in Section WS.3. Section WS.2 follows the JTA Section 2 service area structure. The structure of Section WS.3 will evolve as WS-specific service areas are identified and a common structure is coordinated amongst the other annexes.

WS.2 ADDITIONS TO THE JTA CORE

WS.2.1 INTRODUCTION

The DoD TRM Interface View provides for sufficient fidelity to identify critical functions, interfaces, and technical issues.

WS.2.2 INFORMATION PROCESSING STANDARDS

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

WS.2.2.1 Mandate Additions

There are no additions mandated for the Information Processing Standards section.

WS.2.2.2 Emerging Standards

WS.2.2.2.1 Emerging General Standards

There are no emerging general standards for the Information Processing Standards section.

WS.2.2.2.2 Emerging Service Area Standards

WS.2.2.2.2.1 Operating System Services

The OSJTF is sponsoring and synchronizing Weapon Systems domain involvement in the IEEE POSIX working groups. Many POSIX standards are at various stages of standardization and are expected to be revised shortly to accommodate real-time systems' requirements and to provide for test methods. The following standards are emerging:

- IEEE P1003.5c/D3 POSIX-Part 1: Binding for API - Amendment 2: Protocol Independent Interfaces, October 1997.
- IEEE P1003.5f POSIX: Ada binding to 1003.21, January 1997.
- IEEE P1003.1e/D15 POSIX: Protection Audit And Control Interface (C Language), December 1995.
- IEEE P1003.22/D6. POSIX-Open System Security Framework, August 95.

WS.2.2.2.2.2 Real-time Common Object Request Broker Architecture (CORBA)

Real-time Common Object Request Broker Architecture (CORBA) - The OMG Special Interest Group is evaluating the need for real-time object oriented standards and products to support real-time embedded systems. As more information becomes available from this group the Weapon Systems domain will consider adopting the standards as additions to the JTA information processing standards.

WS.2.3 INFORMATION TRANSFER STANDARDS

There are no additions mandated for the Information Transfer Standards section.

WS.2.4 INFORMATION MODELING, METADATA, AND INFORMATION EXCHANGE STANDARDS

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

Real-time, embedded processing systems must be developed within a development support environment for an entire system. As such, they must integrate into a systems engineering process that culminates in prototype or production weapon systems that meet specific functional and performance requirements.

WS.2.4.1 Emerging Standards

The following emerging standard is being considered for mandate by the Weapon Systems domain as an addition to the JTA information modeling standards:

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

Additional emerging standards are:

- IEEE 1076.2: VHDL Mathematical Package, 1996.
- IEEE 1076.3: Standard VHDL Synthesis Packages, 1997.
- IEEE 1076.4: VITAL Application-Specific Integrated Circuit (ASIC) Modeling Specification, 1995. (Provides VITAL timing and primitives).

WS.2.5 HUMAN-COMPUTER INTERFACE STANDARDS

This section provides a common framework for Human-Computer Interfaces (HCI) design and implementation in weapon systems. It complements and extends the DoD HCI Style Guide, Version 2.0, 10 October, 1997. 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 HCI's that can be common across the Weapon Systems domain, while others are subdomain specific. Hence, an HCI style guide is required at the weapon systems level, and currently for each subdomain.

WS.2.5.1 Additions

There are no additional mandates for the Human-Computer Interface Standards section.

WS.2.5.2 Emerging Standards

The Weapon Systems Human-Computer Interface (WSHCI) Style Guide addresses guidelines that are 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 army document is proposed as the starting point to become the joint weapons system style guide:

- U.S. Army Weapon Systems Human-Computer Interface (WSHCI) Style Guide, Version 1.0, 30 September 1996.

WS.2.6 INFORMATION SYSTEMS SECURITY STANDARDS

There are no additions mandated for the Information Systems Security Standards section.

WS.3 DOMAIN SPECIFIC SERVICE AREAS

WS.3.1 APPLICATION SYSTEMS HARDWARE STANDARDS

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

Real-time embedded processing systems must control, sense, and integrate with an application hardware environment. The application hardware is generally a custom built electronic or mechanical module. The application hardware along with the processing system and application software must work together to perform unique mission requirements. The level of coupling of the processing system to the application hardware environment determines the possibility of modular partitioning.

WS.3.1.1 Additions

There are no additional standards mandated for the Application Hardware section.

WS.3.1.2 Emerging Standards

There are no emerging standards in this section.

WS.3.2 EMERGING EMBEDDED COMPUTING STANDARDS

There are no emerging embedded computing standards in this version of the Weapon Systems Annex.

AVIATION SUBDOMAIN ANNEX FOR THE WEAPON SYSTEMS DOMAIN

WS.AV.1 SUBDOMAIN OVERVIEW

A weapon system is a combination of one or more weapons with all related equipment, materials, services, personnel and means of delivery and deployment (if applicable) required for self sufficiency.

Systems covered within the Aviation subdomain include all DoD weapon systems on aeronautical platforms, except missiles, both manned and unmanned, fixed wing and rotorcraft.

This subdomain has been designated as an “emerging subdomain” for JTA 2.0; all standards in this subdomain are designated as emerging and are not mandated by JTA 2.0.

WS.AV.1.1 PURPOSE

This annex identifies standards for the Aviation subdomain of the Weapon Systems domain to include information standards and analogous standards applicable to Aviation systems.

WS.AV.1.2 BACKGROUND

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

WS.AV.1.3 SUBDOMAIN DESCRIPTION

The subdomain description is given in Section WS.AV.1.

WS.AV.1.4 SCOPE AND APPLICABILITY

This subdomain annex does not include any mandates at this time. Emerging standards are identified. Mandates are expected to be added in the next version of the JTA. Some proposed standards are identified.

WS.AV.1.5 TECHNICAL REFERENCE MODEL

The technical reference model adopted for use in this subdomain is the DoD TRM which is described in the Weapon Systems Domain Annex. The DoD TRM Service View and Interface View are used as applicable.

WS.AV.1.6 ANNEX ORGANIZATION

This annex is divided into three sections: the Overview in Section WS.AV.1, the additions to the JTA core standards in Section WS.AV.2, and the Subdomain Specific Services in Section WS.AV.3. Section WS.AV.2 follows the JTA Section 2 service area structure. The structure of Section WS.AV.3 will evolve as aviation-specific service areas are identified and a common structure is coordinated amongst the other annexes.

WS.AV.2 ADDITIONS TO THE JTA CORE

WS.AV.2.1 INTRODUCTION

This section identifies the standards for the Aviation Subdomain that are additional to standards in the JTA core.

WS.AV.2.2 INFORMATION PROCESSING STANDARDS

WS.AV.2.2.1 Additions

There are no additions mandated for the Information Processing Standards section.

WS.AV.2.2.2 Emerging Standards

WS.AV.2.2.2.1 Emerging Service Area Standards

WS.AV.2.2.2.1.1 Operating System Services

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

- SAE xxx: Operating System API for Ada Run Time System.

WS.AV.2.3 INFORMATION TRANSFER STANDARDS

There are no additions or emerging standards for the Information Transfer Standards section.

WS.AV.2.4 INFORMATION MODELING, METADATA, AND INFORMATION EXCHANGE STANDARDS

There are no additions or emerging standards for the JTA Information Modeling, Metadata, and Information Exchange Standards section.

WS.AV.2.5 HUMAN-COMPUTER INTERFACE STANDARDS

WS.AV.2.5.1 Additions

WS.AV.2.5.1.1 Symbology

There are no mandated standards for the Human-Computer Interface Standards section.

WS.AV.2.5.2 Emerging Standards

The following standard is not mandated in this version of the JTA, but is proposed for the next version of the JTA:

- MIL-STD-1787, Aircraft Display Symbology.

WS.AV.2.6 INFORMATION SYSTEMS SECURITY STANDARDS

There are no additions or emerging standards for the Information Systems Security Standards section.

WS.AV.3 SUBDOMAIN SPECIFIC SERVICE AREAS

WS.AV.3.1 APPLICATION SYSTEMS HARDWARE STANDARDS

WS.AV.3.1.1 Additions

WS.AV.3.1.1.1 Hardware Interface Standards

There are no mandated standards for the Hardware Interface Standards section.

WS.AV.3.1.1.1.1 Bus Interface Standards

There are no mandated standards for the Bus Interface Standards section.

WS.AV.3.1.1.1.2 General Hardware Interface Standards

There are no mandated standards for General Hardware Interface.

WS.AV.3.1.2 Emerging Standards

The following Bus Interface standards are not mandated in this version of the JTA but are proposed for the next version of the JTA:

- MIL-STD-1553B, Standard for Medium Speed System Network Bus, 21 September 1978, with Notice of Change 1, 12 February 1980, Notice of Change 2, 8 September 1986, Notice of Change 3, 31 January 1993, and Notice of Change 4, 15 January 1996.
- ANSI/VITA 1, VME64 Specification, 1994.
- MIL-STD-1773, Fiber Optics Mechanization of an Aircraft Internal Time Division Command/Response Multiplex Data Bus, 20 May 1988 with Notice of Change 1, 2 October 1989.

The following General Hardware standard is not mandated in this version of the JTA but is proposed for the next version of the JTA:

- MIL-STD-1389D, Design Requirements for Standard Electronic Module (SME), 30 March 1989.

GROUND VEHICLE SUBDOMAIN ANNEX FOR THE WEAPON SYSTEMS DOMAIN

WS.GV.1 SUBDOMAIN OVERVIEW

A weapon system is a combination of one or more weapons with all related equipment, materials, services, personnel and means of delivery and deployment (if applicable) required for self-sufficiency.

Systems covered within the Ground Vehicle subdomain include all DoD weapon systems on moving ground platforms, except missiles, both wheeled and tracked, manned and unmanned.

WS.GV.1.1 PURPOSE

This annex identifies standards for the Ground Vehicle subdomain of the Weapon Systems domain to include information standards and analogous standards applicable to Ground Vehicle systems.

WS.GV.1.2 BACKGROUND

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

WS.GV.1.3 SUBDOMAIN DESCRIPTION

The subdomain description is given in Section WS.GV.1.

WS.GV.1.4 SCOPE AND APPLICABILITY

The scope of this Subdomain Annex is the entire Ground Vehicle subdomain as defined in Section WS.GV.1.

WS.GV.1.5 TECHNICAL REFERENCE MODEL

The technical reference model used in this subdomain is the DoD TRM which is described in the Weapon Systems Domain Annex. The DoD TRM Service View and Interface View are used as applicable.

WS.GV.1.6 ANNEX ORGANIZATION

This annex is divided into three sections: the Overview in Section WS.GV.1, the additions to the JTA core standards in Section WS.GV.2, and the Subdomain Specific Services in Section WS.GV.3. Section WS.GV.2 follows the JTA Section 2 service area structure. The structure of Section WS.GV.3 will evolve as ground vehicle-specific service areas are identified and a common structure is coordinated among the other annexes.

WS.GV.2 ADDITIONS TO THE JTA CORE

WS.GV.2.1 INTRODUCTION

This section identifies standards for the Ground Vehicles subdomain additional to the standards in the JTA core.

WS.GV.2.2 INFORMATION PROCESSING STANDARDS

There are no additions or emerging standards for the Information Processing Standards section.

WS.GV.2.3 INFORMATION TRANSFER STANDARDS

There are no additions or emerging standards for this section.

WS.GV.2.4 INFORMATION MODELING, METADATA, AND INFORMATION EXCHANGE STANDARDS

There are no additions or emerging standards for this section.

WS.GV.2.5 HUMAN-COMPUTER INTERFACE STANDARDS

There are no additions or emerging standards for this section.

WS.GV.2.6 INFORMATION SYSTEMS SECURITY STANDARDS

There are no additions or emerging standards for this section.

WS.GV.3 SUBDOMAIN SPECIFIC SERVICE AREAS

WS.GV.3.1 APPLICATION SYSTEMS HARDWARE STANDARDS

WS.GV.3.1.1 Additions

WS.GV.3.1.1.1 Hardware Interface Standards

WS.GV.3.1.1.1.1 Bus Interface Standards

- MIL-STD-1553B, Standard for Medium Speed System Network Bus, 21 September 1978, with Notice of Change 1, 12 February 1980, Notice of Change 2, 8 September 1986, Notice of Change 3, 31 January 1993, and Notice of Change 4, 15 January 1996.
- ANSI/VITA 1, VME64 Specification, 1994.
- SAE J 1850, Class B Data Communication Network Interface, 1 July 1995.
- ANSI X3.131, Information Systems - Small Computer Systems Interface - 2 (SCSI-2), 1994.

WS.GV.3.1.1.1.2 General Hardware Interface Standards

- Personal Computer Memory Card International Association (PCMCIA), PC Card Standard, March 1997.
- IEEE 1101.2, Standard for Mechanical Core Specifications for Conduction-Cooled Eurocards (ANSI), 1992.
- EIA 170, Electrical Performance Standards - Monochrome Television Studio Facilities, November 1957.
- EIA 330, Electrical Performance Standards for Closed Circuit Television Camera 525/60 Interlaced 2:1 (ANSI/EIA 330-68), November 1966.
- EIA 343-A, Electrical Performance Standard for High Resolution Monochrome Closed Circuit Television Camera (November 1966), September 1969.
- SMPTE 170M, Television - Composite Analog Video Signal - NTSC for Studio Applications, 1994.

WS.GV.3.1.2 Emerging Standards

– PCI Industrial Computer Manufacturer's Group (PICMG): Compact PCI Specification, R2.1, September 1997.

This page intentionally left blank.

MISSILE DEFENSE SUBDOMAIN ANNEX FOR THE WEAPON SYSTEMS DOMAIN

WS.MD.1 SUBDOMAIN OVERVIEW

A weapon system is a combination of one or more weapons with all related equipment, materials, services, personnel and means of delivery and deployment (if applicable) required for self-sufficiency.

Systems covered within the Missile Defense subdomain include any system or subsystem (including associated BM/C4I systems) with a mission to detect, classify, identify, intercept, and destroy or negate the effectiveness of enemy missiles before launch or while in flight so as to protect US and coalition forces, people, and geopolitical assets.

This subdomain has been designated as an "emerging subdomain" for JTA 2.0; all standards in this subdomain are designated as emerging and are not mandated by JTA 2.0.

WS.MD.1.1 PURPOSE

This JTA Subdomain Annex identifies standards for missile defense systems. This version is focused solely on active ballistic missile defense, with the intent of expanding this annex in the future.

WS.MD.1.2 BACKGROUND

The following documents provide useful background information regarding missile defense (sorted by title), with particular emphasis on ballistic missile defense:

1. Ballistic Missile Defense (BMD) Command, Control, and Communications (C3) Operational Requirements Document (ORD), Air Force Space Command, working draft, 19 May 1997, Secret (US. Only).
2. Battle Management Concept for Joint Theater Air and Missile Defense Operations, Joint Theater Air and Missile Defense Organization (JTAMDO), final draft, 11 September 1997. This document is downloadable from the following World Wide Web address:
   http://199.114.114.8/~dj9snops/samd_files_for_download

3. Capstone Theater Missile Defense (TMD) Cost and Operational Effectiveness Analysis (COEA), BMDO, 1996.
4. Doctrine for Joint Theater Missile Defense. Joint Pub 3-01.5. February 22, 1996.
5. FY96 Analysis Of The Ballistic Missile Defense Interoperability Standards, Fife et al., IDA-P-3277, Alexandria, VA: Institute For Defense Analyses.
6. JTAMD Mission Area Assessment, DoD J8, draft, October 30, 1997, Secret. (Note that this document combines the capstone TMD COEA, TAD, and information on land attack cruise missiles).
7. National Ballistic Missile Defense (NBMD) Capstone Requirements Document (CRD), U.S. Space Command, August 24, 1996, Secret (Release Can-US).
8. NMD Capability 2 System Requirements Document, TRW Inc., April 4, 1997, BMC3 SE&I, Rosslyn, VA: TRW.
9. Operational Requirements Document (ORD) for National Ballistic Missile Defense (NBMD), US Army Space and Strategic Defense Command, March 10, 1997, Secret.
10. Theater Air and Missile Defense Architecture for Joint Force Operations, Bean et al., June 1997, MP 97W 105.
11. Theater Air and Missile Defense Master Plan, September 1997, JTAMDO. POET control number MCNEIL 000396/97.
12. Theater Ballistic Missile Defense (TBMD) Capstone Requirements Document (CRD), U.S. Space Command, draft, August 7, 1997, Secret.
13. Theater Missile Defense (TMD) Command and Control (C2) Plan, August 1996.

WS.MD.1.3 SUBDOMAIN DESCRIPTION

For a description of this subdomain, see the background material in Section WS.MD.1.2.

WS.MD.1.4 SCOPE AND APPLICABILITY

The scope of this Subdomain Annex is the entire domain of missile defense (as defined in the overview above). However, the standards listed within this version of the annex solely address support for active defense against theater and strategic ballistic missiles (BMs) in flight, as a first step in evolving a comprehensive and complete set of standards for all missile defense systems. It is acknowledged that this evolution will require interaction with many communities to resolve standardization issues.

WS.MD.1.5 TECHNICAL REFERENCE MODEL

Missile defense systems typically include one or more sensors, one or more weapons systems, and a communication infrastructure all coordinated by a BMC3 system (which also coordinates with external systems). Kinetic missile defense systems have a weapon system including one or more launchers with one or more interceptors. Sensors, launchers, interceptors, and other weapon systems include information technology (IT) components and other components. At this time no single document or view has been officially designated as the missile defense technical reference model. No reference models have yet been developed for the non-IT parts of these systems.

WS.MD.1.6 ANNEX ORGANIZATION

This annex is divided into three sections: the Overview in Section WS.MD.1, the missile defense mandates and emerging standards additional to those in the JTA core in Section WS.MD.2, and the Subdomain Specific Services in Section WS.MD.3. Section WS.MD.2 follows the JTA Section 2 service area structure. The structure of Section WS.MD.3 will evolve as missile defense-specific service areas are identified and a common structure is coordinated amongst the other annexes.

WS.MD.2 ADDITIONS TO THE JTA CORE

WS.MD.2.1 INTRODUCTION

This section identifies standards for the Missile Defense Subdomain that are additional to standards in the JTA core.

WS.MD.2.2 INFORMATION PROCESSING STANDARDS

WS.MD.2.2.1 Mandates

There are no mandates in this section.

WS.MD.2.2.2 Emerging Standards

WS.MD.2.2.2.1 Navigation Standard

The following standard may be mandated by the JTA for ballistic missile defense systems to ensure that navigation-related data (e.g. position, velocity, and time) can be shared and properly used between missile defense systems. Note that this standard is consistent with and extends the mandates in the JTA core (e.g., WGS-84):

- BMD-P-SD-92-000002-A, *Ballistic Missile Defense (BMD) Navigation Standard*, 23 June 1993, Ballistic Missile Defense Organization.

WS.MD.2.3 INFORMATION TRANSFER STANDARDS

There are no mandates or emerging standards for this section.

WS.MD.2.4 INFORMATION MODELING, METADATA, AND INFORMATION EXCHANGE STANDARDS

WS.MD.2.4.1 Mandates

There are no mandates in this section.

WS.MD.2.4.2 Emerging Standards

It is anticipated that future versions of the JTA may mandate that missile defense systems which are identified as part of the "Theater Missile Defense" system shall support MIL-STD-6016 (TADIL-J/link-16) as a mobile interoperable communication link.

It is also anticipated that future versions of the JTA may mandate that those missile defense systems which support MIL-STD-6016 shall also support the following additional standard, which adds a message type and conventions necessary to support ballistic missile defense:

- *Interface Change Proposal (ICP) TJ93-096 Ch9*, commonly called the "Space Track Message," Ballistic Missile Defense Organization, 26 September 1997.

Note that there are ongoing efforts to include ICP TJ93-096 (listed above) as part of MIL-STD-6016.

Efforts are ongoing to merge the data element definitions (DEDs) developed for Theater Missile Defense (TMD), National Missile Defense (NMD), and the Joint Theater and Air Missile Defense Organization (JTAMDO).

The NMD program is in the process of selecting communication mechanisms. An IPT formed to study the issue has recommended that NMD use a VMF-based message set.

BMDO has formed the "Time and Geospatial Working Group" (TGWG) to identify additional time and geospatial issues and to develop cross-system resolutions of those issues.

WS.MD.2.5 HUMAN-COMPUTER INTERFACE STANDARDS

There are no mandates or emerging standards for this section.

WS.MD.2.6 INFORMATION SYSTEMS SECURITY STANDARDS

There are no mandates or emerging standards for this section.

WS.MD.3 SUBDOMAIN SPECIFIC SERVICE AREAS

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

APPENDIX A: ACRONYMS AND GLOSSARY

A.1 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 acronym "Mbps" is used in the titles of some standards.

AAC	Advance Audio Coding
AAL	ATM Adaptation Layer
ABBET	A Broad Based Environment for Test
ABOR	Abort
ACC	Architecture Coordination Council
ACP	Allied Communication Publication
ACR-NEMA	American College of Radiology - National Electrical Manufacturers Association
ACTD	Advanced Concept Technology Demonstration
ADE	Application Development Environment
AES	Application Environment Specification
AES3	Audio Engineering Society 3
AF	ATM Forum
AFMSS	Air Force Mission Support System
AFP	Adapter Function and Parametric Data Interface
AH	Authentication Header
AITI	Automated Interchange of Technical Information
ALE	Automated Link Establishment
ALSP	Aggregate Level Simulation Protocol
ANSI	American National Standards Institute
AOR	Area of Responsibility
API	Application Program Interface
AR	Airborne Reconnaissance
ARI	ATS Research and Development Integrated Product Team
ARITA	Airborne Reconnaissance Information Technical Architecture
ARL	Airborne Reconnaissance Low
ARP	Address Resolution Protocol
ARTAWG	Airborne Reconnaissance Technical Architecture Working Group
ASAS	All-Source Analysis System
ASD	Assistant Secretary of Defense
ASD C3I	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ATA	Army Technical Architecture
ATARS	Advanced Tactical Air Reconnaissance System
ATD	Advanced Technology Demonstration
ATE	Automated Test Equipment
ATIS	Alliance for Telecommunication Industry Solutions
ATLAS	Abbreviated Test Language for All Systems
ATM	Asynchronous Transfer Mode
ATPG	Automatic Test Program Generator
ATS	Automatic Test Systems
ATV	Advanced Television Systems
AUTODIN	Automatic Digital Network
AV	Air Vehicle

AVI	Audio-Video Interleaved
AWE	Avionics/Weapons/Electronics

BCD	Binary Coded Decimal
BER	Bit Error Rate
BGP	Border Gateway Protocol
BIPM	Bureau International des Poids et Mesures
bits/s	Bits per second
BMDO	Ballistic Missile Defense Organization
BOOTP	Bootstrap Protocol
bps	Bits Per Second
BRI	Basic Rate Interface
BUFR	Binary Universal Format for Representation

C/S/A	CINCs/Services/Agencies
C2	Command and Control
C2CDM	Command and Control Core Data Model
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAC	Computer Asset Controller
CADRG	Compressed Arc Digitized Raster Graphics
CAE	Common Application Environment
CALS	Continuous Acquisition and Life Cycle Support
CARS	Contingency Airborne Reconnaissance System
CASE	Computer Automated Software Engineering
CBC	Cipher Block Chaining
CBR	Constant Bit Rate
CBS	Commission for Basic Systems
CBW	Chemical and Biological Weapons
CC	Common Criteria for Information Technology Security Evaluation
CCB	Change Control Board
CCITT	International Telegraph & Telephone Consultative Committee (now ITU)
CDE	Common Desktop Environment
CDENext	Next Version of CDE
CDL	Common Data Link
CDMA	Code Division Multiple Access
CD-ROM	Compact Disk-Read Only Memory
CFCSE	Center For Computer Systems Engineering
CFS	Center for Standards
CG	Commanding General
CGI	Computer Graphics Interface
CGM	Computer Graphics Metafile
CI	Critical Interface
CIB	Controlled Image Base
CIDE	Communication Information Data Exchange
CIGSS	Common Imagery Ground/Surface System
CINC	Commander In Chief
CIPSO	Common Internet Protocol Security Options
CIS	Combat Information System
CISA	C4I Integration Support Activity
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Memorandum

CLI	Call Level Interface
CM	Configuration Management
CMA	Collection Management Authority
CMIP	Common Management Information Protocol
CMMS	Conceptual Models of the Mission Space
CMST	Collection Management Support Tools
CNR	Combat Net Radio
COE	Common Operating Environment
COM	Common Object Model
CONUS	Continental United States
CORBA	Common Object Request Broker Architecture
COSE	Common Open Software Environment
COTS	Commercial Off-the-Shelf
CRM	Computer Resources Management
CRMA	Collection Requirement Management Application
CRMS	Collection Requirement Management System
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
CSP	Common Security Protocol
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
CTRS	Conventional Terrestrial Reference System
CXE	Computer to External Environments Interface
DAA	Designated Approving Authority
DAMA	Demand Assigned Multiple Access
DAP	Directory Access Protocol
DARO	Defense Airborne Reconnaissance Office
DARP	Defense Airborne Reconnaissance Program
DARSC	Defense Airborne Reconnaissance Steering Committee
DAT	Digital Audio Tape
DBDB	Digital Bathymetric Database
DBMS	Data Base Management System
DCA	Defense Communications Agency (now DISA)
DCAC	Defense Communications Agency (now DISA) Circular
DCE	Distributed Computing Environment
DCGS	Distributed Common Ground System
DCOM	Distributed Component Object Mode
DCRSi	Digital Cassette Recording System - Improved
DDDS	Defense Data Dictionary System
DDM	DoD Data Model
DDNS	Dynamic Domain Name System
DDRS	Defense Data Repository System
DEF	Data Exchange Format
DFC	Diagnostic Flow Charts
DGSA	DoD Goal Security Architecture
DHCP	Dynamic Host Configuration Protocol
DIA	Defense Intelligence Agency
DIA	Diagnostic processing interface protocol (ATS Sub-domain)
DIGEST	Digital Geographic Information Exchange Standard
DII	Defense Information Infrastructure
DIS	Distributed Interactive Simulation
DIS	Draft International Standard
DISA	Defense Information Systems Agency (formerly Defense Communication Agency (DCA))
DISN	Defense Information System Network
DLA	Defense Logistics Agency

DLWG	Data Link Working Group
DMS	Defense Message System
DMSO	Defense Modeling and Simulation Office
DMTD	Digital Message Transfer Device
DNC	Digital Nautical Chart
DNS	Domain Name System
DoD	Department of Defense
DoDD	DoD Directive
DoDIIS	DoD Intelligence Information Systems
DoDISS	DoD Index of Specifications and Standards
DoDSSP	DoD Single Stock Point
DOI	Domain Of Interpretation
DPPDB	Digital Point Positioning Data Base
DRV	Instrument Driver Application Programming Interface
DSIC	Defense Standards Improvement Council
DSN	Defense Switched Network
DSP	Defense Standardization Program
DSS1	Digital Subscriber Signaling System No 1
DSSS	Direct Sequence Spread Spectrum
DTED	Digital Terrain Elevation Data
DTF	Digital Test Data Formats
DTOP	Digital Topographic Data
DTSR	Digital Temporary Storage Recorder
DVI	Digital Video Interactive

E/O	Electro-optical
EAO	Executive Agent Office
EEI	External Environment Interface
EHF	Extremely High Frequency
EHF	Extra High Frequency (AR Sub-Domain)
EIA	Electronics Industries Association
E-MAIL	Electronic Mail
ESP	Encapsulating Security Payload
ETRAC	US Army Enhanced Tactical Radar Correlator

F3	Form, Fit, and Function
FAQ	Frequently Asked Question
FDDI	Fiber Distributed Data Interface
FDMA	Frequency Division Multiple Access
FED-STD	Federal Telecommunication Standard
FIPS	Federal Information Processing Standards
FOM	Federation Object Model
FPLMTS	Future Public Land Mobile Telecommunications Systems
FRM	Frameworks Interface
FRM	Functional Requirements Model (AR Sub-domain)
FTP	File Transfer Protocol
FTR	Federal Telecommunications Recommendation

GBS	Global Broadcast Service
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GIC	Generic Instrument Class Interface
GIF	Graphics Interchange Format

GIS	Geographic Information System
GKS	Graphical Kernel System
GOA	Generic Open Architecture
GOTS	Government Off-the-Shelf
GPS	Global Positioning System
GRIB	Gridded Binary
GSD	Global Situation Display
GSM	Global System for Mobile Communications
GSS	Generic Security Service
GUI	Graphical User Interface
HCI	Human-Computer Interface
HDBK	Handbook
HDTV	High Definition Television
HF	High Frequency
HITL	Human-in-the-Loop
HLA	High Level Architecture
HMAC	keyed-Hashing for Message Authentication
HST	Host Computer Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HUMINT	Human Intelligence
HyTime	Hypermedia Time-based Structuring Language
I&RTS	Integration and Runtime Specification
I/O	Input/Output
IAB	Internet Architecture Board
ICB	Instrument Communication Bus Interface
ICCCM	Inter-Client Communications Convention Manual
ICL	Instrument Command Language Interface
ICM	Instrument Communications Manager Interface
ICMP	Internet Control Message Protocol
IDEF0	Integrated Definition for Function Modeling
IDEF1X	Integrated Definition for Information Modeling
IDL	Interface Definition Language
IDUP	Independent Data Unit Protection
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IER	Information Exchange Requirements
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IF	Intermediate Frequency
IFOG	Interferometric Fiber Optic Gyro
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	Interactive Multimedia Association
IMETS	Integrated Meteorological System
IMINT	Imagery Intelligence
INS	Inertial Navigation System
IP	Internet Protocol
IPA	Image Product Archive

IPCP	Internet Protocol Control Protocol
IPDS	Integrated Deployable Processing System
IPL	Image Product Library
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Next Generation Version 6
IR	InfraRed
IRDS	Information Resource Dictionary System
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
ISP	International Standardized Profile
ISP	ISDN Security Program
ISPT	Intelligence Support Processing Tool
ISR	Intelligence, Surveillance & Reconnaissance
ISS	Intelligence Systems Secretariat
ITF	Integrated Task Force
ITSEC	European Information Technology Security Evaluation Criteria
ITSG	Information Technology Standards Guidance
ITU	International Telecommunications Union (formerly called CCITT)
ITU-T	International Telecommunications Union - Telecommunications Standardization Sector

JAMA	Joint Airborne MASINT Architecture
JASA	Joint Airborne SIGINT Architecture
JASASH	JASA Standards Handbook
JBS	Joint Broadcast Service
JCMT	Joint Collection Management Tool
JFIF	JPEG File Interchange Format
JIEO	Joint Interoperability & Engineering Organization
JII	Joint Integration Interface
JPEG	Joint Photographic Expert Group
JROC	Joint Requirements Oversight Council
JSA	Joint Systems Architecture
JTA	Joint Technical Architecture
JTADG	Joint Technical Architecture Development Group
JTAWG	Joint Technical Architecture Working Group
JTDLMP	Joint Tactical Data Link Management Plan
JTIDS	Joint Tactical Information Distribution System
JV	Joint Vision
JVM	Java Virtual Machine
JWICS	Joint Worldwide Intelligence Communications System

Kbits/s	Kilobits per second
kbps	Kilobits Per Second
KCIOC	Korean Combined Operational Intelligence Center
KHz	Kilohertz
KMP	Key Management Protocol

LAN	Local Area Network
LASINT	Laser Intelligence
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol
LD-CELP	Low Delay-Code Excited Linear Prediction
LDR	Low Data Rate
LF	Low Frequency
LOS	Line-of-Sight
LPI	Low Probability of Intercept
LUNI	LANE User Network Interface
LWD	Littoral Warfare Data
LWR	LASINT/Laser Warning Receivers

M&S	Modeling and Simulation
MAGTF	Marine Air Ground Task Force
MAN	Metropolitan-Area Network
MASINT	Measurement and Signature Intelligence
MAU	Medium-Access Unit
Mbits/s	Megabits per second
Mbps	Megabits per second
MC&G	Mapping, Charting and Geodesy
MCCDC	Marine Corps Combat Development Command
MDR	Medium Data Rate
MHP	Mobile Host Protocol
MHz	Megahertz
MIB	Management Information Base
MIDB	Management Information Database
MIDS	Multi-functional Information Distribution System
MIES	US Army Modernized Imagery Exploitation System
MIL-HDBK	Military Handbook
MILSATCOM	Military Satellite Communications
MIL-STD	Military Standard
MIPE	Mobile Intelligence Processing Element
MISSI	Multilevel Information Systems Security Initiative
MLPP	Multi-Level Precedence and Preemption
MMF	Multimedia Formats Interface
MMP	Modular Mission Payloads
MOF	Meta-Object Facility
MOSPF	Multicast Open Shortest Path First
MPCS	Mission Planning and Control Station
MPEG	Motion Pictures Expert Group
MPOA	Multiprotocol over ATM
MSIIRS	Multispectral Imagery Interpretation Scale
MSMP	Modeling and Simulation Master Plan
MSP	Message Security Protocol
MTA	Message Transfer Agent
MTIMSP	Moving Target Indicator Message Security Protocol

NAIC	National Air Intelligence Center
NATO	North Atlantic Treaty Organization
NCSC	National Computer Security Center
NET	Network Protocols Interface
NIIRS	National Imagery Interpretation Rating Scale
NIMA	National Imagery and Mapping Agency

NIPNET	Non-secure IP Routing Network
NIST	National Institute of Standards and Technology
NITF	National Imagery Transmission Format
NITFS	National Imagery Transmission Format Standard
NIUF	North American ISDN User's Forum
NLSP	Network Layer Security Protocol
NRIIRS	National Radar Imagery Interpretation Scale
NRO	National Reconnaissance Office
NSA	National Security Agency
NSM	Network and Systems Management
NTIS	National Technical Information Service
NTP	Network Time Protocol
NTSC	National Television Standards Committee
NTSDS	National Target/Threat Signature Data System

ODBC	Open Database Connectivity
ODMG	Object Data Management Group
OLE	Object Linking and Embedding
OMA	Object Management Architecture
OMG	Object Management Group
OODBMS	Object-Oriented Database Management System
OOM	Object-Oriented Methods
OOT	Object Oriented Technology
OOTW	Operations Other Than War
OS	Operating System
OSD	Office of the Secretary of Defense
OSD A&T	Office of the Secretary of Defense for Acquisition and Technology
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OSJTF	Open Systems Joint Task Force
OSO	Operational Support Office
OSPF	Open Shortest Path First

PASV	Passive
PCAT	PC Access Tool
PCI	Peripheral Computer Interface
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Services
PDF	Portable Document Format
PDU	Protocol Data Units
PHIGS	Programmers Hierarchical Interactive Graphics Systems
PICS	Protocol Implementation Conformance Statement
PINES	Pacific Air Forces Interim National Exploitation System
PM	Program Manager
PNG	Portable Network Graphics
PN-NI	Private Network-Network Interface
POC	Point of Contact
POSIX	Portable Operating System Interface
PPP	Point-to-Point Protocol
PPS	Precise Position Service
PPS	Pulse Per Second (AR Sub-domain)
PRI	Primary Rate Interface
PSK	Phase Shift Keying
PSM	Persistent Stored Modules

PST	Prestructured Technology
PSTN	Public Switched Telephone Networks
QoS	Quality of Service
RDA	Remote Data Access
RDBMS	Relational Database Management System
RF	Radio Frequency
RFC	Request for Comments
RFI	Receiver Fixture Interface Alliance
RFP	Requests for Proposals
RFX	Receiver/Fixture Interface
RMON	Remote Monitoring
RPC	Remote Procedure Call
RPF	Raster Product Format
RTI	Run Time Infrastructure
RTS	Run Time Services Interface
SA	Systems Architecture
SAE	Society of Automotive Engineers
SAMP	Security Association Management Protocol
SAR	Synthetic Aperture Radar
SAR PH	SAR Phase History
SATCOM	Satellite Communications
SCC	Standards Coordinating Committee
SCPS	Space Communications Protocol Standards
SDE	Support Data Extensions
SDF	Simulation Data Format
SDN	Secure Data Network
SDNS	Secure Data Network System
SE	Synthetic Environments
SEDRIS	Synthetic Environment Data Representation and Interchange Specification
SFP	Switch Function and Parametric Data Interface
SGML	Standard Generalized Markup Language
SHF	Super High Frequency
SIDR	Secure Intelligence Data Repository
SIF	Standard Simulator Database Interchange Format
SIGINT	Signal Intelligence
SILS	Standard for Interoperable LAN Security
SIPRNET	Secure IP Routing Network
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMPTE	Society of Motion Picture and Television Engineers
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOM	Simulation Object Model
SONET	Synchronous Optical Network
SOO	Statement Of Objective
SOW	Statements of Work
SQL	Structured Query Language
SSL	Secure Socket Layer
STANAG	Standard NATO Agreement
STD	Standard
STOU	Store Unique

STS	Synchronous Transport Signal
SUS	Single UNIX Specification
SWM	Switch Matrix Interface

TACO2	Tactical Communications Protocol 2
TADIL	Tactical Digital Information Link
TAFIM	Technical Architecture Framework for Information Management
TAMPS	Tactical Aviation Mission Planning System
TASG	Technical Architecture Steering Group
TAWDS	Tactical Automated Weather Distribution System
TCP	Transmission Control Protocol
TCSEC	Trusted Computer Security Evaluation Criteria
TDDS	TRAP Data Dissemination System
TDL	Tactical Data Link
TDMA	Time Division Multiple Access
TEG	Marine Corps' Tactical Exploitation Group
TELNET	Telecommunications Network
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TIBS	Tactical Information Broadcast System
TIDP	Technical Interface Design Plan
TIS	Technical Interface Specification
TMN	Telecommunications Management Network
TOS	Type-of-Service
TOS	Test Program to Operating System Interface (ATS Sub-domain)
TP	Transport Protocol
TP0	Transport Protocol Class 0
TPD	Test Program Documentation Interface
TPI	Test Program Instructions
TPS	Test Program Set
TRAP	Tactical Receive Equipment and Related Applications
TRC	Technical Reference Code
TRD	Test Requirements Document
TRIXS	Tactical Reconnaissance Intelligence Exchange System
TRM	Technical Reference Model
TRMWG	Technical Reference Model Working Group
TSIG	Trusted Systems Interoperability Group
TSIX(RE)	Trusted Security Information Exchange for Restricted Environments
TSR	Test Strategy Report

UAV	Unmanned Aerial Vehicle
UCS	Universal Multiple-Octet Coded Character Set
UDP	User Datagram Protocol
UGS	Unattended Ground Sensors
UHF	Ultra High Frequency
UI	User Interface
UML	Unified Modeling Language
UMS	Unattended MASINT Sensors
UNEST	UNIX-based National Exercise Support Terminal
UNI	User-Network Interface
URL	Uniform Resource Locator
USAF	United States Air Force
USD(A&T)	Under Secretary of Defense for Acquisition and Technology
USIGS	United States Imagery and Geospatial Information System

USIPS	US. Joint Service Image Processing System
USMC	US. Marine Corps
USMTF	United States Message Text Format
USNO	US. Naval Observatory
UTC	Coordinated Universal Time
UTC(USNO)	UTC as maintained at the U.S. Naval Observatory
UTR	Unit Under Test Requirements Interface
UUT	Unit Under Test
UVMap	Urban Vector Map
VHF	Very High Frequency
VHS	Vertical Helical Scan
VISA	Virtual Instrument Standard Architecture
VISP	Video Imagery Standards Profile
VITC	Vertical Interval Time Code
VITD	Vector Product Interim Terrain Data
VLF	Very Low Frequency
VMap	Vector Map
VME	Versa Modulo Europa
VMF	Variable Message Format
VPF	Vector Product Format
VPP	VXI*plug&play*
VRML	Virtual Reality Modeling Language
VSM	Video Systems Matrix
VTC	Video Teleconferencing
VXIVMap AD	VME Extensions for InstrumentationVMap Aeronautical Data
W3C	World Wide Web Consortium
WGS	World Geodetic System
WMO	World Meteorological Organization
WNDP	Worldwide Numbering and Dialing Plan
WVS+	World Vector Shoreline Plus
WWW	World Wide Web
XML	eXtensible Markup Language
Y2K	Year 2000

This page intentionally left blank.

A.2 GLOSSARY

Note:
Where two textual variants of the same term, e.g., "real time" and "real-time" occur in the document, both are shown.

Access Control

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

Accreditation

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

Activity Model (IDEF0)

A graphic description of a system or subject that is developed for a specific purpose and from a selected viewpoint. A set of one or more IDEF0 diagrams that depict the functions of a system or subject area with graphics, text and glossary. (FIPS Pub 183, Integration Definition For Function Modeling (IDEF0), December 1993).

Aggregate Level Simulation Protocol (ALSP)

A family of simulation interface protocols and supporting infrastructure software that permit the integration of distinct simulations and war games. Combined, the interface protocols and software enable large-scale, distributed simulations and war games of different domains to interact at the combat object and event level. The most widely known example of an ALSP confederation is the Joint/Service Training Confederation (CBS, AWSIM, JECEWSI, RESA, MTWS, TACSIM, CSSTSS) that has provided the backbone to many large, distributed, simulation-supported exercises. Other examples of ALSP confederations include confederations of analytical models that have been formed to support U.S. Air Force, U.S. Army, and U.S. TRANSCOM studies. (DoD 5000.59-P, "Modeling and Simulation Master Plan," October 1995, authorized by DoD Directive 5000.59, January 4, 1994).

American National Standards Institute (ANSI)

The principal standards coordination body in the U.S. ANSI is a member of the ISO. (TAFIM, Version 3.0, Volume 4).

Application Platform

1. The collection of hardware and software components that provide the services used by support and mission-specific software applications. (TAFIM, Version 3.0, Volumes 1 and 3)
2. The application platform is defined as the set of resources that support the services on which application software will execute. It provides services at its interfaces that, as much as possible, make the implementation-specific characteristics of the platform transparent to the application software. (TAFIM, Version 3.0, Volume 2).

Application Platform Entity

The application platform is defined as the set of resources that support the services on which application software will execute. It provides services at its interfaces that, as much as possible, make the implementation-specific characteristics of the platform transparent to the application software. (TAFIM, Version 3.0, Volume 2).

Application Program Interface (API)

1. The interface, or set of functions, between the application software and the application platform. (NIST Special Publication 500-230; TAFIM, Version 3.0, Volumes 1 and 3)
2. The means by which an application designer enters and retrieves information. (TAFIM, Version 3.0, Volumes 1 and 3).

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. (TAFIM, Version 3.0, Volume 2).

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 610.12-1900; TAFIM, Version 3.0, Volumes 1 and 3).

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. (OS-JTF).

Authentication

1. To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
2. To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

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.

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. (JP1-02).

Command, Control, Communications, and Computer Systems

Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations. (JP1-02).

Commercial Item

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

2. Any item that evolved from an item described in 1) above through advances in technology or performance that is not yet available in the commercial market, but will be available in time to meet the delivery requirements of the solicitation.
3. Any item that, but for modifications of a type customarily available in the commercial market or minor modifications made to meet DoD requirements, would satisfy the criteria in 1) or 2) above.
4. Any combination of items meeting the requirements of 1, 2, or 3 above or 5 below that are of a type customarily combined and sold in combination to the general public.
5. Installation services, maintenance services, repair services, training services, and other services if such services are procured for support of any item referred to paragraphs 1, 2, 3. or 4 above, if the sources of such services:
   - offers such services to the general public and the DoD simultaneously and under similar terms and conditions and
   - offers to use the same work force for providing the DoD with such services as the source used for providing such services to the general public.
6. Services offered and sold competitively, in substantial quantities, in the commercial marketplace based on established catalog prices of specific tasks performed and under standard commercial terms and conditions.
7. Any item, combination of items or service referred to in 1 through 6 above notwithstanding the fact that the item or service is transferred between or among separate divisions, subsidiaries, or affiliates of a contractor.
8. A nondevelopmental item developed exclusively at private expense and sold in substantial quantities, on a competitive basis, to State and local governments.

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

Commercial off-the-Shelf (COTS)

1. See the definition of Commercial Item found above. (OS-JTF 1995).
2. 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. (TAFIM, Version 3.0, Volumes 1 and 3)

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).

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. (TAFIM, Version 3.0, Volumes 1 and 3).

Coordinated Universal Time (UTC)

Time scale, based on the second (SI), as defined and recommended by the CCIR and maintained by the Bureau International des Poids et Mésures (BIPM).

Data Dictionary

A specialized type of database containing metadata that is managed by a data dictionary system; arepository 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

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

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 AIS or network at an acceptable level of risk. (NSTISSI No. 4009).

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. (2) A synthetic environment within which humans may interact through simulation(s) at multiple sites networked using compliant architecture, modeling, protocols, standards, and data bases. (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.

External Environment Interface (EEI)

The interface that supports information transfer between the application platform and the external environment. (NIST Special Publication 500-230; TAFIM, Version 3.0, Volumes 1 and 3).

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. (HLA Glossary: **http://www.dmso.mil/projects/hla/docslib/hlagloss.html**).

Federation

A named set of interacting federates, a common federation object model, and supporting RTI, that are used as a whole to achieve some specific objective. (HLA Glossary: **http://www.dmso.mil/projects/hla/docslib/hlagloss.html**).

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. (HLA Glossary, http://www.dmso.mil/projects/hla/docslib/hlagloss.html).

Government off-the-Shelf (GOTS)

See COTS.

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.).

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. (HLA Glossary: **http://www.dmso.mil/projects/hla/docslib/hlagloss.html**).

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)

A. 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 which (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.

B. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

C. Notwithstanding subparagraphs (A) and (B), 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.dtic.mil/c3i/cio/references/itmra.Annot.html).

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. (TAFIM, Version 3.0, Volume 4).

Intelligence

1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.
2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (JP1-02).

Interactive Model

A model that requires human participation. Syn: human-in-the-loop. ("A Glossary of Modeling and Simulation Terms for Distributed Interactive Simulation (DIS)," August, 1995).

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 Comitè Consultatif International de Tèlègraphique et Tèlèphonique (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, etc.). The IETF is a subdivision of the Internet Architecture Board (IAB) responsible for the development of protocols, their implementations and standardization.

Interoperability

1. The ability of two or more systems or components to exchange data and use information. (IEEE STD 610.12).
2. The ability of two or more systems to exchange information and to mutually use the information that has been exchanged. (Army Science Board).

Interworking

The exchange of meaningful information between computing elements (semantic integration), as opposed to interoperability, which provides syntactic integration among computing elements..

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.

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. (TAFIM 2.0, vol 1).

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. (TAFIM 2.0, vol 1).

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).

A. Live Simulation. A simulation involving real people operating real systems.

B. 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).

C. 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 computer using sound, graphics, animation, and text; using various input and output devices.

National Institute of Standards and Technology (NIST)

The division of the U.S. Department of Commerce that ensures standardization within Government agencies. NIST was formerly known as the National Bureau of Standards. NIST develops and maintains 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

A. 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.

B. 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.dtic.mil/c3i/cio/references/itmra.Annot.html**).

Nondevelopmental Item (NDI)

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

2. Any item described in subparagraph 1 above, that requires only minor modification in order to meet the requirements of the procuring agency.
3. Any item currently being produced that does not meet the requirement of paragraphs 1 or 2 above, solely because the item is not yet in use.

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

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 that exist between objects. (HLA Glossary: **http://hla.dmso.mil/hla/general/hlagloss.html**).

Open System

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

- Well defined, widely used, non-proprietary interfaces/protocols, and
- Use of standards which are developed/adopted by industrially recognized standards bodies, and
- Definition of all aspects of system interfaces to facilitate new or additional systems capabilities for a wide range of applications, and
- Explicit provision for expansion or upgrading through the incorporation of additional or higher performance elements with minimal impact on the system.

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

Open Systems Approach

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

Operational Architecture (OA)

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

Portability

The ease with which a system, component, body of data, or user can be transferred from one hardware or software environment to another. (TAFIM, Version 3.0, Volumes 1 and 3).

Practice

A recommended implementation or process that further clarifies the implementation of a standard or a profile of a standard. (VISP (Video Imagery Standards Profile)).

Profile of a Standard

An extension to a existing, approved standard which further defines the implementation of that standard in order to ensure interoperability. A profile is generally more restrictive than the base standard it was extracted from. (VISP).

Protocol Data Unit (PDU)

DIS terminology for a unit of data that is passed on a network between simulation applications. (DoD 5000.59-P, "Modeling and Simulation Master Plan," October 1995, authorized by DoD Directive 5000.59, January 4, 1994).

Real Time, Real-time

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

or

Absence of delay, except for the time required for transmission. (DoD HCI Style Guide).

Real-Time Control System

Systems capable of responding to external events with negligible delays. (DoD HCI Style Guide).

Real-time Systems

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

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. (JP1-02).

Reference Model

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

Runtime Infrastructure (RTI)

The general purpose distributed operating system software which provides the common interface services during the runtime of an HLA federation. (HLA Glossary: **http://hla.dmso.mil/hla/general/hlagloss.html**).

Scalability, Scaleability

1. The capability to adapt hardware or software to accommodate changing work loads. (OS-JTF).
2. 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. (TAFIM, Version 3.0, Volumes 1 and 3).

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

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

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. (HLA Glossary: http://hla.dmso.mil/hla/general/hlagloss.html).

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 and technical requirements for processes, procedures, practices, and methods. Standards may also establish requirements for selection, application, and design criteria of material. (DoD 4120.3-M).

Standards Based Architecture

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

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. (TAFIM, Version 3.0, Volumes 1 and 3).

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. (JP1-02).

Synthetic Environment Data Representation and Interchange Specification (SEDRIS)

The specification encompasses a robust data model, data dictionary, and interchange format supported by read and write application programmer's interfaces (APIs), data viewers, a data model browser, and analytical verification and validation data model compliance tools.

Synthetic Environments (SE)

Interneted simulations that represent activities at a high level of realism from simulations of theaters of war to factories and manufacturing processes. These environments may be created within a single computer or a vast distributed network connected by local and wide area networks and augmented by super-realistic special effects and accurate behavioral models. They allow visualization of and immersion into the environment being simulated. (DoD 5000.59-P, "Modeling and Simulation Master Plan," October 1995, authorized by DoD Directive 5000.59, January 4, 1994); (CJCSI 8510.01, Chairman of the Joint Chiefs of Staff Instruction 8510.01, "Joint Modeling and Simulation Management," February 17, 1995).

System

1. People, machines and methods organized to accomplish a set of specific functions. (FIPS 11-3).
2. An integrated composite of people, products, and processes that provides a capability or satisfies a stated need or objective. (DoD 5000.2).

Systems Architecture (SA)

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

Technical Architecture (TA)

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

Technical Reference Model (TRM)

A conceptual framework that provides the following:

A. Consistent set of service and interface categories and relationships used to address interoperability and open system issues.

B. Conceptual entities that establish a common vocabulary to better describe, compare, and contrast systems and components.

C. 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 and does not contain standards.

Video

Electro-Optical imaging sensors and systems which generate sequential or continuous streaming imagery at specified rates. Video standards are developed by recognized bodies such as ISO, ITU, SMPTE, EBU, etc. (VISP).

Weapon Systems

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

APPENDIX B: LIST OF MANDATED STANDARDS AND SOURCES

B.1 INTRODUCTION

This appendix summarizes the mandated standards from the Joint Technical Architecture (JTA), and provides references to locations where the standards may be obtained. In Section B.2, the mandated standards are summarized in a set of tables, with one table for each section of the JTA core (Sections 2.2 to 2.6) and one table for each Domain and Subdomain Annex.

The first column in each table contains a reference to the JTA section where the standard is mandated. When there are multiple standards mandated in a section, only the first standard contains a reference. The second column contains the full citation for the mandated standard, including an identifying number, date, and title.

If the mandated standard is based on other standards (e.g., it is a Government profile of one or more industry standards), the third column identifies the "base standards" that are referenced by the mandated standard. These are included as a convenience to allow greater understanding of the scope of these mandated standards. Depending on how the base standards are referenced in the mandated standard, part or all of the base standards may implicitly also be mandated.

The fourth column provides a view of the standards mandated in previous versions of the JTA.

The fifth column provides information on the emerging standards which are expected to be mandated in future versions of the JTA. There is a clear separation between mandated and emerging standards in the JTA; for example, JTA core mandated standards are found within sections 2.X.2, and emerging standards within sections 2.X.3. In addition, the need was identified to map (whenever possible) emerging standards to mandated standards or service areas. Therefore, Appendix B includes emerging standards once in the emerging section, and, when appropriate, duplicated (mapped) to mandated service areas/standards.

Section B.3 lists the organizations from which standards documents cited in the JTA may be obtained. It contains two tables: Commercial Documents, and Government Documents. Each entry gives the full name of the relevant organization, and, where available, the organization's postal address and telephone number. Where possible, each entry also includes a World Wide Web Uniform Resource Locator (URL) providing access to information about the cited documents. In many cases, the text of the documents can be downloaded from the corresponding World Wide Web site.

B.2 SUMMARY LIST OF JTA STANDARDS

Information Processing Standards

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.2.2.2.1.2 User Interface Services	C507, Window Management (X11R5): X Window System Protocol, X/Open CAE Specification, April 1995		FIPS PUB 158-1: 1993, User Interface Component of the Application Portability Profile, X-Windows Version 11, Release 5	2.2.3.1 Common Desktop Environment (CDE), Version 2.1, which integrates Motif 2.1 graphical user interface, X Window System (XIIR6), and CDE	FIPS cancelled. FIPS was an adoption of X11R5 (MIT X Consortium).
	C508, Window Management (X11R5): Xlib - C Language Binding, X/Open CAE Specification, April 1995		FIPS PUB 158-1: 1993, User Interface Component of the Application Portability Profile, X-Windows Version 11, Release 5	2.2.3.1 Common Desktop Environment (CDE), Version 2.1, which integrates Motif 2.1 graphical user interface, X Window System (XIIR6), and CDE	
	C509, Window Management (X11R5): X Toolkit Intrinsics, X/Open CAE Specification, April 1995		FIPS PUB 158-1: 1993, User Interface Component of the Application Portability Profile, X-Windows Version 11, Release 5	2.2.3.1 Common Desktop Environment (CDE), Version 2.1, which integrates Motif 2.1 graphical user interface, X Window System (XIIR6), and CDE	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	C510, Window Management (X11R5): File Formats & Application Conventions, X/Open CAE Specification, April 1995		FIPS PUB 158-1: 1993, User Interface Component of the Application Portability Profile, X-Windows Version 11, Release 5	2.2.3.1 Common Desktop Environment (CDE), Version 2.1, which integrates Motif 2.1 graphical user interface, X Window System (XIIR6), and CDE	
	C320, Motif Toolkit API, X/Open CAE Specification, April 1995		OSF Motif Application Environment Specification (AES) Release 1.2, 1992 and OSF/Motif Motif Inter Client Communications Converntion Manual (ICCCM)	2.2.3.1 Common Desktop Environment (CDE), Version 2.1, which integrates Motif 2.1 graphical user interface, X Window System (XIIR6), and CDE	C320 replaced both, AES and ICCCM.
	X/Open C323, Common Desktop Environment (CDE) Version 1.0, April 1995		same	2.2.3.1 Common Desktop Environment (CDE), Version 2.1, which integrates Motif 2.1 graphical user interface, X Window System (XIIR6), and CDE	
	Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993 or later, Microsoft Press		same (see Comment)		Same reference as previously mandated; but defaults to latest version (i.e., ".. 1993 or later")

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.2.2.2.1.3 Data Management Services	ISO/IEC 9075:1992, Information Technology - Database Language - SQL, as modified by FIPS PUB 127-2:1993, Database Language for Relational DBMS		same		Entry-level SQL
	Open Data-Base Connectivity ODBC 2.0		same		
2.2.2.2.1.4.1 Document Interchange	ISO 8879:1986, Standard Generalized Markup Language (SGML), with Amendment 1, 1988		same	2.2.3.3.1 eXtensible Markup Language (XML), REC-xml-19980210, Extensible Markup Language, W3C Recommendation, 10 February 1998	
	REC-html-971218-, Hypertext Markup Language (HTML), Internet Version 4.0, Reference Specification, World Wide Web Consortium (W3C), 18 December 1997.		RFC-1866:1995, Hypertext Markup Language (HTML), Internet Version 2.0	2.2.3.3.1 eXtensible Markup Language (XML), REC-xml-19980210, Extensible Markup Language, W3C Recommendation, 10 February 1998	Interchange format used by the World Wide Web for hypertext format and embedded navigational links.
2.2.2.2.1.4.2 Graphics Data Interchange	ANSI/ISO/IEC 8632-1,2,3,4:1992 (R1997); ISO 8632:1992 with Amendment 1:1994 and Amendment 2:1995; as profiled by FIPS PUB 128-2,Computer Graphics Metafile (CGM) Interchange format for vector graphics data, 17 April 1996		ISO 8632.1-4: 1992 Computer Graphics Metafile (CGM), profiled by FIPS PUB 128-1: 1993, Computer Graphics Metafile (CGM) - Interchange format for vector graphics data		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	JPEG File Interchange Format (JFIF), Version 1.02, C-Cube Microsystems for raster graphics data encoded using the ISO/IEC 10918-1:1994, Joint Photographic Experts Group (JPEG) algorithm	ISO/IEC 10918-1:1994 Joint Photographic Experts Group (JPEG) algorithm	same		
	Graphics Interchange Format (GIF), Version 89a, 31 July 1990, CompuServe Incorporated			2.2.3.3.2 IETF RFC-2083, Portable Network Graphics (PNG) Specification V1.0, 16 January 1997	
2.2.2.2.1.4.3 Geospatial Data Interchange	MIL-STD-2411A, Raster Product Format (RPF), 6 October 1994, with Notice of Change 1, 17 January 1995	MIL-STD-2500A, National Imagery Transmission Format Standard (NITFS) , 12 October 1994; Revised 7 February 1997	MIL-STD-2411, Raster Product Format (RPF)	2.2.3.3.4 DIGEST (Digital Geographic Information Exchange Standard) 2.0, June 1997;	Date and version number were changed.
	MIL-STD-2407, Interface Standard for Vector Product Format (VPF), 28 June 1996		MIL-STD-2407, Interface Standard for Vector Product Format (VPF)		Date was added.
	MIL-STD-2401, Department of Defense World Geodetic System (WGS-84), 11 January 1994		MIL-STD-2401, World Geodetic System 84 (WGS-84), 21 March 1994	2.2.3.3.4 NIMA Technical Report for the DoD World Geodetic System (WGS-84) 1984, NIMA TR8350.2, Third Edition, 4 July 1997	Date was corrected.
	FIPS PUB 10-4, Countries, Dependencies, Areas of Special Sovereignty, and Their Principal Administrative Divisions, April 1995				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.2.2.2.1.4.4 Still Imagery Data Interchange	MIL-STD-2500A, National Imagery Transmission Format (Version 2.0) for the National Imagery Transmission Format Standard, 12 October 1994; Revised 7 February 1997		same	2.2.3.3.5 MIL-STD-2500B, National Imagery Transmission Format (Version 2.1), 22 August 1997	
	MIL-STD-188-196, Bi-Level Image Compression for the National Imagery Transmission Format Standard, 18 June 1993		same		
	MIL-STD-188-199, Vector Quantization Decompression for the National Imagery Transmission Format Standard, 27 June 1994		same		
	MIL-STD-2301A, Computer Graphics Metafile (CGM) Implementation Standard for the National Imagery Transmission Format Standard, 18 June 1993 with Notice of Change 1, 12 October 1994	ANSI/ISO 8632-1,2,3,4:1992, Computer Graphics Metafile (CGM) for the Storage and Transfer of Picture Description Information	ANSI/ISO 8632:1992 Computer Graphics Metafile (CGM), profiled by MIL-STD-2301: 18 June 1993		
	MIL-STD-188-198A, Joint Photographic Experts Group (JPEG) Image Compression for the National Imagery Transmission Format Standard, 15 December 1993	ISO/IEC 10918-1: 1994, Joint Photographic Experts Groups (JPEG)	same		
2.2.2.2.1.4.5.1.1 Video Imagery	ITU-R BT.601-4, Encoding Parameters of Digital Television for Studios, Component (4:2:2) Digital Video, 1994				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	ANSI/SMPTE 259M-1993, Television - 10 bit 4:2:2 Component (Serial Digital Interface), using ITU-R BT.601-4 Component (4:2:2) digital video waveforms				
	MPEG-2, 4:2:2 Production Profile @ Main Level (4:2:2 P @ ML), 1996	ISO/IEC 13818 - 1,2, 4, 1996 (commonly known as MPEG-2)			
	MPEG-2, 4:2:0 Main Profile @ Main Level (MP @ ML), 1996	ISO/IEC 13818 - 1,2, 4, 1996 (commonly known as MPEG-2)			
	ANSI/SMPTE 12M-1995, Television, Audio and Film - Time and Control Code				Within 12M, Vertical Interval Time Code (VITC), Drop Frame shall be used for 29.97 FPS systems, Non-Drop Frame Time Code shall be used for 24, 25, 30, 50, and 60 FPS systems. Note: Analog NTSC systems are based on 29.97 FPS.
				2.2.3.3.6.1.1 VISP DoD/IC/USIGS Video Imagery Standards Profile (VISP), Version 1.21, 7 January 1998, Chapter 3	Profile of multiple standards
2.2.2.2.1.4.5.1.4 Video Support	ISO/IEC 11172-1:1993 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s – Part 1: Systems, 1993				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	ISO/IEC 11172-1:1993/Cor. 1:1995 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s - Part 1: Systems Technical Corrigendum 1, 1993/1995				
	ISO/IEC 11172-2:1993 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s - Part 2 Video, 1993				
	ISO/IEC 13818-1:1996 with Amendment 1:1997, Generic Coding of Moving Pictures and Associated Audio Information - Part 1: Systems (MPEG-2), 1996				
	ISO/IEC 13818-2:1996 with Amendment 1:1997 and Amendment 2:1997, Generic Coding of Moving Pictures and Associated Audio Information - Part 2: Video (MPEG-2), 1996				
2.2.2.2.1.4.6 Audio Data Interchange	ISO/IEC 11172-3:1993, Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s - Part 3 (Audio Layer-3 only)		same		
	ISO/IEC 11172-3/Cor. 1:1996, Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -Part 3: Audio Technical Corrigendum (Audio Layer-3 only)		same		
	ISO/IEC 11172-1:1993, Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s - Part 1: Systems, 1993				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	ISO/IEC 11172-1:1993/Cor. 1:1995, Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s - Part 1: Systems Technical Corrigendum 1, 1993/1995				
			ISO/IEC 11172-1:1993, Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s – Part 1: Systems, 1993		
2.2.2.2.1.4.6.1.1 Audio for Video Imagery	ANSI S4.40-1992/AES3-1992, AES (Audio Engineering Society) Recommended Practice for Digital Audio Engineering - Serial transmission format for two-channel linearly represented digital audio data, 1992 (reaffirmed and amended 1997)				
	ISO/IEC 13818-3:1995, Information technology - Generic coding of moving pictures and associated audio information, with Amendment 1:1996. Used for compressed digital audio systems, MPEG-2 Part 3: Audio				
2.2.2.2.1.4.6.1.4 Audio for Video Support	ISO/IEC 11172-3:1993, Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s - Part 3 (Audio Layer-3 only)		same	2.2.3.3.6.1.1 ATSC A/52 (Audio), Dolby Digital AC3	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	ISO/IEC 11172-3/Cor. 1:1996, Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s – Part 3: Audio Technical Corrigendum (Audio Layer-3 only)		same		
2.2.2.2.1.4.9 Atmospheric Data Interchange	FM 92-X Ext. GRIB WMO No. 306, Manual on Codes, International Codes, Volume I.2 (Annex II to WMO Technical Regulations) Parts B and C		FM 92-X-GRIB, The WMO Format for the Storate of Weather Product Information and the Exchange of Weather Product Messages in Gridded Binary (GRIB) Form		Deleted Data Exchange Format (DEF), Appendix 30 to the TAWDS.
	FM 94-X Ext. BUFR WMO No. 306, Manual on Codes, International Codes, Volume I.2 (Annex II to WMO Technical Regulations) Parts B and C		FM 94-X-BUFR, The WMO Binary Universal Format for Representation (BUFR) of meteorological data		
2.2.2.2.1.4.10 Oceanographic Data Interchange	FM 94-X Ext. BUFR WMO No. 306, Manual on Codes, International Codes, Volume I.2 (Annex II to WMO Technical Regulations) Parts B and C		FM 94-X-BUFR, The WMO Binary Universal Format for Representation (BUFR) of meteorological data		
2.2.2.2.1.4.11 Time of Day Data Interchange	ITU-R Recommendation TF.460-4, Standard-frequency and Time-signal Emissions, International Telecommunications Union, July 1986				
2.2.2.2.1.5 Graphic Services	ANSI/ISO/IEC 9636-1,2,3,4,5,6:1991 (R1997), Information Technology-Computer Graphics-Interfacing (CGI) Techniques for Dialogue with Graphics Devices		same		Reaffirmed in 1997

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	The OpenGL Graphics System: A Specification (Version 1.1) 25 June 1996		ISO 9592: 1989, as profiled by FIPS PUB 153, Programmers Hierarchical Interactive Graphics Systems (PHIGS) - for 3-D graphics		For 3D Graphics.
			ISO 7942: 1985, as profiled by FIPS PUB 120-1 (change notice 1): 1991, Graphical Kernel System (GKS) - for 2-D graphics		
2.2.2.2.1.7 Operating System Services	ISO/IEC 9945-1:1996, Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) [C language] (Mandated Services)		ISO 9945-1: 1990, Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 1: System Application Program Interface (API) [C language], (as profiled by FIPS PUB 151-2: 1993). IEEE 1003.1i: 1995, POSIX - Part 1: System Application Program Interface (API) Amendment : Technical Corrigenda to Real-time Extension [C Language]	2.2.3.4.1 P1003.1d Real-Time System API Extensions, draft 10, March 1997	ISO/IEC 9945-1:1996, replaces 2 previously mandated JTA 1.0 standards.

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.2.3.4.1 P1003.1g - Protocol Independent Interfaces, draft 6.6, April 1997	
				2.2.3.4.1 P1003.1h - Services for Reliable, Available, Serviceable Systems, draft 3, January 1998	
				2.2.3.4.1 P1003.1j - Advanced Real-time System API Extensions, draft 6, February 1998	
				2.2.3.4.1 P1003.1m - Checkpoint Restart, draft 1.3, October 1997	
				2.2.3.4.1 P1003.1q - System API: The Trace Amendment, draft 2.6, January 1998	
				2.2.3.4.1 P1003.13 Standardized Application Environment Profile - POSIX Real-Time Application Support, draft 9, January 1998	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.2.3.4.1 P1003.21 Real-Time Distributed Systems Communication, Version 1.0, October 1996	
	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)		IEEE 1003.1b: 1993, POSIX - Part 1: System Application Program Interface (API) Amendment 1; Real Time Extension [C Language], (as profiled by FIPS PUB 151-2: 1993)		
	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)		IEEE 1003.1c: 1995, POSIX - Part 1: System Application Program Interface (API) Amendment 2: Threads Extension [C Language]		
	ISO/IEC 9945-2: 1993, Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities, as profiled by FIPS PUB 189: 1994, Information Technology - Portable Operating System Interface (POSIX) - Recommendations (Section 12) and Implementation Guidance (Section 13).	FIPS PUB 189:1994, Information Technology - Portable Operating System Interface (POSIX) - Recommendations (section 12) and Implementation Guidance (section 13)	ISO/IEF 9945-2:1993, Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities as profiled by FIPS PUB 189:1994		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	IEEE 1003.2d:1994, POSIX - Part 2: Shell and Utilities - Amendment: Batch Environment		same		
				2.2.3.4.2 UNIX X/Open Single UNIX Specification (SUS) Version 2 (T912) (previously referred to as Specification 1170), February 1997	Will be used in conjunction with POSIX.1 and POSIX.2
	IEEE 1003.5, IEEE Standard for Information Technology - POSIX Ada Language Interfaces - Part 1: Binding for System Application Program Interface (API), 1992, with Interpretations: March 1994				
	IEEE 1003.5b - 1996, IEEE Standard for Information Technology - POSIX Ada Language Interfaces - Part 1: Binding for System Application Programming Interface (API) - Amendment 1: Real-time Extensions (Incorporates IEEE 1003.5:1992)				
	Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993 or later, Microsoft Press		Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993, Microsoft Press.		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.2.3.4.3 JVM Java Virtual Machine (JVM) and Supporting Libraries, Addison – Wesley, 1997	Will be used for web browser and portable applications
2.2.2.2.2.1 International-ization Services	ANSI/ISO 8859-1:1987, Information Processing – 8-Bit Single Byte Coded Character Sets, Part 1: Latin Alphabet No. 1		same		
	ISO/IEC 10646-1:1993, Information Technology - Universal Multiple-Octet Coded Character Set (UCS), Part 1: Architecture and Basic Multilingual Plane with Technical Corrigendum 1:1996		same		
2.2.2.2.2.4.1 Remote Procedure Computing	C310, DCE 1.1: Time Services Specification, X/Open CAE Specification, November 1994		OSF - DCE Time Services, Version 1.1, 1994	2.2.3.5 DCE 1.2.2 OSF-DCE Version 1.2.2, November 1997	
	C311, DCE 1.1: Authentication and Security Services, Open Group CAE Specification, August 1997			2.2.3.5 DCE 1.2.2 OSF-DCE Version 1.2.2, November 1997	
	C705, DCE 1.1: Directory Services, Open Group CAE Specification, August 1997		OSF - DCE Directory Services, Version 1.1, 1994.	2.2.3.5 DCE 1.2.2 OSF-DCE Version 1.2.2, November 1997	
	C706, DCE 1.1: Remote Procedure Call, Open Group CAE Specification, August 1997		OSF - DCE Remote Procedure Call (RPC), Version 1.1, 1994	2.2.3.5 DCE 1.2.2 OSF-DCE Version 1.2.2, November 1997	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.2.2.2.2.4.2 Distributed Object Computing	The Common Object Request Broker: Architecture and Specification, Version 2.1, OMG document formal/1 September 1997		OMG - The Common Object Request Broker: Architecture and Specification (CORBA), Version 2: July 1995, (also available as: X/Open Common Application Environment (CAE) Specification P431 - Common Object Request Broker Architecture & Specification, Version 2)		
				2.2.3.5 UML Unified Modeling Language (UML), Rational Corp., Version 1.0, January 1997	
				2.2.3.5 MOF Meta-Object Facility (MOF) Specification, 1 September 1997	
				2.2.3.5 COM/CORBA Interworking Part B Joint Revised Submission, 19 November 1997	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.2.3.5 MAF Mobile Agent System Interoperability Facilities Specification, 10 November 1997	
	Naming Service, 7 December 1993, contained in CORBAservices: Common Object Services Specification, OMG Document formal/4 July 1997		OMG - CORBA services: Common Object Services Specification, March 1996 (also available as: X/Open CAE Specification P432 - Common Object Services, Volume 1 and X/Open CAE Specification P502 - Common Object Services, Volume 2)		
	Event Notification Service, 7 December 1993, contained in CORBAservices: Common Object Services Specification, OMG Document formal/24 February 1997		OMG - CORBA services: Common Object Services Specification, March 1996 (also available as: X/Open CAE Specification P432 - Common Object Services, Volume 1 and X/Open CAE Specification P502 - Common Object Services, Volume 2)		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	Object Transaction Service, 6 December 1994, contained in CORBAservices: Common Object Services Specification, OMG Document formal/24 February 1997		OMG - CORBA services: Common Object Services Specification, March 1996 (also available as: X/Open CAE Specification P432 - Common Object Services, Volume 1 and X/Open CAE Specification P502 - Common Object Services, Volume 2)		
			OMG - CORBA facilities: Common Object Facilities Architecture, November 1995		
2.2.3.1 User Interface				Common Desktop Environment (CDE), Version 2.1, which integrates Motif 2.1 graphical user interface, X Window System (XIIR6), and CDE	
2.2.3.3.1 Document Interchange				eXtensible Markup Language (XML), REC-xml-19980210, Extensible Markup Language, W3C Recommendation, 10 February 1998	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.2.3.3.2 Graphics Data Interchange				IETF RFC-2083, Portable Network Graphics (PNG) Specification V1.0, 16 January 1997	
2.2.3.3.4 Geospatial Data Interchange				DIGEST (Digital Geographic Information Exchange Standard) 2.0, June 1997	
				NIMA Technical Report for the DoD World Geodetic System (WGS-84) 1984, NIMA TR8350.2, Third Edition, 4 July 1997	
2.2.3.3.5 Still Imagery Data Interchange				MIL-STD-2500B, National Imagery Transmission Format (Version 2.1), 22 August 1997	
2.2.3.3.6.1.1 Video Imagery				DoD/IC/USIGS Video Imagery Standards Profile (VISP), Version 1.21, 7 January 1998, Chapter 3	
				ATSC A/52 (Audio), Dolby Digital AC3	
2.2.3.4.1 POSIX				P1003.1d - Real-Time System API Extensions, draft 10, March 1997	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				P1003.1g - Protocol Independent Interfaces, draft 6.6, April 1997	
				P1003.1h - Services for Reliable, Available, Serviceable Systems, draft 3, January 1998	
				P1003.1j - Advanced Real-time System API Extensions, draft 6, February 1998	
				P1003.1m - Checkpoint Restart, draft 1.3, October 1997	
				P1003.1q - System API: The Trace Amendment, draft 2.6, January 1998	
				P1003.13 - Standardized Application Environment Profile - POSIX Real-Time Application Support, draft 9, January 1998	
				P1003.21 - Real-Time Distributed Systems Communication, Version 1.0, October 1996	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.2.3.4.2 UNIX				X/Open Single UNIX Specification (SUS) Version 2 (T912) (previously referred to as Specification 1170), February 1997	
2.2.3.4.3 Virtual Machines				Java Virtual Machine (JVM) and Supporting Libraries, Addison – Wesley, 1997	
2.2.3.5 Distributed Computing				OSF-DCE Version 1.2.2, November 1997	
				Unified Modeling Language (UML), Rational Corp., Version 1.0, January 1997	
				Meta-Object Facility (MOF) Specification, 1 September 1997	
				COM/CORBA Interworking Part B Joint Revised Submission , 19 November 1997	
				Mobile Agent System Interoperability Facilities Specification, 10 November 1997	

Information Transfer Standards

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.3.2.1.1 Host Standards	IETF Standard 3/RFC-1122/RFC-1123, Host Requirements, October 1989		IAB-Standard-3/RFC-1122/RFC-1123, Host Requirements, October 1989		“IAB” changed to “IETF”; no change in content of standard.
2.3.2.1.1.1.1 Electronic Mail	ACP 123, Common Messaging Strategy and Procedures, November 1994		same		
	ACP 123, U.S. Supplement No. 1, Common Messaging Strategy and Procedures, November 1995		same		
	IETF Standard 10/RFC-821/RFC-1869/RFC-1870, Simple Mail Transfer Protocol (SMTP) Service Extensions, November 1995				
	IETF Standard 11/RFC-822/RFC-1049, Standard for the Format of ARPA Internet Text Messages, August 1982				
	IETF RFCs 2045-2049, Multipurpose Internet Mail Extensions (MIME) Parts 1-5, November 1996				
2.3.2.1.1.1.2.1 X.500 Directory Services	ITU-T X.500, The Directory - Overview of Concepts, Models and Services - Data Communication Networks Directory, 1993		same		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.3.2.1.1.1.2.2 Lightweight Directory Access Protocol (LDAP)	IETF RFC-1777, LDAP, March 1995			2.3.3.1.1 LDAPv3 IETF RFC-2251 (LDAPv3), 23 December 1997	
2.3.2.1.1.1.2.3 Domain Name System (DNS)	IETF Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987		IAB Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987	2.3.3.1.1 DDNS IETF RFC-2136 (DDNS), 21 April 1997	"IAB" changed to "IETF"; no change in content of standard.
2.3.2.1.1.1.3 File Transfer	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).		IAB Standard 9/RFC-959, File Transfer Protocol, October 1985		"IAB" changed to "IETF"; no change in content of standard.
				2.3.3.1.3 MIL-STD-2045-47000: Department of Defense Interface Standard: File and Record Transfer Protocol for Resource-Constrained Environments, 30 September 1997	New Service Area: Space Communications Protocol
2.3.2.1.1.1.4 Remote Terminal	IETF Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983		IAB Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983		"IAB" changed to "IETF"; no change in content of standard.
2.3.2.1.1.1.5 Network Time Synchronization	IETF RFC-1305, Network Time Protocol (V3), 9 April 1992		same		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.3.2.1.1.1.6 Bootstrap Protocol (BOOTP)	IETF RFC-951, Bootstrap Protocol, 1 September 1985		same		
	IETF RFC-1533 DHCP Options and BOOTP Vendor Extensions, 8 October 1993		same		
	IETF RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, 27 October 1993		same		
2.3.2.1.1.1.7 Configuration Information Transfer	IETF RFC-1541, Dynamic Host Configuration Protocol, 27 October 1993		same		Section (service area) name changed from "Dynamic Host Configuration Protocol" in V1.0.
2.3.2.1.1.1.8.1 Hypertext Transfer Protocol (HTTP)	IETF RFC-1945, Hypertext Transfer Protocol - HTTP/1.0, 17 May 1996		same		
2.3.2.1.1.1.8.2 Uniform Resource Locator (URL)	IETF RFC-1738, Uniform Resource Locators, 20 December 1994		same		
	IETF RFC-1808, Relative Uniform Resource Locators, 14 June 1995		same		
2.3.2.1.1.1.9 Connection-less Data Transfer	MIL-STD-2045-47001B, Connectionless Data Transfer Application Layer Standard, 20 January 1998		MIL-STD-2045-47001, Connectionless Data Transfer Application Layer Standard, 27 July 1995		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.3.2.1.1.2.1.1 Transmission Control Protocol (TCP)	IETF-Standard 7/RFC-793, Transmission Control Protocol, September 1981. In addition, TCP shall implement the PUSH flag and the Nagle Algorithm, as defined in IETF Standard 3, Host Requirements.		IAB-Standard 7/RFC-793, Transmission Control Protocol, September 1981		"IAB" changed to "IETF"; no change in content of standard.
	IETF RFC-2001, TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms, 24 January 1997				
				2.3.3.1.3 MIL-STD-2045-44000: Department of Defense Interface Standard: Transport Protocol for High-Stress, Resource-Constrained Environments, 30 September 1997	New Service Area: Space Communications Protocol
2.3.2.1.1.2.1.2 User Datagram Protocol (UDP)	IETF Standard 6/RFC-768, User Datagram Protocol, August 1980		IAB-Standard 6/RFC-768, User Datagram Protocol, August 1980		"IAB" changed to "IETF"; no change in content of standard.
2.3.2.1.1.2.1.3 Internet Protocol (IP)	IETF Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112, Internet Protocol, September 1981. In addition, all implementations of IP must pass the 8-bit Type-of-Service (TOS) byte transparently up and down through the transport layer as defined in IETF Standard 3, Host Requirements.		IAB-Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/ RFC-792/RFC-1112, Internet Protocol, September 1981	2.3.3.1.1 IETF RFC-1883 (IPv6 Specification), 4 January 1996	"IAB" changed to "IETF"; no change in content of standard.

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	IETF RFC-1770, IPv4 Option for Sender Directed Multi-Destination Delivery, 28 March 1995				To be used only with Combat Net Radio (CNR) routers.
				2.3.3.1.1 IETF RFC-1884 (IPv6 Addressing Architecture), 4 January 1996	
				2.3.3.1.1 IETF RFC-1885 (ICMPv6 for IPv6), 4 January 1996	
				2.3.3.1.1 IETF RFC-1886 (DNS Extensions to Support IPv6), 4 January 1996	
				2.3.3.1.1 Integrated Services and RSVP IETF RFC-1633 (Integrated Services and RSVP), 9 June 1994	
				2.3.3.1.1 MHP IETF RFC-2002 (IP Mobility Support), 22 October 1996	
				2.3.3.1.3 MIL-STD-2045-43000: Department of Defense Interface Standard: Network Protocol for High-Stress, Resource-Constrained Environments, 30 September 1997	New Service Area: Space Communications Protocol

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.3.3.1.3 MIL-STD-2045-43001: Department of Defense Interface Standard: Network Security Protocol for Resource-Constrained Environments, 30 September 1997	New Service Area: Space Communications Protocol
2.3.2.1.1.2.2 OSI Transport Over IP-based Networks	IETF Standard 35/RFC-1006, ISO Transport Service on top of the TCP, May 1987		IAB-Standard 35/RFC-1006, ISO Transport Service on top of the TCP, May 1987		"IAB" changed to "IETF"; no change in content of standard.
2.3.2.1.2 Video Teleconferencing (VTC) Standards	FTR 1080-97, Profile for Video Teleconferencing, Appendix A, 30 October 1997		VTC001, Industry Profile for Video Teleconferencing, Revision 1, April 25, 1995	2.3.3.1.2 FTR 1080 new draft appendix A	VTC001 changed to FTR 1080-97, App A; no change in content of standard.
				2.3.3.1.2 ITU-T H.321, March 1996	
				2.3.3.1.2 ITU-T H.323, November 1996	
				2.3.3.1.2 ITU-T H.310, Broadband Audiovisual Communication Systems and Terminals, November 1996.	
	ITU-T G.728, Coding of Speech at 16 kbps Using Low-Delay Code Excited Linear Prediction (LD-CELP), September 1992				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	ITU-T H.224, A Real Time Control Protocol for Simplex Applications using H.221 LSD/HSD/MLP channels, November 1994				
	ITU-T H.281, A Far-End Camera Protocol for Videoconferencing Using H.224, November 1994				
	ITU-T H.324, Terminal for Low Bit Rate Multimedia Communications, March 1996		same		
	ITU-T T.120, Transmission Protocols for Multimedia Data, July 1996			ITU-T T.128, Application Sharing	
	ITU-T T.122, Multipoint Communications Service for Audiographic and Audiovisual Conferencing Service Definition, March 1993				
	ITU-T T.123, Protocol Stacks for Audiographic and Audiovisual Teleconferencing Applications, November 1994				
	ITU-T T.124, Generic Conference Control for Audiographic and Audiovisual Terminals and Multipoint Control Units, August 1995				
	ITU-T T.125, Multipoint Communications Service Protocol Specification, April 1994				
	ITU-T T.126, Multipoint Still Image and Annotation Conferencing Protocol Specification, August 1995				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	ITU-T T.127, Multipoint Binary File Transfer Protocol, August 1995				
	ITU-T H.244, Synchronized Aggregation of Multiple 64 or 56 kbps channels, July 1995				
2.3.2.1.3.1 Analog Facsimile Standards	TIA/EIA-465-A, Group 3 Facsimile Apparatus for Document Transmission, 21 March 1995		same		
	TIA/EIA-466-A, Procedures for Document Facsimile Transmission, 27 September 1996		TIA/EIA-466, Procedures for Document Facsimile Transmission, May 1981		
2.3.2.1.3.2 Digital Facsimile Standard	MIL-STD 188-161D, Interoperability and Performance Standards for Digital Facsimile Equipment, 10 January 1995		same		
2.3.2.1.4 Secondary Imagery Dissemination Communications Standards	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		MIL-STD-2045-44500, National Imagery Transmission Standard (NITFS) Tactical Communications Protocol 2 (TACO2), 18 June 1993		Added notice of changes 1 and 2.
2.3.2.2.1 Internetworking (Router) Standards	IETF RFC-1812, Requirements for IP Version 4 Routers, 22 June 1995		same		
	IETF Standard 6/RFC-768, User Datagram Protocol, August 1980		IAB Standard 6/RFC-768, User Datagram Protocol, August 1980		"IAB" changed to "IETF"; no change in content of standard.

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	IETF Standard 7/RFC-793, Transmission Control Protocol, September 1981		IAB Standard 7/RFC-793, Transmission Control Protocol, September 1981		"IAB" changed to "IETF"; no change in content of standard.
	IETF Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983		IAB Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983		"IAB" changed to "IETF"; no change in content of standard.
	IETF Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987		IAB Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987		"IAB" changed to "IETF"; no change in content of standard.
	IETF RFC-951, Bootstrap Protocol, 1 September 1985		same		
	IETF RFC-1533, DHCP Options and BOOTP Vendor Extensions, 8 October 1993		same		
	IETF RFC-1541, DHCP, 27 October 1993		same		
	IETF RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, 27 October 1993		same		
	IETF Standard 33/RFC-1350, Trivial FTP (TFTP), July 1992, to be used for initialization only		IAB Standard 33/RFC-1350, Trivial FTP (TFTP), July 1992, to be used for initialization only		"IAB" changed to "IETF"; no change in content of standard.

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.3.2.2.1.1 Internet Protocol (IP)	IETF Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/ RFC-792/RFC-1112, Internet Protocol, September 1981		IAB Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/ RFC-792/RFC-1112, Internet Protocol, September 1981		"IAB" changed to "IETF"; no change in content of standard.
	IETF RFC-1770, IPv4 Option for Sender Directed Multi-Destination Delivery, 28 March 1995				To be used only with Combat Net Radio (CNR) routers.
2.3.2.2.1.2.1 Interior Routers	IETF RFC-1583, Open Shortest Path First Routing Version 2, 23 March 1994		same		For unicast routing.
	IETF RFC-1584, Multicast Extensions to OSPF, 24 March 1994		same		For multicast routing.
2.3.2.2.1.2.2 Exterior Routers	IETF RFC-1771, Border Gateway Protocol 4, 21 March 1995		same		
	IETF RFC-1772, Application of BGP-4 In the Internet, 21 March 1995		same		
2.3.2.2.2.1 Local Area Network (LAN) Access	ISO/IEC 8802-3:1996, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification, 10BASE-T Medium-Access Unit (MAU)		ISO/IEC 8802-3:1993, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 10BaseT Medium-Access Unit (MAU)		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	IEEE 802.3u-1995, Supplement to ISO/IEC 8802-3:1993, Local and Metropolitan Area Networks: Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100 Mb/s Operation, Type 100BASE-T (Clauses 21-30)				
	IETF Standard 41/RFC-894, Standard for the Transmission of IP Datagrams Over Ethernet Networks, April 1984		IAB Standard 41/RFC-894, Standard for the Transmission of IP Datagrams Over Ethernet Networks, April 1984		"IAB" changed to "IETF"; no change in content of standard.
	IETF Standard 37/RFC-826, An Ethernet Address Resolution Protocol, November 1982		IAB Standard 37/RFC-826, An Ethernet Address Resolution Protocol, November 1982		"IAB" changed to "IETF"; no change in content of standard.
				2.3.3.2 IEEE 802.11-1997 Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 1997	New Service Area—Wireless LANs
2.3.2.2.2.2 Point to Point Standards	IETF Standard 51/RFC-1661/RFC-1662, Point-to-Point Protocol (PPP), July 1994		IAB Standard 51/RFC-1661/RFC-1662, Point-to-Point Protocol (PPP), July 1994		"IAB" changed to "IETF"; no change in content of standard.
	IETF RFC-1332, PPP Internet Protocol Control Protocol (IPCP), 26 May 1992		same		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	IETF RFC-1989, PPP Link Quality Monitoring (LQM), 16 August 1996		RFC-1333, PPP Link Quality Monitoring, May 26, 1992		
	IETF RFC-1994, PPP Challenge Handshake Authentication Protocol (CHAP), 30 August 1996		RFC-1334, PP Authentication Protocols, October 20, 1992		
	IETF RFC-1570, PPP Link Control Protocol (LCP) Extensions, 11 January 1994		same		
				2.3.3.2 IETF RFC-1990, PPP Multilink Protocol, 16 August 1996	
	EIA/TIA-232-E, Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, July 1991		EIA 232E, Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, July 1991		"EIA" changed to "EIA/TIA"; no change in content of standard.
	EIA/TIA-530-A, High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, June 1992, Including Alternate 26-Position Connector, 1992		EIA 530A, High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, June 1992, Including Alternate 26-Position Connector, 1992		"EIA" changed to "EIA/TIA"; no change in content of standard

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
			EIA 449, General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, February 1980		
2.3.2.2.2.3 Combat Net Radio (CNR) Networking	MIL-STD-188-220B, Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, 20 January 1998		MIL-STD-188-220A, Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, 27 July 1995		
2.3.2.2.2.4 Integrated Services Digital Network (ISDN)	ANSI T1.601, ISDN Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT (Layer 1 Specification), 1992		same		
	ANSI T1.408, ISDN Primary Rate - Customer Installation Metallic Interfaces (Layer 1 Specification), 1990		same		
	ANSI T1.602, ISDN Data Link Signaling Specification for Application at the User Network Interface, 1996		ITU-T Q.921, ISDN User-Network Interface - Data Link Layer Specification - Digital Subscriber Signaling System No. 1, 1993		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	ANSI T1.607, Digital Subscriber Signaling System No. 1 (DSS1) - Layer 3 Signaling Specification for Circuit Switched Bearer Service, 1990		ITU-T Q.931, ISDN User-Network Interface Layer 3 Specification for basic Call Control - Digital Subscriber Signaling System No. 1(DSS 1), Network Layer, User-Network Management, 1989		
	ANSI T1.607a, Supplement, 1996				
	ANSI T1.610, DSS1 - Generic Procedures for the Control of ISDN Supplementary Services, 1994				
	ANSI T1.619, Multi-Level Precedence and Preemption (MLPP) Service, ISDN Supplementary Service Description, 1992				
	ANSI T1.619a, Supplement, 1994.				
	SR-3875, National ISDN 1995, 1996, and 1997, Bellcore				
	SR-3888, 1997 Version of National ISDN Basic Rate Interface Customer Premise Equipment Generic Guidelines, Bellcore				
	SR-3887, 1997 Version of National ISDN Primary Rate Interface Customer Premise Equipment Generic Guidelines, Bellcore				
	ITU-T E.164, Numbering Plan for the ISDN Era, May 1997		same		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	DISA Circular (DISAC) 310-225-1, Defense Switched Network (DSN) User Services Guide, 2 April 1998		DCAC 370-175-13, Defense Switched Network System Interface Criteria, section titled Worldwide Numbering and Dialing Plan (WNDP), September 1993		
	IETF RFC-1356, Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode, 6 August 1992		same		
	IETF RFC-1618, PPP over ISDN, 13 May 1994		same		
2.3.2.2.2.5 Asynchronous Transfer Mode (ATM)	ATM Forum, af-phy-0040.000, Physical Interface Specification for 25.6 Mbps over twisted pair, November 1995				
	ATM Forum, af-uni-0010.002, ATM UNI Specification V 3.1, Section 2, September 1994		same		For Physical Layer
	ATM Forum, af-phy-0016.000, DS1 Physical Layer Interface Specification, September 1994				
	ATM Forum, af-phy-0054.000, DS3 Physical Layer Interface Specification, January 1996				
	ATM Forum, af-phy-0046.000, 622.08 Mbp/s Physical Layer, January 1996				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	ATM Forum, af-uni-0010.002, ATM UNI Specification V 3.1, September 1994				For User to Network Interface
	ANSI T1.630, ATM Adaptation Layer for Constant Bit Rate (CBR) Services Functionality and Specification, 1993		same		
	ANSI T1.635, ATM Adaptation Layer Type 5 Common Part Functions and Specifications, 1994, which adopts ITU-T I.363, section 6		same		
	ATM Forum, af-pnni-0055.000, PNNI Specification, Version 1.0, March 1996				
	ATM Forum, af-pnni-0066.000, PNNI Version 1.0 Addendum, September 1996				
	ATM Forum, af-lane-0021.000, LANE over ATM, Ver. 1.0 January 1995		IETF RFC-1577, Classical IP and Address Resolution Protocol (ARP) over ATM, 20 January 1994		
	ATM Forum, af-lane-0050.000, LANE Ver. 1.0 Addendum, December 1995				
	ATM Forum, af-lane-0038.000, LANE Client Management Specification, September 1995				
	ATM Forum, af-lane-0057.000, LANE Servers Management Specification, March 1996				
	ATM Addressing Format specified as Notice of Change 1, 20 October 1997, to MIL-STD-188-176, Standardized Profile for ATM, 21 May 1996				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.3.3.2 af-sig-0061.000, UNI signaling	
				2.3.3.2 af-sig-0076.000, signaling ABR addendum	
				2.3.3.2 af-ilmi-0065.000, integrated local management	
				2.3.3.2 af-tm-0056.000, traffic management	
				2.3.3.2 af-tm-0077.000; traffic management ABR addendum	
				2.3.3.2 af-vtoa-0078.000, Circuit Emulation Service Interoperability Specification	
				2.3.3.2 af-lane-0084.000; LANE Version 2.0 LANE UNI (LUNI)	
				2.3.3.2 af-mpoa-0087.000, MultiProtocol Over ATM (MPOA) Version 1.0	
				2.3.3.2 af-vtoa-0089.000, ATM trunking using AAL1 for Narrowband Services Version 1.0	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.3.3.2 IS-41-C, North American standard signaling protocol for CDMA and TDMA mobile cellular	
				2.3.3.2 IMT-2000, International Mobile Telecommunications	New Service Area: International Mobile Telecommunications
				2.3.3.2 J-STD-008, PCS standard for CDMA	New Service Area: PCS & Mobile Cellular
				2.3.3.2 IS-95-A, Mobile Cellular standard for CDMA	
2.3.2.3.1.1.1 5- and 25-kHz Service	MIL-STD-188-181A, Interoperability Standard for Single Access 5-kHz and 25-kHz UHF Satellite Communications Channels, 31 March 1997		MIL-STD-188-181, Interoperability Standard for Dedicated 5-kHz and 25-kHz UHF Satellite Communications, 18 September 1992		
2.3.2.3.1.1.2 5-kHz DAMA Service	MIL-STD-188-182A, Interoperability Standard for 5 kHz UHF DAMA Terminal Waveform, 31 March 1997		MIL-STD-188-182, Interoperability Standard for 5 kHz UHF DAMA Terminal Waveform, 18 September 1992		
2.3.2.3.1.1.3 25-kHz TDMA/ DAMA Service	MIL-STD-188-183, Interoperability Standard for 25 kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992; with Notice of Change 1, dated 2 December 1996		MIL-STD-188-183, Interoperability Standard for 25 kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.3.2.3.1.1.4 Data Control Waveform	MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993		same		
2.3.2.3.1.1.5 DAMA Control System	MIL-STD-188-185, DoD Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System, 29 May 1996				
2.3.2.3.1.2.1 Earth Terminals	MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995		same		
2.3.2.3.1.2.2 Phase Shift Keying (PSK) Modems	MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995		same		
				2.3.3.3 MIL-STD-188-166, Interface Standard, Interoperability and Performance Standard for SHF SATCOM Link Control	
				2.3.3.3 MIL-STD-188-167, Interface Standard, Message Format for SHF SATCOM Link Control	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.3.3.3 MIL-STD-188-168, Interface Standard, Interoperability and Performance Standards for SHF Satellite Communications Mulitplexers and Demultiplexers	
2.3.2.3.1.3.1 Low Data Rate (LDR)	MIL-STD-1582D, EHF LDR Uplinks and Downlinks, 30 September 1996; with Notice of Change 1, 14 February 1997		MIL-STD-1582, EHF LDR Uplinks and Downlinks, 10 December 1992		
2.3.2.3.1.3.2 Medium Data Rate (MDR)	MIL-STD-188-136, EHF MDR Uplinks and Downlinks, 26 August 1995; with Notice of Change 1, 15 August 1996, and Notice of Change 2, 14 February 1997		MIL-STD-188-136, EHF MDR Uplinks and Downlinks, 26 August 1995		Added notice of changes 1 and 2.
2.3.2.3.2.1 Low Frequency (LF) and Very Low Frequency (VLF)	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				
2.3.2.3.2.2.1 HF and Automated Link Establishment (ALE)	MIL-STD-188-141A, Interoperability and Performance Standards for Medium and High Frequency Radio Equipment Standard, 15 September 1988; with Notice of Change 1, 17 June 1992, and Notice of Change 2, 10 September 1993		same		
2.3.2.3.2.2.2 Anti-Jamming Capability	MIL-STD-188-148A, Interoperability Standard for Anti-Jam Communications in the HF Band (2-30 MHz), 18 March 1992		same		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.3.2.3.2.2.3 Data Modems	MIL-STD-188-110A, Data Modems, Interoperability and Performance Standards, 30 September 1991		same		
2.3.2.3.2.3 Very High Frequency (VHF)	MIL-STD-188-242, Tactical Single Channel (VHF) Radio Equipment, 20 June 1985		same		
				2.3.3.4 MIL-STD-188-241, RF Interface Requirements for VHF Frequency Hopping Tactical Radio Systems	
2.3.2.3.2.4.1 UHF Radio	MIL-STD-188-243, Tactical Single Channel (UHF) Radio Communications, 15 March 1989		same		
2.3.2.3.2.4.2 Anti-Jamming Capability	STANAG 4246, Edition 2, HAVE QUICK UHF Secure and Jam-Resistant Communications Equipment, 17 June 1987; with Amendment 3, August 1991				
2.3.2.3.2.5 Super High Frequency (SHF)	MIL-STD-188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment, 7 May 1987; with Notice of Change 1, 28 July 1992		same		
2.3.2.3.2.6 Link 16 Transmission Standards	STANAG 4175, Edition 1, Technical Characteristics of the Multifunctional Information Distribution System (MIDS), 29 August 1991		same		Previous section (service area) in Volume 1.0 was named "JTIDS/MIDS Transmission Media"
			JTIDS System Segment Specification (Class 2 Terminal)		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.3.2.3.3 SONET Transmission Facilities	ANSI T1.105, Telecommunications - Synchronous Optical Network (SONET) Basic Description Including Multiplex Structure, Rates and Formats (ATIS) (Revision and Consolidation of ANSI T1.105-1991 and ANSI T1.105A-1991), 1995		same		
	ANSI T1.107, Digital Hierarchy - Formats Specifications, 1995		same		
	ANSI T1.117, Digital Hierarchy - Optical Interface Specifications (SONET) (Single Mode - Short Reach), 1991		same		
2.3.2.4.1 Data Communica-tions Management	IETF Standard 15/RFC-1157, Simple Network Management Protocol (SNMP), May 1990		same		
	IETF Standard 16/RFC-1155/RFC-1212, Structure of Management Information, May 1990		same		
	IETF Standard 17/RFC-1213, Management Information Base, March 1991		same	2.3.3.5 IETF RFC-2011, SNMPv2 Management Information Base for the Internet Protocol using SMIv2, 12 November 1996	
	IETF RFC-1514, Host Resources MIB, September 1993				
	IETF Standard 50/RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	IETF RFC-1757, Remote Network Monitoring Management Information Base (RMON Version 1), February 1995				
	IETF RFC-1850, Open Shortest Path First (OSPF) Version 2 Management Information Base, November 1995				
				2.3.3.5 IETF RFC-1471, The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol, 8 June 1993	
				2.3.3.5 IETF RFC-1472, The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol, 8 June 1993	
				2.3.3.5 IETF RFC-1473, The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol, 8 June 1993	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.3.3.5 IETF RFC-1474, The Definitions of Managed Objects for the Bridge Network Control Protocol of the Point-to-Point Protocol, 8 June 1993	
				2.3.3.5 IETF RFC-2021, Remote Network Monitoring Management Information Base Version 2 using SMIv2, 16 January 1997	
				2.3.3.5 IETF RFC-2012, SNMPv2 Management Information Base for the Transmission Control Protocol, 12 November 1996	
				2.3.3.5 IETF RFC-2013, SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2, 12 November 1996	
				2.3.3.5 IETF RFC-1567, X.500 Directory Monitoring MIB, 11 January 1994	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.3.3.5 IETF RFC-2248, Network Services Monitoring MIB, 13 January 1998	
				2.3.3.5 IETF RFC-2249, Mail Monitoring MIB, 13 January 1998	
				2.3.3.5 IETF RFC-1695, Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2, 25 August 1994	
				2.3.3.5 IETF RFC-1657, Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2, 21 July 1994	
				2.3.3.5 IETF RFC-1611, DNS Server MIB Extensions, 17 May 1994	
				2.3.3.5 IETF RFC-1612, DNS Resolver MIB Extensions, 17 May 1994	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.3.3.5 IETF RFC-2006, The Definitions of Managed Objects for IP Mobility Support using SMIv2, 22 October 1996	
				2.3.3.5 IETF RFC-2011, SNMPv2 Management Information Base for the Internet Protocol using SMIv2, 12 November 1996	
2.3.2.4.2 Telecommunications Management	ANSI T1.204, OAM&P - Lower Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements, 1993.				
	ANSI T1.208, OAM&P - Upper Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements, 1993				
	ITU-T M.3207.1, TMN management service: maintenance aspects of B-ISDN management, 1996				
	ITU-T M.3211.1, TMN management service: Fault and performance management of the ISDN access, 1996				
	ITU-T M.3400, TMN Management Functions, 1992				
	ISO/IEC 9595 Information Technology - Open Systems Interconnection Common Management Information Services, December 1991				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	ISO/IEC 9596-1:1991 Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) - Part 1: Specification				
	ISO/IEC 9596-2:1993 Information Technology - Open Systems Interconnection - Common Management Information Protocol: Protocol Implementation Conformance Statement (PICS) proforma				
2.3.3.1.1 Internet Standards				IETF RFC-1883 (IPv6 Specification), 4 January 1996	
				IETF RFC-1884 (IPv6 Addressing Architecture), 4 January 1996	
				IETF RFC-1885 (ICMPv6 for IPv6), 4 January 1996	
				IETF RFC-1886 (DNS Extensions to Support IPv6), 4 January 1996	
				IETF RFC-2136 (DDNS), 21 April 1997	
				IETF RFC-2251 (LDAPv3), 23 December 1997	
				IETF RFC-2002 (IP Mobility Support), 22 October 1996	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				IETF RFC-1633 (Integrated Services and RSVP), 9 June 1994	
2.3.3.1.2 Video Teleconferencing (VTC) Standards				FTR 1080-1997	
				ITU-T H.321, March 1996	
				ITU-T H.323, November 1996	
				ITU-T H.310, Broadband Audiovisual Communication Systems and Terminals, November 1996.	
2.3.3.1.3 Space Communication Protocol Standards				MIL-STD-2045-44000: Department of Defense Interface Standard: Transport Protocol for High-Stress, Resource-Constrained Environments, 30 September 1997.	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				MIL-STD-2045-43000: Department of Defense Interface Standard: Network Protocol for High-Stress, Resource-Constrained Environments, 30 September 1997	
				MIL-STD-2045-47000: Department of Defense Interface Standard: File and Record Transfer Protocol for Resource-Constrained Environments, 30 September 1997.	
				MIL-STD-2045-43001: Department of Defense Interface Standard: Network Security Protocol for Resource-Constrained Environments, 30 September 1997	
2.3.3.2 Network Standards				IEEE 802.11-1997 Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 1997	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				af-sig-0061.000, UNI signaling	
				af-sig-0076.000, signaling ABR addendum	
				af-ilmi-0065.000, integrated local management	
				af-tm-0056.000, traffic management	
				af-tm-0077.000; traffic management ABR addendum	
				af-vtoa-0078.000, Circuit Emulation Service Interoperability Specification	
				af-vtoa-0089.000, ATM trunking using AAL1 for Narrowband Services Version 1.0	
				af-lane-0084.000; LANE Version 2.0 LANE UNI (LUNI)	
				af-mpoa-0087.000, MultiProtocol Over ATM (MPOA) Version 1.0	
				J-STD-008, PCS standard for CDMA	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				IS-95-A, Mobile Cellular standard for CDMA	
				IS-41-C, North American standard signaling protocol for CDMA and TDMA mobile cellular	
				IMT-2000, International Mobile Telecommunications	
				IETF RFC-1990, PPP Multilink Protocol, 16 August 1996	
2.3.3.3 Military Satellite Communications (MILSATCOM)				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	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				MIL-STD-188-168, Interface Standard, Interoperability and Performance Standards for SHF Satellite Communications Mulitplexers and Demultiplexers	
2.3.3.4 Radio Communications				MIL-STD-188-241, RF Interface Requirements for VHF Frequency Hopping Tactical Radio Systems	
2.3.3.5 Network Management				IETF RFC-1695, Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2, 25 August 1994	
				IETF RFC-1657, Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2, 21 July 1994	
				IETF RFC-1611, DNS Server MIB Extensions, 17 May 1994	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				IETF RFC-1612, DNS Resolver MIB Extensions, 17 May 1994	
				IETF RFC-2006, The Definitions of Managed Objects for IP Mobility Support using SMIv2, 22 October 1996	
				IETF RFC-2011, SNMPv2 Management Information Base for the Internet Protocol using SMIv2, 12 November 1996	
				IETF RFC-1471, The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol, 8 June 1993	
				IETF RFC-1472, The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol, 8 June 1993	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				IETF RFC-1473, The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol, 8 June 1993	
				IETF RFC-1474, The Definitions of Managed Objects for the Bridge Network Control Protocol of the Point-to-Point Protocol, 8 June 1993	
				IETF RFC-2021, Remote Network Monitoring Management Information Base Version 2 using SMIv2, 16 January 1997	
				IETF RFC-2012, SNMPv2 Management Information Base for the Transmission Control Protocol, 12 November 1996	
				IETF RFC-2013, SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2, 12 November 1996	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				IETF RFC-1567, X.500 Directory Monitoring MIB, 11 January 1994	
				IETF RFC-2248, Network Services Monitoring MIB, 13 January 1998	
				IETF RFC-2249, Mail Monitoring MIB, 13 January 1998	

Information Modeling, Metadata, and Information Exchange Standards

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.4.2.1 Activity model	FIPS PUB 183, Integration Definition for Function Modeling (IDEF0), December 1993, as based on the Air Force Wright Aeronautical Laboratories Integrated Computer-Aided Manufacturing (ICAM) Architecture, Part II, Volume IV – Function Modeling Manual (IDEF0), June 1981		same	2.4.3.1 IEEE P1320.1, IDEF0 Function Modeling	
2.4.2.2 Data Model	DoD Manual 8320.1-M-1, DoD Data Standardization Procedures, April 1998		DoD Manual 8320.1-M-1, DoD Data Element Standardization Procedures, January 1993		
	FIPS PUB 184, Integration Definition for Information Modeling (IDEF1X), December 1993, as based on the Integration Information Support System (IISS), Volume V – Common Data Model Subsystem, Part 4 – Information Modeling Manual – IDEF1 Extended, 1 (IDEF1X) November 1985		same	2.4.3.2 IDEF1X97, Conceptual Schema Modeling, September 1997.	
				2.4.3.2 Unified Modeling Language (UML), Rational Corp., Version 1.0, January 1997	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.4.2.3 DoD Data Definitions	DoD Manual 8320.1-M-1, DoD Data Standardization Procedures, April 1998		DoD Manual 8320.1-M-1, DoD Data Element Standardization Procedures, January 1993	2.4.3.3 DoD 8320.1-compliant information exchange standards	
	Defense Data Dictionary System (DDDS)		Database-to-Database Exchange shall use standard data elements from DDDS, Version 3.2, May 1996 (previously mandated in Version 1.0, Section 4.2.4.2.3)		The DoD Data Model, used by the DDDS, is updated semi-annually (DDM is released in April and October) and data elements are updated dynamically as submitted by DoD Services, Agencies and Components.
	Secure Intelligence Data Repository (SIDR)				The DoD Data Model, used by the SIDR, is updated semi-annually (DDM is released in April and October) and data elements are updated dynamically as submitted by DoD Services, Agencies and Components.
2.4.2.3.1 DoD Date Standards	Calendar Date: DDDS Counter ID # 195 Format: YYYYMMDD (8-digit contiguous) Where: YYYY = year; MM = month; DD = day (Also referenced in ISO 8601, ANSI X3.30-1985, and FIPS PUB 4-1)				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	Ordinal Date: DDDS Counter ID # 165 Format: YYYYDDD (7-digit contiguous) Where: YYYY = year; DDD = ordinal day within year (Also referenced in ISO 8601)				
	Year Date: DDDS Counter ID #166 Format: YYYY (4-digit contiguous) Where: YYYY = year (Also referenced in ISO 8601)				
2.4.2.4.2.1 Bit-Oriented Formatted Messages	MIL-STD-6016, Tactical Digital Information Link (TADIL) J Message Standard, 7 February 1997		JTIDS Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 3 August 1994		
	STANAG 5516, Edition 1, Tactical Data Exchange - LINK 16, Ratified 15 January 1997		STANAG 5516, Edition 1, Tactical Data Exchange - LINK 16, Ratified 2 March 1990		
	Joint Interoperability of Tactical Command and Control Systems Variable Message Format (VMF) Technical Interface Design Plan (Test Edition) Reissue 2, August 1996		VMF Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 1 February 1995		
				2.4.3.4 STANAG 5522, Edition 1, Tactical Data Exchange - LINK 22 (Undated), distributed as ADSIA(DLWG)-RCU-C-74-95	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.4.2.4.2.2 Character-Based Formatted Messages	MIL-STD-6040, United States Message Text Format (USMTF), 1 January 1997		same		
2.4.3.1 Activity Modeling				IEEE P1320.1, IDEF0 Function Modeling	
2.4.3.2 Data Modeling				IDEF1X97, Conceptual Schema Modeling, September 1997.	
				Unified Modeling Language (UML), Rational Corp., Version 1.0, January 1997	
2.4.3.3 DoD Data Definitions				DoD 8320.1-compliant information exchange standards	
2.4.3.4 Information Exchange Standards				STANAG 5522, Edition 1, Tactical Data Exchange - LINK 22 (Undated), distributed as ADSIA(DLWG)-RCU-C-74-95	
				Multi-functional Information Distribution System (MIDS) System Specification, 11 April 1995.	

Human-Computer Interface Standards

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.5.2.1.1 Character-Based Interfaces	DoD HCI Style Guide, TAFIM Version 3.0, Volume 8, 30 April 1996		DoD HCI Style Guide, TAFIM Version 2.0, Volume 8, 30 September 1994		
2.5.2.2.1.1 X-Window Style Guides	Open Software Foundation (OSF)/Motif Style Guide, Revision 1.2 (OSF 1992)		same	2.5.3.Motif 2.1 Style Guide [published as part of CDE 2.1]	
	Triteal Enterprise Desktop (TED) 4.0 Style Guide and Certification Checklist, Carlsbad, CA: TriTeal Corporation, 1995				
2.5.2.2.1.2 Windows Style Guide	The Windows Interface Guidelines for Software Design, Microsoft Press, 1995		The Windows Interface: An Application Design Guide, Microsoft Press, 1992		
2.5.2.2.2 DoD Human-Computer Interface (HCI) Style Guide	DoD HCI Style Guide, TAFIM Version 3.0, Volume 8, 30 April 1996		DoD HCI Style Guide, TAFIM Version 2.0, Volume 8, 30 September 1994.		
2.5.2.2.3 Domain-level Style Guides	User Interface Specification for the Defense Information Infrastructure (DII), Version 2.0, June 1996		same		Version 1.0 had incorrectly cited "User Interface Specification for the Global Command and Control System (GCCS), October 1994" as the mandated standard in Appendix B

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.5.2.3 Symbology	MIL-STD-2525A, Common Warfighting Symbology, 15 December 1996				
2.5.3 Emerging Standards				Motif 2.1 Style Guide	Published as part of CDE 2.1

Information Systems Security Standards

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.6.2.2.1 Application Software Entity Security Standards	DoD 5200.28-STD, The Department of Defense Trusted Computer System Evaluation Criteria, December 1985		same		
	NCSC-TG-021, Version 1, Trusted Database Management System Interpretation, April 1991		same		
	FORTEZZA Application Implementers Guide, MD4002101-1.52, 5 March 1996		same		
	FORTEZZA Cryptologic Interface Programmers' Guide, MD4000501-1.52, 30 January 1996		same		
2.6.2.2.2.1 Data Management Services	NCSC-TG-021, Version 1, Trusted Database Management System Interpretation, April 1991		same		
2.6.2.2.2.2 Operating System Services Security	DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985		same		
2.6.2.2.2.2.1 Security Auditing and Alarms Standards	DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985		same		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.6.2.2.2.2.2 Authentication Security Standards	IETF RFC-1510, The Kerberos Network Authentication Service, Version 5, 10 September 1993		same		
	FIPS PUB 112, Password Usage, 30 May 1985		same		
				2.6.3.2.2.3 DCE Authentication and Security Specification (P315); Common Object Request Broker Architecture (CORBA), OMG 95-12-1, December 1995	
				2.6.3.2.2.2.2 IETF RFC 2138, Remote Authentication Dial In User Service (RADIUS), April 1997	
				IETF RFC-1938, A One-Time Password System, May 1996	
				2.6.3.3.1.1.2 FIPS PUB 196, Entity Authentication Using Public Key Cryptography, 18 February 1997, based on ISO/IEC 9798-3: 1993, Entity Authentication Using a Public Key System	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.6.2.3.1.1 Host Security Standards	FORTEZZA Interface Control Document, Revision P1.5, 22 December 1994		same		
			FORTEZZA Plus Interface Control Document, Release 3.0, 1 June 1995		
2.6.2.3.1.1.1 Security Algorithms	SKIPJACK, NSA, R21-TECH-044, 21 May 1991		FIPS PUB 180-1, Secure Hash Standard, NIST, April 1995		
	FIPS PUB 186, Digital Signature Standard, May 1994		same		
			FIPS PUB 185, Escrowed Encryption Standard, NIST, 9 February 1994		
	Key Exchange Algorithm, NSA, R21-TECH-23-94, 12 July 1994		same		
2.6.2.3.1.1.2 Security Protocols	MIL-STD-2045-48501, Common Security Label, 25 January 1995		same		
	ITU-T Rec. X.509 (ISO/IEC 9594-8.2), Version 3, The Directory: Authentication Framework, 1993		same		
	ACP-120, Allied Communications Publication 120, Common Security Protocol, CSP, 1997		MIL-STD-2045-18500, Message Handling System Message Security Protocol (MSP) Profile, October 1993.		Replaced MIL-STD-2045-18500.

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	SDN.903, revision 3.2, Secure Data Network System (SDNS) Key Management Protocol (KMP), 1 August 1989		same		
2.6.2.3.1.1.3 Evaluation Criteria Security Standards	DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985		same	2.6.3.2.1.1 ISO/IEC JTC1/SC27/WG3 N304, 23 April 1996, Evaluation Criteria for Information Technology Security (Common Criteria)	
	NCSC-TG-005, Version 1, Trusted Network Interpretation, July 1987		same		
2.6.2.3.2 Network Security Standards	SDN.301, Revision 1.5, Secure Data Network System (SDNS) Security Protocol 3 (SP3), 1989		same		
	MIL-STD-2045-48501, Common Security Label, 25 January 1995		same		

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.6.3.2.1.2 "The Transport Layer Security (TLS) Protocol, Version 1.0," Tim Dierks (Consensus Development), Christopher Allen (Consensus Development), 21 May 1997, draft-ietf-tls-protocol-03.txt, which incorporates the Secure Sockets Layer (SSL) Protocol Version 3.0, 18 November 1996	
				2.6.3.2.2.1.1 IETF RFC-1508, September 1993 (GSS-API); Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API), C. Adams, 25 March 1997, draft-ietf-cat-idup-gss-07.txt	Proposed Standard IETF RFC-2078 "GSS-API, Version 2.0," J. Linn, January 1997, revises RFC-1508.
				2.6.3.2.2.1.2 IEEE P1003.1e, POSIX Part 1: System API - Protection, Audit, and Control Interfaces [C Language], Draft 16, June 1997;	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.6.3.2.2.1.2 IEEE P1003.2c, POSIX Part 2: Shell and Utilities - Protection and Control Interfaces, Draft 16, June 1997	
				2.6.3.3.1.1.1 IEEE 802.10c/D13, Standard for Interoperable LAN Security-Part C: Key Management	
				2.6.3.3.1.1.1 IEEE 802.10g/D7, Secure Data Exchange – Security Label, 1995	
				2.6.3.3.2.1 IETF RFC-1825, Security Architecture for the Internet Protocol, August 1995	
				2.6.3.3.2.1 draft-ietf-ipsec-auth-05.txt, IP Authentication Header (AH), 30 May 1997	
				2.6.3.3.2.1 draft-ietf-ipsec-esp-04.txt, IP Encapsulating Security Payload (ESP), 30 May 1997	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.6.3.3.2.1 IETF RFC-2104, HMAC: Keyed-Hashing for Message Authentication, February 1997	
				2.6.3.3.2.1 IETF RFC-1829, The ESP DES-CBC Transform, August 1995	
				2.6.3.3.2.1 IETF RFC-2065, DNS Security Extensions, January 1997	
				2.6.3.3.2.1 draft-ietf-ipsec-isakmp-07.txt, Internet Security Association and Key Management Protocol (ISAKMP), 21 February 1997	
				2.6.3.3.2.1 draft-ietf-ipsec-isakmp-oakley-03.txt, The Resolution of ISAKMP with Oakley, February 1997	
				2.6.3.3.2.1 draft-ietf-ipsec-ipsec-doi-02.txt, The Internet IP Security Domain of Interpretation for ISAKMP, 28 February 1997	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.6.3.3.2.1 IEEE 802.10, IEEE Standards for Local and Metropolitan Area Networks (MANs): Interoperable LAN/MAN Security (SILS), 1992.	Incorporates IEEE 802.10b-1992 Secure Data Exchange Clause 2.
				2.6.3.3.2.1 IEEE 802.10a, Standard for Interoperable LAN Security - The Model, Draft January 1989	
				2.6.3.3.2.1 IEEE 802.10b, Secure Data Exchange, 1992	Incorporated into IEEE 802.10 –1992.
2.6.2.5 Human-Computer Interface (HCI) Security Standards	DoD Human-Computer Interface Style Guide, TAFIM, Version 3.0, Volume 8, 30 April 1996		DoD Human-Computer Interface Style Guide, TAFIM, Version 2.0, Volume 8, 30 September 1994		
				2.6.3.5 ISO/IEC JTC1/SC27/WG3 N304, 23 April 1996, Evaluation Criteria for Information Technology Security (Common Criteria)	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				2.6.3.5 FIPS PUB 196, Entity Authentication Using Public Key Cryptography, 18 February 1997, based on ISO/IEC 9798-3: 1993, Entity Authentication Using a Public Key System	
2.6.3.2.1.1 Evaluation Criteria Security Standards				ISO/IEC JTC1/SC27/WG3 N304, 23 April 1996, Evaluation Criteria for Information Technology Security (Common Criteria)	
2.6.3.2.1.2 World Wide Web Security Standards				"The Transport Layer Security (TLS) Protocol, Version 1.0," Tim Dierks (Consensus Development), Christopher Allen (Consensus Development), 21 May 1997, draft-ietf-tls-protocol-03.txt, which incorporates the Secure Sockets Layer (SSL) Protocol Version 3.0, 18 November 1996	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
2.6.3.2.2.1.1 Generic Security Service (GSS)-Application Program Interface (API) Security				IETF RFC-1508, September 1993 (GSS-API); Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API), C. Adams, 25 March 1997, draft-ietf-cat-idup-gss-07.txt	IETF RFC-2078 "GSS-API, Version 2.0," J. Linn, January 1997, revises RFC-1508.
2.6.3.2.2.1.2 POSIX Security Standards				IEEE P1003.1e, POSIX Part 1: System API - Protection, Audit, and Control Interfaces [C Language], Draft 16, June 1997	
				IEEE P1003.2c, POSIX Part 2: Shell and Utilities - Protection and Control Interfaces, Draft 16, June 1997	
2.6.3.2.2.2.1 Evaluation Criteria Security Standards				ISO/IEC JTC1/SC27/WG3 N304, 23 April 1996, Evaluation Criteria for Information Technology Security (Common Criteria)	
2.6.3.2.2.2.2 Authentication Security Standards				IETF RFC-1938, A One-Time Password System, May 1996	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				IETF RFC 2138, Remote Authentication Dial In User Service (RADIUS), April 1997	
2.6.3.2.2.3 Distributed Computing Services Security Standards				DCE Authentication and Security Specification (P315); Common Object Request Broker Architecture (CORBA), OMG 95-12-1, December 1995;	
2.6.3.3.1.1.1 Security Protocols				IEEE 802.10c/D13, Standard for Interoperable LAN Security-Part C: Key Management	
				IEEE 802.10g/D7, Secure Data Exchange – Security Label, 1995	
2.6.3.3.1.1.2 Public Key Infrastructure Security Standards				FIPS PUB 196, Entity Authentication Using Public Key Cryptography, 18 February 1997, based on ISO/IEC 9798-3: 1993, Entity Authentication Using a Public Key System	
2.6.3.3.2.1 Internetworking Security Standards				IETF RFC-1825, Security Architecture for the Internet Protocol, August 1995	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				draft-ietf-ipsec-auth-05.txt, IP Authentication Header (AH), 30 May 1997	
				draft-ietf-ipsec-esp-04.txt, IP Encapsulating Security Payload (ESP), 30 May 1997	
				IETF RFC-2104, HMAC: Keyed-Hashing for Message Authentication, February 1997	
				IETF RFC-1829, The ESP DES-CBC Transform, August 1995	
				IETF RFC-2065, DNS Security Extensions, January 1997	
				draft-ietf-ipsec-isakmp-07.txt, Internet Security Association and Key Management Protocol (ISAKMP), 21 February 1997	
				draft-ietf-ipsec-isakmp-oakley-03.txt, The Resolution of ISAKMP with Oakley, February 1997	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				draft-ietf-ipsec-ipsec-doi-02.txt, The Internet IP Security Domain of Interpretation for ISAKMP, 28 February 1997	
				IEEE 802.10, IEEE Standards for Local and Metropolitan Area Networks (MANs): Interoperable LAN/MAN Security (SILS), 1992. (Incorporates IEEE 802.10b-1992 Secure Data Exchange Clause 2)	
				IEEE 802.10a, Standard for Interoperable LAN Security - The Model, Draft January 1989	
				IEEE 802.10b, Secure Data Exchange, 1992	
2.6.3.5 Human-Computer Interface (HCI) Security Standards				ISO/IEC JTC1/SC27/WG3 N304, 23 April 1996, Evaluation Criteria for Information Technology Security (Common Criteria)	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				FIPS PUB 196, Entity Authentication Using Public Key Cryptography, 18 February 1997, based on ISO/IEC 9798-3: 1993, Entity Authentication Using a Public Key System	

Airborne Reconnaissance Subdomain Annex Standards

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFLED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
C4ISR.AR.2.2.2.1.2 Common Imagery Ground Surface System (CIGSS)	Common Imagery Ground/Surface System (CIGSS) Acquisition Standards Handbook, Version 1, 19 July 1995				The standards in this Handbook are mandated.
C4ISR.AR.2.2.2.2 SIGINT Information Processing	Joint Airborne SIGINT Architecture Standards Handbook, Version 2.0, 30 October 1997				The standards in this Handbook are mandated.
C4ISR.AR.2.3.2.2 Data Link Standards	System Specification for the CDL Segment, Specification #7681990, Revision D, 29 January 1997				
	System Description Document for CDL, Specification #7681996, 5 May 1993				
C4ISR.AR.3.1.2.1.1.3 Synthetic Aperture Radar	Kalman filtering for navigation and timing, as defined in Kalman, R.E., A new approach to linear filtering and prediction problems, Trans. ASME, Series D, J. Basic Eng., V. 82, March 1960				
C4ISR.AR.3.1.2.1.2 SIGINT	Joint Airborne SIGINT Architecture Standards Handbook, Version 2.0, 30 October 1997				The standards in this Handbook are mandated.

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFLED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
C4ISR.AR.3.1.2.1.3.1 Unattended MASINT Sensors	Interface Specification, Radio Frequency Transmission Interfaces for DoD Physical Security Systems, SEIWG-005, 15 December 1981				
C4ISR.AR.3.1.2.2.1 Timing	Telemetry Group, Range Commanders Council, Telemetry Standards, IRIG 106-96, Secretariat, Range Commanders Council, U.S. Army White Sands Missile Range, New Mexico, 21 March 1996				Chapter 4, Pulse Coded Modulation Standards, Chapter 8 - MIL-STD-1553, Department of Defense Interface Standard for Digital Time Division Command/Response Multiplex Data Bus
C4ISR.AR.3.1.2.2.2 Navigation, Geospatial	SNU-84-1, Revision D Specification for USAF Standard Form, Fit, and Function (F3) Medium Accuracy Inertial Navigation Unit (INS), 21 September 1992				
	ICD-GPS-200, Interface Control Document GPS (200), 1 July 1992				
C4ISR.AR.3.1.2.3 Airborne Platform-Internal Communications	MIL-STD-1553B, Notice 4, Department of Defense Interface Standard for Digital Time Division Command/Response Multiplex Data Bus, 15 January 1996				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFLED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	ANSI X3.184, Information Systems - Fiber Distributed Data Interface (FDDI) Single-Mode Fiber Physical Layer Medium Dependent (SMF-PMD) (100 Mb/s dual counter rotating ring), 1 January 1993				
	ANSI X3.230, Information Technology - Fiber Channel - Physical and Signaling Interface (FC-PH), (800 Mb/s), 1 January 1996				
C4ISR.AR.3.1.2.4 Air Vehicle/ Sensor Telemetry Mandates	Telemetry Group, Range Commanders Council, Telemetry Standards, IRIG 106-96, Secretariat, Range Commanders Council, U.S. Army White Sands Missile Range, New Mexico, 21 March 1996				Chapter 4, Pulse Coded Modulation Standards, Chapter 8 - MIL-STD-1553, Department of Defense Interface Standard for Digital Time Division Command/Response Multiplex Data Bus
C4ISR.AR.3.1.2.5 Mission Recorder Mandates	Compatibility with the published "AMPEX Digital Instrumentation Recorder DCRSi 240 User Manual"				
	ANSI X3.175, 19-mm Type ID-1 Recorded Instrumentation - Digital Cassette Tape Form, 1990, ID 1				
	Instrumentation Group (IRIG) B format as defined in IRIG Document 104-70, August 1970				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFLED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
C4ISR.AR.3.2.2.1 Collection Management Mandates	FIPS PUB 10-4: April 1995, Countries, Dependencies, Areas of Special Sovereignty, Municipal Divisions				
C4ISR.AR.3.2.2.2 Mission Planning Mandates	TCS RPP Software Requirements Specification, Version 1.0, 14 November 1997 (TCS Document Control Number: TCS-303)				
	The Tactical Control System (TCS) Flight Route Plan to Tactical Control System, Version 1.0 Interface Design Description (IDD), 1 October 1997 (TCS Document Control Number: TCS-244)				
C4ISR.AR.3.2.2.3 Mission Control Mandates	Tactical Control System (TCS) Software Design Description (SDD) 117, Version 1.0, 31 March 1997 (TCS Document Control Number: TCS-117)				
	TCS JII 2, Tactical Control System Joint Interoperability Interface 2 (JII 2) - Tactical Control System to Service Command, Control, Communications, Computers and Intelligence (C4I) Systems, Version 1.0, 9 May 1997 (TCS Document Control Number: TCS-233)				
	TCS IDD 229, Tactical Control System Segment to Air Vehicle Standard Segment Interface (TCS AVSI) Interface Design Description (IDD), Version 1.2, 29 August 1997 (TCS Document Control Number: TCS-229)				

Combat Support Domain Annex Standards

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
CS.2.2.1 Document Interchange	MIL-PRF-28001C, Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text (CALS SGML), 2 May 1997				
	MIL-STD-1840C, Automated Interchange of Technical Information (AITI), 26 June 1997				
CS.2.2.2 Graphics Data Interchange	ANSI/ISO 8632, as profiled by MIL-PRF-28003A, CGM Application Profile, with Amendment 1, 14 August 1992				
	MIL-PRF-28002C, Requirements for Raster Graphics Representation in Binary Format, 30 September 1997				
	NEMA/ACR DICOM V3.0, parts 1-12, Digital Imaging and Communication in Medicine, 1993				
CS.2.2.3 Product Data Interchange	FIPS PUB 177-1, IGES, adopts CALS IGES and ANSI/US PRO-100-1993, V5.2, 23 April 1996				
	MIL-PRF-28000A with Amendment 1, Digital Representation for Communications of Product Data: IGES Application Subsets and IGES Application Protocols, 14 December 1992				
	ISO/IEC 10303-1:1994, Standards for the Exchange of Product Model Data (STEP), Part 1: Overview and Principles				
	MIL-STD-2549, Configuration Management Data Interface, 30 June 1997				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	MIL-STD-1840C, Automated Interchange of Technical Information, 26 June 1997				
	AIM BC1, Uniform Symbology Specification Code 39				
CS.2.2.4 Electronic Data Interchange	FIPS PUB 161-2, Electronic Data Interchange (EDI) adopts, with specific conditions ANSI ASC X12, UN/EDIFACT and ANSI HL7, 22 May 1996	ANSI ASC X12 Electronic Data Interchange (ASC X12S 97-372 is latest edition); ANSI HL7 Version 2.3; ISO/UN/EDIFACT			
CS.2.3 Information Transfer Standards				CS.2.3 IEEE 1073, Protocol for Medical Device Communications, 1996	New Service Area

Automatic Test System Subdomain Annex Standards

JTA SECTION & SERVICE AREAS	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
CS.ATS.2.2.2.1 Instrument Driver API Standards				VXI*plug&play* Systems Alliance Instrument Driver Functional Body Specification VPP-3.2, Revision 4.0, 2 February 1996	
CS.ATS.2.2.2.2 Digital Test Data Formats				NAWCADLKE-MISC-05-PD-003, Navy Standard Digital Simulation Data Format (SDF), January 1998	
CS.ATS.2.2.2.3 Generic Instrument Class Standards				IEEE 1226 ABBET Trial-Use Standard for a Broad-Based Environment for Test (ABBET) Overview and Architecture, 1993	New Service Area
				VXI*plug&play* Systems Alliance	New Service Area
CS.ATS.2.2.2.4 Diagnostic Processing Standards				IEEE 1232.1, Artificial Intelligence Exchange and Services Tie to All Test Environments (AI-ESTATE) Data and Knowledge Specification, 1997	New Service Area

JTA SECTION & SERVICE AREAS	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
CS.ATS.2.2.2.5 Adapter Function and Parametric Data Standards				IEEE P1226.11 ABBET Test Resource Information Model (TRIM)	New Service Area
CS.ATS.2.2.2.6 ATS Instrument Function and Parametric Data Standards				IEEE P1226.11 ABBET TRIM	New Service Area
CS.ATS.2.2.2.7 ATS Switching Function and Parametric Data Standards				IEEE P1226.11 ABBET TRIM	New Service Area
CS.ATS.2.2.2.8 UUT Test Requirements Data Standards				IEEE P1226.11 ABBET TRIM	New Service Area
CS.ATS.2.2.2.9 TPS Documentation Standards				DI-ATTS-80284A, Test Program Set Document	New Service Area
				DI-ATTS-80285A, Engineering Support Data	New Service Area

JTA SECTION & SERVICE AREAS	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
CS.ATS.2.3.2.1 Data Networking Standards				Any hardware that has support for the software protocol standards specified in JTA Section 2.3.2.1.1.2.1.1, Transmission Control Protocol (TCP), and JTA Section 2.3.2.1.1.2.1.3, Internet Protocol (IP)	
CS.ATS.2.3.2.2 Instrument Communication Manager Standards				VXI*plug&play* (VPP) Systems Alliance Virtual Instrument Standard Architecture (VISA) Library, VPP-4.3, 22 January 1997	
CS.ATS.3.1.2.1 Test Program to Operating System Calls				Any element of the technical architecture that is implemented shall not be bypassed by a direct communication to another interface or layer further on in the process	
CS.ATS.3.3.2.1 System Framework Standards				VXI*plug&play* System Alliance System Frameworks Specification, VPP-2, Revision 4.0, 29 January 1996	

Modeling and Simulation Domain Annex Standards

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
M&S.2.2.2.1 HLA Rules	High Level Architecture Rules, Version 1.3, February 1998				
M&S.2.2.2.2 HLA Interface Specification	High Level Architecture Interface Specification, Version 1.3, February 1998				
M&S.2.2.2.3 HLA Object Model Template Specification	High Level Architecture Object Model Template, Version 1.3, February 1998				
M&S.2.4.2.1 Federation Execution Details Data Interchange Format (FED DIF)	Federation Execution Details Data Interchange Format, Version 1.3, February 1998				
M&S.2.4.2.2 Object Model Template Data Interchange Format	Object Model Template Data Interchange Format (OMT DIF), Version 1.3, February 1998				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
M&S.2.4.2.3 Standard Simulator Database Interchange Format (SIF)	MIL-STD-1821, Standard Simulator Data Base (SSDB) Interchange Format (SIF) Design Standard, 17 June 1993, with Change Notice 1, 17 April 1994, and Change Notice 2, 17 February 1996			M&S 2.4.3.1 Synthetic Environment Data Representation and Interchange Specification (SEDRIS) Interchange Specification (Draft), April 1998	
M&S.2.4.3.2 Object Model Data Dictionary				M&S 2.4.3.2 Object Model Data Dictionary Version 1.3 (Build 2) 16 March 1998.	New Service Area. Previously addressed by IEEE 1278.1.

Weapons Systems Domain Annex Standards

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
WS.2.2.2.2.1 Operating System Services				IEEE P1003.5c/D3 POSIX - Part 1: Binding for API – Amendment 2: Protocol Independent Interfaces, October 1997	
				IEEE P1003.5f POSIX: Ada binding to 1003.21, January 1997	
				IEEE P1003.1e/D15 POSIX: Protection Audit and Control Interface (C Language), December 1995	
				IEEE P1003.22/D6 POSIX - Open System Security Framework, August 1995	
WS.2.4.1 Emerging Standards (Information and Data Exchange)				IEEE 1076, Standard VHSIC Hardware Description Language (VHDL) Reference Manual, 1993	
				IEEE 1076.2 VHDL Mathematical Package, 1996	
				IEEE 1076.3 Standards VHDL Synthesis Package, 1997	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				IEEE 1076.4, VITAL Application-Specific Integrated Circuit (ASIC) Modeling Specifications, 1995	It provides VITAL timing and primitives.
WS.2.5.2 Emerging Standards (HCI)				U.S. Army Weapon Systems Human-Computer Interface (WSHCI) Style Guide, Version 1.0, 30 September 1996	
WS.3.1.2.1 Emerging General Standards				IEEE P996.1/D1, Compact Embedded PC Modules, October 1993	
				IEEE P1386.1/D2.0, Physical/Environmental Layers for Peripheral Component Interface (PCI) Mezzanine Cards, PMC, April 1995	
				ATSC Document A/53, ATSC Digital Television Standard, 16 September 1995	
				IEC 1158/ANSI 850, Fieldbus Standard, 1996	

Aviation Subdomain Annex Standards

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
WS.AV.2.2.2.2 Operating System Services				SAE xxx: Operating System API for Ada Run Time System	Maps to 2.2.2.2.1.7 in the core
WS.AV.2.5.2 Emerging Standards				MIL-STD-1787, Aircraft Display Symbology, Revision B, 5 April 1996	Maps to 2.5.2.3 in the core
WS.AV.3.1.2 Emerging Standards				MIL-STD-1553B, Standard for Medium Speed System Network Bus, 21 September 1978, with Notice of Change 1, 12 February 1980, Notice of Change 2, 8 September 1986, Notice of Change 3, 31 January 1993, and Notice of Change 4, 15 January 1996	
				ANSI/VITA 1, VME64 Specification, 1994	

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
				MIL-STD-1773, Fiber Optics Mechanization of an Aircraft Internal Time Division Command/Response Multiplex Data Bus, 20 May 1988, with Notice of Change 1, 2 October 1989	
WS.AV.3.1.1.1.2 General Hardware Interface Standard				MIL-STD-1389D, Design Requirements for Standard Electronic Module (SME), 30 March 1989	

Ground Vehicle Subdomain Annex Standards

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
WS.GV.3.1.1.1.1 Bus Interface Standards	MIL-STD-1553B, Standard for Medium Speed System Network Bus, 21 September 1978, with Notice of Change 1, 12 February 1980, Notice of Change 2, 8 September 1986, Notice of Change 3, 31 January 1993, and Notice of Change 4, 15 January 1996				
	ANSI/VITA 1, VME64 Specification, 1994				
	SAE J 1850, Class B Data Communication Network Interface, 1 July 1995				
	ANSI X3.131, Information Systems - Small Computer Systems Interface - 2 (SCSI-2), 1994				
WS.GV.3.1.1.1.2 General Hardware Interface Standards	Personal Computer Memory Card International Association (PCMCIA), PC Card Standard, March 1997				
	IEEE 1101.2, Standard for Mechanical Core Specifications for Conduction-Cooled Eurocards (ANSI), 1992				
	EIA 170, Electrical Performance Standards - Monochrome Television Studio Facilities, November 1957				

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
	EIA 330, Electrical Performance Standards for Closed Circuit Television Camera 525/60 Interlaced 2:1 (ANSI/EIA 330-68), November 1966				
	EIA 343-A, Electrical Performance Standard for High Resolution Monochrome Closed Circuit Television Camera (November 1966), September 1969				
	SMPTE 170M, Television - Composite Analog Video Signal - NTSC for Studio Applications, 1994				
WS.GV.3.1.2 Emerging Standards				WSGV.3.1.2 PCI Industrial Computer Manufacturer's Group (PICMG): Compact PCI Specification, R2.1, September 1997	New Hardware Interface Standard.

Missile Defense Subdomain Annex Standards

JTA SECTION & SERVICE AREA	CURRENTLY MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED	PREVIOUSLY MANDATED STANDARD	EMERGING STANDARD	COMMENTS
WS.MD.2.2.3.1 Navigation Standard				BMD-P-SD-92-000002-A, Ballistic Missile Defense (BMD) Navigation Standard, Ballistic Missile Defense Organization, 23 June 1993	Maps to 2.2.2.2.1.4.3 in the core.
WS.MD.2.4.2 Emerging Standards				Interface Change Proposal (ICP) TJ93-096 Ch9, commonly called the "Space Track Message," Ballistic Missile Defense Organization, 26 September 1997	Maps to 2.4.2.4.2.1 in the core.

This page intentionally left blank.

B.3 DOCUMENT SOURCES

Commercial Documents

Organization	Source Location	URL
ANSI	American National Standards Institute, Attention Customer Service, 11 West 42nd St., New York, NY 10036 USA Tel: +1 212 642 4900.	http://www.ansi.org
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.ch
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
EIA	Electronics Industries Association Global Engineering Documents 7730 Carondelet Ave., Suite 407 Clayton, MO 63105 USA Tel: +1 800 854 7179	http://global.ihs.com
IAB	Internet Architecture Board (IAB) documents are available from Internet Engineering Task Force (IETF). See the IETF entry for source location information.	
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://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 ftp://ds.internic.net
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/publication/catalog
OMG	Information about the Object Management Group (OMG) is available from the OMG Web site.	http://www.omg.org
OSF	Open Systems Foundation (OSF), X/Open, and Open Group documents may be obtained from: Open Group, Apex Plaza Foxbury Road Reading, RG1 1AX England Tel: +44 118 9 508311 Fax: +44 118 9 500110	http://www.opengroup.org/public/pubs/catalog/dc.htm
RFC	See IETF	
SAE	Society of Automotive Engineers	http://www.sea.org/PRODSERV/STANDARD/standard.htm
SR	Bellcore Special Report Tel: +1 800 521 2673	http://www.bellcore.com/NIC/platform.htm
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
UML	Information about Unified Modeling Language (UML) can be obtained at the Rational Corporation Web site.	http://www.rational.com
VXI*plug&play*	System Alliance 6504 Bridge Point Parkway Austin, TX 78730 USA	http://www.tek.com
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.org
X/Open	See OSF	

Government Documents

Organization	Source Location	URL
C2CDM	Command and Control Core Data Model (C2CDM) information may be obtained from the referenced URL.	http://www-datadmn.itsi.disa.mil
DDM	DoD Defense Data Model (DDM) Information may be obtained from the referenced URL.	http://www.datadmn.itsi.disa.mil
DCA	Defense Communications Agency is now called Defense Information Systems Agency (DISA). See the DISA entry for source location information.	N/A
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.itsi.disa.mil Take path: DoD Data Administration (DATADMN)
DDM	Information regarding access to the Defense Data Model (DDM) and the C2CDM can be obtained from the DoD Data Administration web page at the referenced URL.	http://www-datadmn.itsi.disa.mil
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
DoD-HDBK	See MIL STD	http://www-library.itsi.disa.mil
DoD-STD	See MIL STD	http://www-library.itsi.disa.mil
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
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://antd.nist.gov/fededi

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
ITSG	The Information Technology Standards Guidance (ITSG) may be obtained from the DISA Center for Standards (CFS) web page.	http://www.itsi.disa.mil Take path: Info Tech Stnds Guidance (ITSG) Ver 3.1
JTA	Information about the the Joint Technical Architecture document can be obtained from the JTA web site.	http://www-jta.itsi.disa.mil/jta.html
MIL-HDBK	See MIL STD	http://www-library.itsi.disa.mil
MIL-STD	Copies of military standards (MIL STD, DoD STD), and handbooks (MIL HDBK, DOD HDBK) are available from: DoD Single Stock Point (DoDSSP) - Customer Service Standardization Document Order Desk 700 Robbins Avenue, Bldg. 4D, Philadelphia, PA 19111-5094 USA. Tel: +1 215 697 2667/2179 (M-F, 7:30 AM-4:00 PM)	http://www-library.itsi.disa.mil
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	http://www.nsa.gov
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/nawcad
NCSC	The Rainbow Series of documents from the National Security 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
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.ntis.gov/search.htm

Organization	Source Location	URL
STANAG	STANAG's 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.	N/A
TAFIM	Technical Architecture Framework for Information Management (TAFIM) information may be obtained from the TAFIM Support Line at the referenced URL.	http://www.itsi.disa.mil
TIDP	Technical Interface Design Plans (TIDPs) may be obtained via the service POC's to the Joint Multi-TADIL CCB from: DISA/JIEO Center for Standards (CFS) TADIL Division, code JEBCA, Tel: +1 703 735 3524 Email: shermans@ncr.disa.mil	
USIGS	The United States Imagery and Geospatial Information System (USIGS) is an umbrella term for the suites of systems formerly called the United States Imagery System (USIS) and the Global Geospatial Information and Services (GGIS). Information related to standards can be found on: the NIMA web page, or contact NIMA: Tel: 301 227 3554 E-Mail: wesdockj@nima.mil	http://www.nima.mil/aig/aigteams.html
USIS	See USIGS	
VTC001	Industry Profile for Video Teleconferencing may be obtained from: Defense Information Systems Agency (DISA) Joint Interoperability and Engineering Organization (JIEO) code JEBBC Fort Monmouth, NJ 07703 USA	http://multi.nosc.mil/profile.htm
Y2K	DoD policy guidance on Year 2000 (Y2K) compliance can be found in the "DoD Year 2000 Management Plan." The plan is available at the referenced URL . For procurement and acquisition purposes, the General Services Administration (GSA) has made the following documents available on its Web site: "recommended Year 2000 Contract Language (11 September 1996)" and "Federal Acquisition Regulation Interim Rule on the Year 2000 (2 January 1997)."	http://www.dtic.mil/c3i http://www.itpolicy.gsa.gov/

This page intentionally left blank.

APPENDIX C: JTA RELATIONSHIP TO DOD STANDARDS REFORM

C.1 DOD (SPECIFICATIONS AND) STANDARDS REFORM - BACKGROUND

The DoD Standards Reform was begun in June 1994 when the Secretary of Defense issued his memorandum entitled "Specifications and Standards - A New Way of Doing Business." the Secretary of Defense directed that performance-based specifications and standards or nationally-recognized private sector standards be used in future acquisitions. The intent of this initiative is to eliminate non-value added requirements, and thus to reduce the cost of weapon systems and materiel; remove impediments to getting commercial state-of-the-art technology into our weapon systems; and integrate the commercial and military industrial bases to the greatest extent possible. The Defense Standards Improvement Council (DSIC) directs implementation of the Reform. The DSIC has interpreted and extended the Reform policy through a series of numbered OSD policy memos. These policy memos and other DSIC decisions, newsletters and other standardization related information are posted on the Defense Standardization Program (DSP) World Wide Web home page at:

http://www.acq.osd.mil/dsp.

C.2 THE JTA AND THE DOD STANDARDS REFORM

The standards and specifications and other standardization documents identified in the Joint Technical Architecture (JTA) can be cited in solicitations without conflicting with the DoD Standards Reform. All JTA standards have been granted Department-wide exemption from the waiver requirement by the Defense Standards Improvement Council. Mandatory application of JTA standards to acquisition solicitations is authorized. Contrary to interpretations that have been made in the recent past by some DoD organizations, the DoD Standards Reform is not eliminating military standards and specifications nor precluding their use. What the Reform is trying to eliminate is the automatic development and imposition of military-unique standards and specifications as the cultural norm. The JTA calls out non-Government standards in every case where it makes sense and where it will lead to the use of commercial products and practices that meet the DoD's needs. The JTA only calls out Military and Federal standards and specifications in those instances where no non-Government standard exists that is cost effective and meets the requirement or where the use of the non-Government standard must be clarified to enable interoperability of DoD systems.

C.3 REFORM WAIVER POLICY

Policy Memo 95-1 establishes procedures for waivers for use of specifications and standards cited as requirements in solicitations. These waiver procedures apply to the types of standards that fall under the province of the Defense Standardization Program and are indexed in the DoD Index of Standards and Specifications (DoDISS). Specifically of relevance to the JTA, Policy Memo 95-1 states that non-Government standards, Interface Standards, Federal Information Processing Standards (FIPS), and Performance Specifications do not require waivers. Also, Policy Memo 95-9 provides that international standardization agreements such as NATO STANAGs (and ACPs) do not require waivers. Federal Telecommunications Standards (FED-STDs) do not require a waiver when they qualify as interface standards. All of the above waiver-free document types encompass most of the standards cited in the JTA. The DSP Home Page provides lists of waiver-free standards and in the near future the DoDIIS will indicate those standards that can be used without a waiver.

C.4 NON-DODISS STANDARDS NOT SUBJECT TO THE REFORM WAIVER POLICY

There are a small number of JTA standards that are not among the types of Government standards that are indexed in the DoDISS and are therefore not subject to the Reform waiver policy. Therefore, they also do not require a waiver to be cited in a solicitation. (An example of a JTA document of a type that is not indexed in the DoDISS is DoD 5200.28-STD.) However, the citation of these non-DoDISS standards in solicitations must comply with Service/Agency requirements for preparation and approval of performance-based program unique specifications. A system specification used to procure a C4I system or a weapon system is a program unique specification. Procedures for preparing performance specifications are provided in MIL-STD-961D, Defense Specifications, Change 1, 22 August 1995 and in the DSP Performance Specification Guide, SD-15, dated 29 June 1995. MIL-STD-961D defines a performance specification as follows: "A specification that states requirements in terms of the required results with criteria for verifying compliance, but without stating the methods for achieving the required results. A performance specification defines the functional requirements for the item, the environment in which it must operate, and interface and interchangeability characteristics." By this definition, standards that define "interface" characteristics can be properly cited in a performance specification. Therefore, JTA non-DoDISS standards that are used to define interface characteristics are not in conflict with service/agency requirements for preparation and approval of performance-based program unique specifications.

C.5 INTERFACE STANDARDS ARE WAIVER-FREE

Most JTA standards qualify as Interface Standards. Policy Memo 95-6 defines the five types of DoD-prepared standards as: interface standards, standard practices, test method standards, manufacturing process standards, and design criteria standards. Policy Memo 95-1 states that of these types, interface standards and standard practices do not require a waiver when cited in a solicitation. MIL-STD-962C (a standard practice) provides definitions, format, and content direction for military standards. It defines an interface standard as follows: "A standard that specifies the physical, functional, or military operational environment interface characteristics of systems, subsystems, equipment, assemblies, components, items or parts to permit interchangeability, interconnection, interoperability, compatibility, or communications." The use of military and Federal interface standards in solicitations is fully compliant with the DoD Standards Reform.

C.6 NON-GOVERNMENT STANDARDS VS. MILITARY/FEDERAL STANDARDIZATION DOCUMENTS

One of DoD's key acquisition reform goals is to reduce acquisition costs and remove impediments to commercial-military integration by emulating commercial buying practices wherever possible. Thus, for any processes, practices, or methods that are described by a non-Government standard used by Commercial firms and which meet DoD's needs, DoD activities should also be using a non-Government standard instead of applying, developing, or revising a military or Federal Standard. The standards selected for the JTA are predominantly non-Government standards. Military or Federal standards have been selected for the JTA only in those instances where non-Government standards failed to satisfy the DoD needs. In most of those instances, in fact, the military or Federal standard is a profile of one or more non-Government standards. The military or Federal profile identifies the chosen classes, subsets, options, and parameters of one or more base standards necessary for achieving interoperability (or other function). In some instances, the profile specifies unique interface requirements not satisfied by the non-Government standard. Therefore the JTA complies fully with this key acquisition reform goal.

APPENDIX A - ACRONYMS AND GLOSSARY

APPENDIX B – LIST OF MANDATED STANDARDS AND SOURCES

APPENDIX C – JTA RELATIONSHIP TO DoD STANDARDS REFORM

This page intentionally left blank.