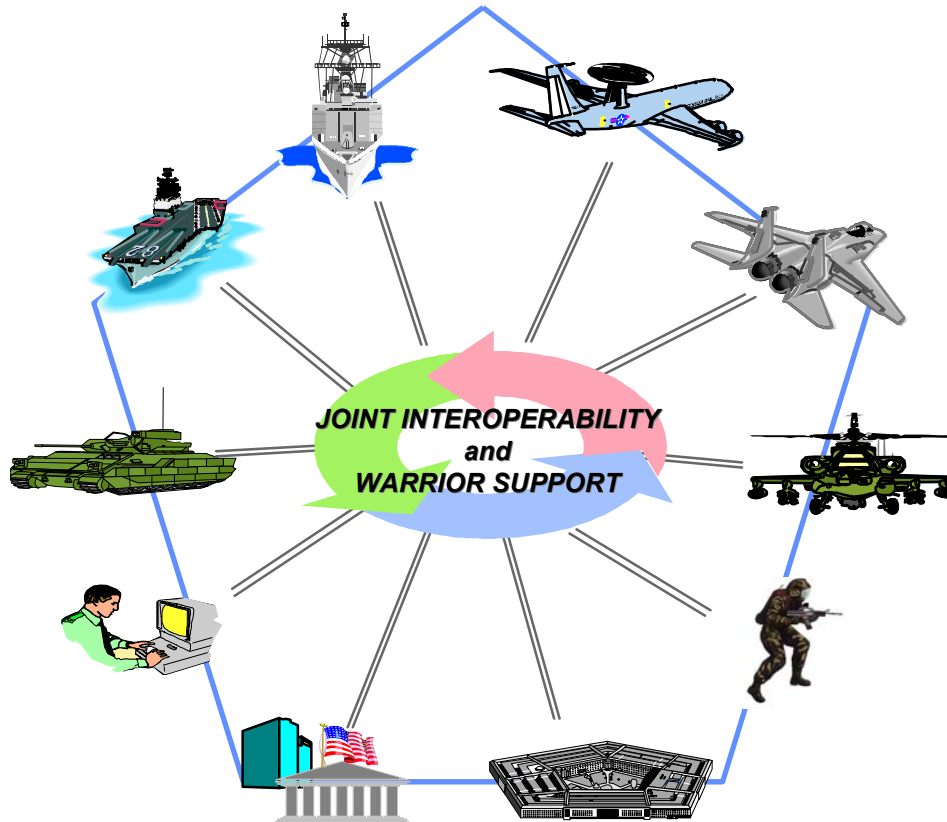


Department of Defense  
**Joint Technical Architecture User  
Guide and Component JTA  
Management Plan**



**Version 1.0**  
**14 September 2001**

---

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

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

---

**Send any comments and suggestions via electronic mail to: [jta@www.disa.mil](mailto:jta@www.disa.mil)**

## Table of Contents

<b>1. Purpose</b> .....	<b>1</b>
<b>2. Scope</b> .....	<b>1</b>
<b>3. Intended Audience</b> .....	<b>1</b>
<b>4. Joint Technical Architecture</b> .....	<b>1</b>
4.1. JTA Terminology and Organization .....	2
4.2. Definitions .....	3
<b>5. JTA Relationships with other DoD Programs</b> .....	<b>4</b>
5.1. C4ISR Architecture Framework .....	5
5.2. Global Information Grid (GIG) .....	6
5.3. DoD Technical Reference Model .....	6
5.4. Defense Information Infrastructure Common Operating Environment .....	6
5.5. Component-Specific Technical Architecture .....	7
<b>6. Relationship of JTA to Acquisition Planning Documents</b> .....	<b>7</b>
6.1. Mission-Needs Statement .....	7
6.2. Capstone/Operational Requirements Document .....	7
6.3. C4I Support Plan .....	7
6.4. Requests for Proposal .....	8
6.5. Contract Statement of Work .....	8
<b>7. Applying the JTA to Systems</b> .....	<b>8</b>
7.1. Service Areas and Standards Profiles .....	8
7.2. Building a Standards Profile .....	9
<b>8. System Migration</b> .....	<b>10</b>
8.1. Selecting the Migration Plan .....	10
8.2. Migrating Legacy Systems Requiring an Upgrade .....	10
8.3. Migration Strategy .....	10
8.4. Applying the JTA to the SBA Process .....	12
8.5. Additional Guidance .....	12
<b>9. DoD Interoperability Policy and Compliance</b> .....	<b>13</b>
9.1. Use of the Current Versions of the JTA .....	14
9.2. Compliance and JTA Metrics .....	14
9.3. Waiver Process .....	15
9.4. Component JTA Management Plans .....	16
9.5. User Selection Standards and Specifications .....	16
<b>10. Contract Language</b> .....	<b>16</b>
10.1. Statement of Work Language .....	16
10.2. System Requirements Specification Language .....	19
10.3. Request for Proposal Language .....	19
<b>Appendix A</b> .....	<b>21</b>
<b>Appendix B</b> .....	<b>25</b>

Page intentionally left blank.

## **DoD Joint Technical Architecture (JTA) User Guide and Component JTA Management Plan**

### **1. Purpose**

The purpose of this User and Management Plan Guide is to provide information and guidance to acquisition executives, requirements developers, program managers, systems architects, and other stakeholders who need to know how to:

- Interpret the Department of Defense (DoD) Joint Technical Architecture (JTA) mandates
- Select standards from the JTA to demonstrate JTA compliance and to build a Technical Architecture (TA) profile
- Implement the DoD JTA mandates for their programs
- Perform compliance assessments against the DoD JTA for impacts on future implementations.

### **2. Scope**

The User Guide and Management Plan was developed to help explain the structure and rationale for the organization of the JTA. It addresses how and when to use a mandated or emerging standard, related DoD policies, and JTA compliance guidelines. It explains how to use the JTA in the development of new systems, and it provides a methodology for migrating existing legacy systems undergoing major upgrades into compliance with the JTA. In addition, Service and Agency implementation plans are discussed, as well as the subject of waivers. While this document applies specifically to the JTA Version 4.0, most of the guidance can also be applied to earlier versions.

### **3. Intended Audience**

Users of the JTA in the DoD components, unified combatant commands, combined operations, and warfighters include:

- Development Managers
- Chief Engineers
- Information Technology (IT) Professionals
- Systems Analysts
- System Engineers
- Development Contractors
- Program and Project Managers
- JTA Development Community
- Domain Architects
- System Acquisition Community
- System and or Technology Development/Industry

### **4. Joint Technical Architecture**

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 consensus on 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 baseline to move toward interoperability.” This document is the JTA.

The DoD JTA guides the acquisition and development of new and emerging systems in the selection of IT functionality. The JTA identifies only the minimum set of mandated and emerging standards that are critical to interoperability.

The standards contained in the JTA are based upon commercial open systems technology that is strongly supported in the commercial marketplace. The JTA considers the following criteria for mandating a standard:

- The standard promotes interoperability by enhancing joint or combined Service/Agency information exchange and support joint activities.
- The standard demonstrates maturity through technical stability and strong support in the marketplace, and maintenance by a recognized organization.
- The standard can be technically implemented.
- Wide distribution and adoption of the standard demonstrates that it is publicly available (with at least three products openly available).
- The standard is consistent with authoritative sources such as laws, regulations, policy, and guidance documents.

#### **4.1. JTA Terminology and Organization**

Proper use of the JTA requires an understanding of the terminology associated with it and a determination made of the JTA applicability to a program or system at the outset.

Each section of the JTA main body, except for the overview, includes background descriptions and definitions that apply to the specific mandated and emerging standards in that section. Figure 1 illustrates the relationships between the JTA Core and its domains.

As the JTA evolves, the standards in the JTA Core, domains, and subdomains are revisited and updated from time to time to ensure correctness. The JTA normalization rules in this section address the movement of elements from subdomain to domain, and from domains into the Core. All standards are placed in the Core unless they are justified as unacceptable to meet domain-specific requirements. When Core standards cannot meet the requirements of a specific domain they are removed from the JTA Core and placed in the appropriate domain. Likewise, when domain standards cannot meet subdomain-specific requirements, those will be removed from the domain and placed in the appropriate subdomain. The intent of the above normalization rules is as follows: (1) The Core applies to all DoD systems; (2) the JTA Core contains selected standards for as many JTA services as possible; and (3) the JTA provides the minimum number of standards for a specified service or interface.

As necessary, each domain and subdomain provides a list of domain-specific standards and guidance in a format consistent with the JTA Core. Subdomain developers define which standards apply to which system interfaces in their domain or subdomain.

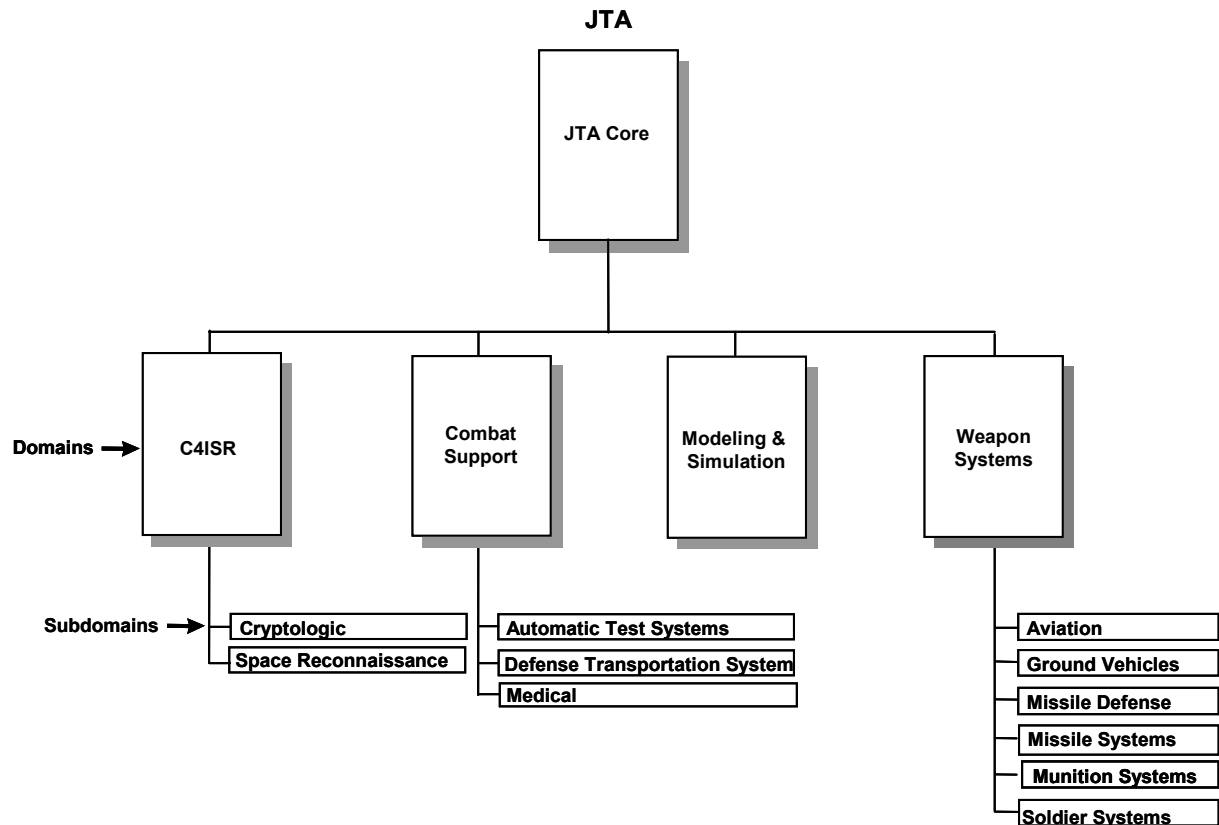


Figure 1: JTA Hierarchy Model

#### 4.2. Definitions

The following are commonly used terms used in this document:

- **Compliance** – means that a system implements all of the applicable DoD JTA standards.
- **User** – is any organization responsible for systems (acquisition or operation), program operation, or sustainment function providing JTF or CINC support in any Service Area identified in the DoD JTA Core, Domains and associated Subdomains.
- **JTA Core** – The DoD JTA is organized into a main body, called the JTA Core, followed by four domains (including their subdomains) and a set of appendices. Listed below are the major service areas contained in JTA Core:
  - a. **Information Processing Standards.** Identifies standards used in user interface, data management, data interchange, graphics, communications, operating system, internationalization, and distributed computing service areas.
  - b. **Information Transfer Standards.** Identifies standards used in communications and system management and service areas applicable to both system and network management.

- c. **Information Modeling, Metadata, and Information Exchange Standards.** Addresses standards for an area supported by engineering support, data management, and software engineering services in the DoD Technical Reference Model (TRM).
  - d. **Human-Computer Interface Standards.** Identifies standards used for information entry and display, complementing the standards cited for user interface.
  - e. **Information Security Standards.** Identifies security-related standards that cut across the previously mentioned service areas.
- **Base Service Area.** A base service area is a further breakdown of the Major Service Areas identified by the DoD Technical Reference Model (TRM). It is a minimum set of functionality for which a standard or standards can be applied. Each base service area in the JTA contains at least one mandated or emerging standard.
  - **Domain.** Represents a family of related systems sharing additional common functional, behavioral, and operational requirements. Each domain addresses the service areas, interfaces, and standards that support interoperability across systems within the family of systems.
  - **Subdomains.** Subsets of a domain that have special interoperability requirements specific to that smaller group of systems. The intention is that a system within a specific subdomain adopt the JTA elements contained in the relevant subdomain, the standards contained in the parent domain, and the relevant standards in the JTA Core.
  - **Mandated Standards.** These are specifications that must be used for the acquisition of all DoD systems that produce, use, or exchange information. Mandated standards are clearly identified in the JTA as a separate item, indented and preceded by a bullet (●). They are formal reference citations that have met the criteria identified in Section 1 of the JTA. Briefly, these criteria state that a standard must promote interoperability, be technically mature and implementable, be publicly available, and be consistent with authoritative sources. These standards citations are suitable for inclusion within Requests for Proposals (RFPs), Statements of Work (SOWs), or Statements of Objectives (SOOs).
  - **Emerging Standards.** Are described as candidates to potentially become JTA mandates. An emerging standard is clearly identified as a separate item indented and preceded by a dashed (–) line. Listing emerging standards is intended to help a user (e.g., a program manager or a systems architect) determine those areas likely to change in the near term (within 3 years). This also suggests areas in which “upgradability” should be a concern. JTA developers expect emerging standards to be elevated to a mandatory status when implementations of the standards mature. Emerging standards can be implemented but shall not be used in lieu of a mandated standard.
  - **System Migration.** For the purposes of this document, Systems Migration is defined as the evolution of an existing capability, program or system, not based on DoD JTA standards including Defense Information Infrastructure (DII) Common Operating Environment (COE) products to a capability based on those standards and/or products.

## 5. JTA Relationships with other DoD Programs

Recent Government legislation is placing more emphasis on the need to pursue interoperable, integrated, and cost-effective business practices and capabilities within each organization and across DoD, particularly with respect to information technology. Two legislative acts that impact DoD architecture analysis and integration activities are the Information Technology Management Reform Act (ITMRA), also known as the Clinger-Cohen Act of 1996, and the Government Performance and Results Act (GPRA) of 1993. Together, the ITMRA and GPRA serve to codify the efficiency, interoperability, and leveraging goals being pursued by the Commands, Services, and Agencies of



DoD. The ITMRA and the GPRA require DoD organizations to measure the performance of existing and planned information systems and to report performance measures on an annual basis. The *C4ISR Architecture Framework* provides uniform methods for describing information systems and their performance in context with mission and functional effectiveness.

The JTA complements and is consistent with other DoD programs and initiatives that are developing and acquiring effective, interoperable information systems. These efforts are listed below.

### 5.1. C4ISR Architecture Framework

The C4ISR Architecture Framework is intended to ensure that the architectural descriptions developed by the Commands, Services, and Agencies interrelate to each organization's operational, systems, and technical architecture views. It provides direction on how to describe architectures, and provides a process for using the Framework to build and integrate them using a six-step process. The Framework describes three major perspectives, i.e., views, that logically combine to describe what an architecture is. These three architecture views are the operational, systems, and technical views.

- The Operational Architecture (OA) view is a description of the tasks and activities, operational elements, and information flows required to accomplish or support a military operation. It contains descriptions (often graphical) of the operational elements, assigned tasks and activities, and information flows required to support the warfighter. It defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges in detail sufficient to ascertain specific interoperability requirements.
- The Systems Architecture (SA) view is a description, including graphics, of systems and interconnections providing for, or supporting, warfighting functions. For a domain, the systems architecture view shows how multiple systems link and interoperate, and may describe the internal construction and operations of particular systems within the architecture. For the individual system, the systems architecture view includes the physical connection, location, and identification of key nodes (including materiel-item nodes), circuits, networks, warfighting platforms, etc., and 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 with the operational view and its requirements per standards defined in the technical architecture.
- The Technical Architecture (TA) view is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The technical architecture view provides the technical systems-implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The technical architecture view includes a collection of the technical standards, conventions, rules and criteria organized into profile(s) that govern system services, interfaces, and relationships for particular systems architecture views and that relate to particular operational views.

Both the C4ISR Architecture Framework and the DoD JTA are required in developing a successful technical architecture. The JTA consists of standards that have been agreed upon by the services to provide the guidance required in developing interoperability among systems. The JTA is not exhaustive. It may contain all the standards required, but not necessarily, depending on the scope of the engineering problem. For more information, see Section 1 of the JTA.

To propose that a standard be added to the JTA, click on Change Request Submission at <http://www-jta.itsi.disa.mil>.

## 5.2. Global Information Grid (GIG)

The Global Information Grid (GIG) Architecture (Version 1.0) was developed to provide the joint warfighter with a single, end-to-end information system capability that includes a secure network environment, allowing DoD users to access shared data and applications, regardless of location and supported by a robust network/information-centric infrastructure. The GIG is a single architecture utilizing the three views specified in the C4ISR Framework. During development of this version of the GIG Architecture, scenario-specific OA and SA Views were built by integrating existing architecture products. The TA View for the GIG Architecture is based on the Joint Technical Architecture (JTA).

As part of the GIG, the JTA is the key factor in achieving DoD's goal of gaining information technology superiority in support of the warfighter's needs and missions. The JTA complements the DII Common Operating Environment (COE), the C4I Surveillance, and Reconnaissance (C4ISR) Architecture Framework, TRM, and the Component-Specific Technical Architecture. The roles played by each element include:

- The DoD TRM provides the common definitions and relationships for the services and interfaces used throughout the enterprise.
- The DII COE (now the GIG COE) addresses needed products for insertion into developments.
- The C4ISR Architecture Framework provides the framework and architectural variations within which products and standards are deployed and implemented.
- The JTA provides the mandated standards to support interoperability.
- Component-specific technical architectures address the Components' technical requirements for standards.

The role and contribution each of these elements provides DoD represents a synergistic solution to DoD's overall information technology needs.

## 5.3. DoD Technical Reference Model

The DoD Technical Reference Model (TRM) provides the foundation and the common services and interface definitions used in the JTA. The purpose of the TRM is to provide a common conceptual framework and a common vocabulary so that the diverse components within DoD can better coordinate acquisition, development, and support of DoD information technology. In addition, the TRM provides the foundation for other DoD initiatives such as the DII COE and the C4ISR Architecture Framework. It supports the C4ISR, the Combat Support, and the Weapon Systems domains contained in the JTA.

## 5.4. Defense Information Infrastructure Common Operating Environment

The Defense Information Infrastructure (DII) Common Operating Environment (COE) concept is best described as an approach for building interoperable systems; a reference implementation containing a collection of reusable software components; a software infrastructure for supporting mission-area applications; and a set of guidelines, standards, and specifications. The guidelines, standards, and specifications describe how to reuse existing software and how to properly build new software so that integration is seamless and, to a large extent, automated. The JTA currently mandates the use of the DII COE (a fundamental Joint Systems Architecture).

Key JTA standards are mandated by the Integration and Run Time Specification (I&RTS). I&RTS Level 1 compliance include standards like Portable Operating Systems Interface (POSIX), and Transmission Control Protocol/Internet Protocol (TCP/IP). Some existing standards used within the DII COE are not JTA-compliant, and require waivers. The DII COE evolves as necessary to maintain compliance with mandated standards found in future JTA updates.

### **5.5. Component-Specific Technical Architecture**

Some DoD components have developed their own technical architectures. These use the DoD JTA as the basis of their technical architectures but frequently include standards that are in addition to, but not in conflict with, the JTA.

## **6. Relationship of JTA to Acquisition Planning Documents**

Acquisition planning documents serve as roadmaps to program managers and contractors for program execution from initiation through postproduction support. Therefore, the Joint Chiefs of Staff and supporting organizations involved in the weapon systems requirements-generation process and the DoD acquisition community include JTA standards requirements in key acquisition planning documents to maximize JTA effectiveness as a tool for achieving overall DoD system interoperability. The key acquisition planning documents are the mission needs statement, the operational requirements document, C4I Support Plan (C4ISP), the request for proposal, and the contract statement of work. The following discusses the general purpose of each of the four acquisition planning documents and the document's relationship to program manager implementation of the JTA standards.

### **6.1. Mission-Needs Statement**

The mission-needs statement is a product of the requirements-generation system. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01A, "Requirements Generation System," August 10, 1999, requires DoD Components to define mission needs in broad operational terms in a mission-needs statement. If DoD decision-makers determine that a mission-needs statement supports the need for a new system or system upgrade, the DoD Components use the broad requirements defined in the mission-needs statement to develop the more detailed system requirements in the operational requirements document. The Instruction promotes warfighter use of JTA standards by requiring that mission-needs statements define operational needs in conformance with DoD interoperability standards.

### **6.2. Capstone/Operational Requirements Document**

Like the mission-needs statement, the operational requirements document is a product of the requirements generational system that document required operational performance parameters for the proposed concept or system. Chairman of the Joint Chiefs of Staff Instruction 3170.01A requires that the DoD Components, in the operational requirements document, include the performance parameters, including interoperability, which an acquisition program must meet. The Instruction promotes use of the JTA by requiring that system capstone/operational requirements documents specify that the system must comply with applicable information technology standards in the JTA.

### **6.3. C4I Support Plan**

DoD Regulation 5000.2R requires DoD Components to develop C4I Support Plans (C4ISPs) for programs in all acquisition categories when they connect in any way to the communications and information infrastructure. This includes IT systems, including NSS, and all infrastructure programs. The C4ISP contains an Integrated Architecture (IA) that includes the operational, technical, and systems views. DoD 5000.2-R requires that the technical view identify applicable technical standards for each IER based on the DoD JTA. The C4ISP also includes potential C4ISR shortfalls with proposed

solutions and descriptions of dependencies and interfaces to enable test planning for interoperability key performance parameters (KPPs) and information exchange requirements (IERs).

#### **6.4. Requests for Proposal**

The Federal Acquisition Regulation, Subpart 15.203, “Requests for Proposal,” October 1, 1999, requires contracting officers for negotiated acquisitions to use requests for proposals to communicate Government requirements to prospective contractors and to solicit contractor proposals. Section C of the request for proposal has a section that includes “External Interfaces” and “Compliance with Standards.” It is the program manager’s responsibility to identify the external interface standards required and to provide a listing of all relevant JTA standards and other standards necessary for the contractor to design into National Security Systems and information technology systems. Through this proposal section, the contracting officer can advise prospective contract offerors that they will be required to develop a system using standards contained in the JTA. The submitted proposals must address implementing the standards contained in the JTA if they want to be considered a responsive offeror to the request for proposal.

#### **6.5. Contract Statement of Work**

The Federal Acquisition Regulation, Subparts 15.406-1, “Uniform Contract Format,” and 15.406-2, “Part 1 – The Schedule,” requires agency solicitations for contracts to include a statement of work or other description that defines the Government’s requirements. Program manager inclusion of JTA standards requirements in this document is necessary to ensure that the contractor uses the JTA in the system design approach. Program managers can use provisions in the contract statement of work, along with the contract data requirements list, to require the contractor to identify instances where cost, schedule, and performance considerations justify submitting a request to DoD authorities for waiver of JTA standards requirements” [Reference DoD Inspector General (IG) Audit Report # D-2001-121, May 14, 2001].

### **7. Applying the JTA to Systems**

The JTA by itself does not select nor provide the capability for the selection of specific standards. Rather, it provides the “list” from which to select standards. The effective selection of standards or development of a standards profile for inclusion into a standards-based (i.e., technical architecture) environment that mandates interoperability and reusability must be accompanied by a complementary process or selection methodology. One such complementary methodology can be found in the DoD TRM. It provides a synergistic environment for effectively selecting the appropriate standards that support both the operational and system architecture needs.

#### **7.1. Service Areas and Standards Profiles**

In general, the JTA is used to correlate system requirements to standards in order to promote interoperability among Joint systems. This includes both newly developed systems and upgrades to existing systems. The user’s mission requirements are used to define the services that will be supplied by the system in support of functionality. These major service areas, as defined in the DoD TRM, provide an area of commonality that enables relationships among disparate entities to be identified and analyzed.

The JTA itself has organized the Core, domains, and subdomains into JTA Core service areas. These Core service areas are equivalent to their corresponding TRM system services contained within the TRM’s Application Platform Entity. These Core service areas are then further broken down into base service areas.

When designing a system, the user will identify the JTA base service areas that meet the mission requirements of the proposed system. The mandated standards contained in each of these base service areas shall then be required. If a base service area does not contain a mandated standard, an emerging standard can be cited. The standards chosen for these corresponding base service areas comprise the Standards Profile that is a part of the system Technical Architecture.

Existing systems often rely on legacy or proprietary standards. If these legacy standards are needed in order to interface with existing systems, they can be implemented on a case-by-case basis, in addition to the mandated standard.

## 7.2. Building a Standards Profile

Selecting a minimum set of standards that provide coverage for all system services is not a trivial task. It must be systematically and rigorously approached. The following process provides guidance for the JTA user who is building a standards profile for a new system:

1. Identify the operational requirements.
  - a. The user must first define the operational requirements for the system(s). High-level requirements will be provided by documents such as the Mission Needs Statements (MNS), Universal Joint Task Lists (UJTLs). The Operational View contained in the C4ISP leads the system designer through the development of a Systems Architecture View and a Technical Architecture View. For example, the OA IERs (OV-3) contain attributes (information description, media type, service requirements), while the Systems Interface Description (SV-1) contains interface descriptions that can be directly applied to the identification of JTA base service areas.
  - b. Identify Standards Profiles utilized by other systems that you have a requirement to operate with. Select the required sub-set of standards contained in that profile that meet your requirement. Identify and apply for any waivers required.
2. Map these requirements to the JTA.

Map these operational requirements to the base service areas contained in the Core, domains, and subdomains.
3. Build a Standards Profile by selecting the standards required.
  - a. Validate the requirement for each of the individual mandated and emerging standards contained in the services and interfaces identified above.
  - b. When multiple standards are identified in the JTA for the same base service area, first look at the functionality covered by each standard and its associated JTA narrative before the other criteria are considered. In many sections, there are multiple standards listed, but each actually addresses different requirements. If both are equally applicable, then the following steps should be considered.
    1. Select mandated standards over emerging standards.
    2. Where base service areas do not contain mandated standards, select mandated standards from other standards sources such as the Component's or Service's JTA implementation.
    3. Select emerging standards that meet the operational requirement. Determine if there are existing implementations of those standards.

## 8. System Migration

### 8.1. Selecting the Migration Plan

There are numerous concerns that need to be analyzed during the initial phase of migrating a system to JTA compliance.

- ❑ In many cases, migration will be a complex and costly undertaking if pursued solely for a compliance reason alone, and not recommended if that is the sole reason for pursuing it.
- ❑ Cost/benefit to individual migrating programs and systems may not be seen, where there are economics of scale to be realized only by DoD as a whole.
- ❑ Timing and planning of upgrades for existing systems and programs needs to be carefully coordinated for those systems required to become JTA (including DII COE)-compliant to allow minimal impact to necessary Mission Capabilities and Performance requirements.
- ❑ To become JTA-compliant may require some trade-off analysis for mission capability/performance versus compliance.
- ❑ Once a commitment to being JTA-compliant (including DII COE) is made, sustaining compliance will require a follow-on effort throughout the system/program life cycle.
- ❑ Complying with the DII COE is only a starting point for JTA compliance. If additional functionality is required, the corresponding base service areas within the JTA need to be considered.

Selecting design options and the migration path requires an understanding of the system parameters—including its requirements, resources, and current status—merged with an awareness of the outside influences on the migration path, including technology and evolving standards. The optimal path must be continually reassessed and adjusted to ensure that requirements are met in an acceptable, cost-effective manner. There is no single optimal migration path; the path is optimized (through a series of iterations) for the conditions that are encountered along the way and which change with time.

The PM needs to identify the funding, available support resources, and the scheduling impacts associated with each increment of the migration path. While cost considerations cannot be permitted to compromise requirements, the optimal path is one that takes into account the total cost of the entire path, rather than simply providing the lowest near-term cost. The first increment often requires a substantial investment, which may be offset by lower costs later.

### 8.2. Migrating Legacy Systems Requiring an Upgrade

In very large systems it is sometimes not practical to convert the entire system at one time. Instead, migration is accomplished at the time of major upgrades or new acquisition. Subsystems must be selected and converted one at a time. The need to preserve a portion of the legacy system, for whatever reason, necessitates an interface path (bridge) that connects the legacy system (subsystem) to the new open system interface standards-based system (subsystem).

### 8.3. Migration Strategy

Several implementation approaches can be taken when migrating from one architectural model to another, depending on the nature of the system, available resources, and infrastructure requirements. Regardless of the environment or the system requirements, and in order to achieve JTA compliance when migrating systems, it is recommended that a Standards-Based Architecture (SBA) methodology be used in the design process. Such an SBA methodology identifies the possible alternative migration approaches and ensures that the target system is designed in compliance with chosen standards.

An SBA methodology encompasses seven distinct processes, as depicted in Figure 2, and can be tailored to develop any level of architecture (e.g., Enterprise, Network, System) or any specialized architecture views (e.g., Security).



**Figure 2: Standards-Based Architecture (SBA) Methodology**

The SBA methodology is a straightforward approach to the migration of legacy systems with the added requirement that the system be designed to standards. The SBA process is initiated after the system requirements have been defined. In brief, the SBA processes are:

1. Identification of guiding principles (e.g., interoperability is a priority—interfaces shall be standards-based, system shall be Y2K-compliant, platform shall be NT-based, etc.)
2. Characterization of the current (“as is”) system—in terms of four views (1) functional – a mapping of key processes; (2) technology – platform/system configuration; (3) application – in terms of quality and value; and (4) information – including data, protocol, and security.
3. Definition of the target (“to be”) system – in terms of the same four views.
4. Identification of discrete projects through “gap” analysis. The current and target architectures are compared along the same four views to identify “opportunities” for change.
5. Identification and analysis of migration options. High-level design solution sets (implementation alternatives) are developed for each of the projects identified in Step 4 and are then analyzed from a cost/benefit viewpoint, resulting in a prioritized list of projects.
6. Development of a migration plan (phased implementation plan). The results of the analysis (prioritized projects and chosen solution sets/migration paths) are refined and formalized. Projects are then released for implementation.

7. Administration. This step categorizes the process as being iterative and basically dictates that the implemented migration becomes part of the “as is” architecture and the process begins again. When the SBA process is defined to be cyclical (or evolutionary) up front, this step is often omitted.

#### **8.4. Applying the JTA to the SBA Process**

Standards assessment and selection are performed at various junctures within the SBA process. To adequately apply the JTA and ensure compliance after migration, Standards Profiles must exist for both the current and the target systems. Unfortunately, since migrations are largely reengineering efforts for legacy systems, Standards profiles may not already exist for the current system and will need to be generated. Fortunately, the current system’s Standards Profile need only catalog already implemented standards, eliminating the need for standards selection.

Creating the Standards Profile for the target system presents a variety of problems and issues that must be addressed and revisited several times throughout the SBA process. The underlying problem is that the Standards Profile cannot be completed until the design options are selected and prioritized in Step 5 (migration option analysis), and yet it is necessary for the gap analysis performed in Step 4.

In light of this drawback, the gap analysis should initially include only a high-level comparison of the current and target Standards Profile (i.e., at the major service area level) and should be performed at progressively lower levels (i.e., base service areas level) as the target Standards Profile evolves.

Migration option analysis and migration planning (Steps 5 and 6) are arduous, detail-oriented processes. It is during these steps that the target Standards Profile is developed; currently implemented standards are evaluated in terms of target requirements, and additional standards are identified to satisfy new functionalities, processes, or operational requirements.

As the target Standards Profile matures it must be compared to the current Standards Profile. This comparison will identify those implemented standards that have been superceded by mandated standards in the current JTA. A standards assessment should be performed on each set of individual standards (current vs. target) to identify and analyze implementation differences. The results of this analysis will be used to refine the selected design option.

#### **8.5. Additional Guidance**

The PM should identify the funding, available support resources, and the scheduling impacts associated with each increment of the migration path. While cost considerations should not be permitted to compromise requirements, the optimal path is one that takes into account the total cost of the entire path, rather than simply providing the lowest near-term cost. The first increment often requires a substantial investment, which may be offset by lower costs later.

Interoperability issues pose a significant challenge to the PM who is planning system funding. Current funding mechanisms and Government acquisition views are oriented toward a single, dedicated system funding approach, in which resources are channeled to each system as a separate entity. Successful implementation of interoperability across the battlefield, by assimilating commercial off-the-shelf (COTS) products into the development process, necessitates a different funding strategy than that currently in practice. Instead of funding discrete systems, DoD needs to fund the acquisition of capabilities, with interoperability costs shared among all systems that will interoperate. Interoperability support for DII COE, for example, will require a different acquisition and systems engineering approach that cuts across the systems concerned and distributes costs and risks.



## 9. DoD Interoperability Policy and Compliance

The JTA mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that create, 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 the JTA within Components, Services, or Agencies is provided in the separate Component JTA Management Plan.

According to the DoD JTA Version 3.0 promulgation memorandum dated 29 November 1999:

*“...the JTA is required for all DoD Acquisition Categories, and all other non-traditional (e.g., Defense Information Infrastructure (DII) Common Operating Environment (COE)), systemic (e.g., Joint Airborne SIGINT Architecture (JASA)), or non-DoD 5000 series acquisitions (e.g., procurement of information technology services, CINC Initiatives) that meet these criteria. In addition, implementation of the JTA is required for pre-acquisition programs such as: Advanced Concept Technology Demonstration (ACTDs), Advanced Technology Demonstrations (ATDs), Joint Warrior Interoperability Demonstrations (JWIDs), “Exploitation-year,” and Battle Laboratory projects that meet these criteria.”*

DoD Standards Reform began in June 1994 when the Secretary of Defense issued a memorandum entitled “Specifications and Standards—A New Way of Doing Business.” The memorandum directed DoD Components to adopt “performance-based specifications and standards—or—nationally recognized private sector standards” for future acquisitions. The Secretary intended the initiative to eliminate requirements that did not “add value” to DoD systems and material, and to reduce the cost and time for developing and fielding systems. The Secretary also sought to integrate the commercial and military industrial bases, by facilitating DoD’s adoption of proven, successful commercial state-of-the-art technology. The Defense Standards Improvement Council (DSIC) directs DoD’s implementation of the reform, and it maintains and extends the Reform policy through a series of OSD policy memos and other guidance. These may be found at the Defense Standardization Program home page site at <http://dsp.dla.mil/>.

The Office of the Chairman, Joint Chiefs of Staff, oversees system interoperability and supportability initiatives as stated in CJCS Instruction 6212.01B, “Interoperability and Supportability of National Security Systems and Information Technology Systems,” May 8, 2000. It can be found at [http://www.dtic.mil/doctrine/jel/cjcsd/cjsi/6212\\_01b.pdf](http://www.dtic.mil/doctrine/jel/cjcsd/cjsi/6212_01b.pdf). The Instruction establishes policies and procedures for the Joint Chiefs of Staff interoperability certification of mission-needs statements and operational requirements documents, developing interoperability key performance parameters for systems, and performing system interoperability validations. As part of the procedures for performing interoperability certification of mission-needs statements and operational requirements documents, the Instruction contains checklist criteria that the Defense Information Systems Agency (DISA) uses to assess the documents for interoperability certification in support of the Office of the Joint Chiefs of Staff. The checklist includes the requirement that the two documents require that systems developed comply with the applicable information technology standards contained in the current JTA.

The JTA promotes this standards reform initiative by identifying the minimum number of standards necessary to achieve joint interoperability, while promoting commercial standards and practices to the maximum extent possible. Thus, the JTA complies with the DoD Standards Reform initiative and its implementing policies. Acquisition managers will not need to apply for waivers from standards reform policies if they adopt JTA-mandated standards. DSIC policy memoranda recognize JTA standards as compliant with DoD’s Standards Reform policies JTA Appendix D: Page 199, Reform Waivery Policy.

### 9.1. Use of the Current Versions of the JTA

Once it has been determined that JTA compliance is applicable to an acquisition, it must be recognized that it is not a one-time effort. Vigilance will have to be maintained throughout system or program life cycle to maintain compliance. This does not mean that ongoing acquisitions need to update their requirements to maintain compliance with later versions of the JTA. However, Agencies need to establish their own guidelines. For example, if your acquisition process has completed milestone B, there may not be a requirement to comply with later versions of the JTA.

### 9.2. Compliance and JTA Metrics

The PMs are responsible for ensuring that their JTA-applicable programs and systems are interoperable with other systems with which they need to interface, as well as the JTA. DoD policy made this responsibility clear in the JTA Policy Memorandum for JTA Version 2.0 on 30 November 1998. This policy was affirmed in the JTA Policy Memorandum for JTA Version 3.0 on 29 November 1999. This DoD policy requires DoD components to apply JTA-mandated standards for all “emerging (systems) or changes to an existing capability that” must include all three of the following attributes:

- Produce, use, or exchange information in any form electronically;
- Cross a functional DoD component boundary; and
- Give the warfighter or DoD decision-maker an operational capability.

Compliance with the DoD JTA may be achieved in varying degrees, based upon the circumstances pertaining to the individual system or program implementation. The issue of JTA compliance is further influenced by other DoD mandates such as the DII COE. [See DII COE Integration and Run Time Specification (I&RTS): Version 4.1, October 3, 2000.] Thus, JTA compliance may not be a clearly defined set of activities or adherence to a particular set of standards. Mandating JTA compliance on a system implementation will depend on several factors:

- The system under development or upgrade: Is the system a legacy system, a system to be completely replaced or incrementally upgraded, or a new system?
- The standards profile currently enforced (on an existing system); the replacement or upgrade schedule for those standards; and the introduction and impact of new standards that are introduced.
- If there is a gap or void in the JTA, the PM should identify a standard and submit a change request to the JTA Development Group (JTADG) [See Change Request Submission, on the JTA Home page Uniform Resource Locator (URL)] via their Service Component Representative.
- The clear identification of the extent of standards application: the entire standard or parts thereof; or new changes to the standard.
- The technology being introduced into the system implementation; and the standards existing or applicable to that technology and their status (i.e., nonexistent, draft, sponsored, approved, or de facto).
- The relationship of products selected, and their degree of compliance of those products (e.g., DII COE compliance) with the mandated standards contained in the JTA. This will help to expose conflicts or ambiguities within the compliance mandates.

Thus, users are responsible for understanding the enterprise and domain of operation in which the system functions and the mission to be supported. Interoperability is required in the context to which personnel and their missions must be supported from information source (origination) to its destination. Users need to recognize that in many cases they must negotiate the decomposition or delegation of

interoperability responsibilities among their system(s) and other systems, with which they must interoperate, if they are to succeed under the current “stovepipe” development environment. Again, the risk is significant, as the failure to provide system interoperability through JTA compliance, can result in programmatic halts or significant reductions in funding per Secretarial or Acquisition Executive decisions.

Compliance of a product or item to a standard can best be achieved in those cases where a mapping of standards is performed. These mappings are very effective but can be labor-intensive and can tax implementation resources. Mappings consist of relational matrices of services and interfaces, versus services and functions that the standard supports and are contained therein. Once a mapping of two or more standards is performed, service and interfaces supported can be compared, with disparities, similarities, and ambiguities quickly identified to a high degree of confidence. The issues surrounding compliance can best be served where compliance procedures or checklists can be clearly established and incorporated into procurements, to ensure that they are addressed properly. Well-defined compliance procedures for specific types of developments (i.e., new, incremental, or legacy development) can assist the Program or Project Manager in developing cost-effective interoperability plans. Compliance procedures and checklists can be found in the specifically developed Service and Agency-level compliance guidance issued by the cognizant Acquisition Executive. For example, the Secretary of the Air Force issued an Air Force JTA Implementation Plan for the DoD Joint Technical Architecture Version 2.0, December 1998, that contained an Information Exchange Requirements Matrix. In addition, the Joint Staff issued policy requiring DoD Components to identify Information Exchange Requirements (IERS) that support development of interoperable systems [See JROCM 132-99, 16 November 1999: Subject – Policy for updating Operational Requirements Documents (ORD’s) to incorporate Interoperability Key Performance Parameter (KPP) and Cost].

Collecting metrics information is a viable method that can be utilized for measuring the compliance and success of JTA implementation. By establishing baselines and collecting quantitative and qualitative metrics, a Service or Agency can measure the positive impacts of implementing a sound JTA compliance program. Metrics can be used to determine return on investment (ROI), cost of ownership, and interoperability data. For example, metrics can be gathered to gauge a reduction in procurement time, a reduction in IT spending, an increase in productivity, an increase in spending for training, a decrease in interoperability spending, an improvement in end-to-end systems performance, a reduction in number of products existing across a service, a faster implementation time, more accurate budget projections, more consistent interfaces, and improved IT quality. The utilization of such metrics will help to measure the value of JTA implementation compliance over time.

### **9.3. Waiver Process**

Each DoD Component should document its specific procedures in its Component JTA Management Plan. Acquisition managers will not need to apply for waivers from standards reform policies if they adopt JTA-mandated standards. DSIC policy memoranda recognize JTA standards as compliant with DoD’s Standards Reform policies. [JTA Appendix D: Page 199 Reform Waiver Policy]

Only the Component Acquisition Executive, or cognizant OSD authority can grant a waiver from the use of an applicable JTA-mandated standard. All waivers shall be submitted to the Under Secretaries of Defense (USDs) Acquisition, Technology, and Logistics (AT&L) and the ASD (C3I) DoD Chief Information Officer, for concurrence. The current policy permits the waiver applicant to assume that a waiver has been approved if there is no response from the cognizant Acquisition Executive’s office within two (2) weeks of the date of receipt. To ensure proper and timely consideration, all waiver requests should also identify cost, schedule, technical performance impacts, and operational limitations

stemming from DoD's failure to grant the waiver. The policy for implementation and waivers for JTA Version 3.0 remains as prescribed in the Memorandum, which promulgated Version 2.0.

#### 9.4. Component JTA Management Plans

Each DoD Component and cognizant OSD authority is required to produce a Component JTA Management Plan that includes the processes for ensuring compliance, for programming and budgeting sufficient resources for ensuring and implementing compliance, and for scheduling compliance activities. This requirement for an implementation plan was the impetus for creating the *Component JTA Management Plan* template to be used by the Services and Agencies. This template is contained in Appendix A.

According to the DoD JTA policy memo for JTA Version 3.0, dated 30 November 1998:

*“Implementation of JTA, that is the use of applicable JTA-mandated standards, is required for all emerging, or changes to an existing capability that produce, use, or exchange information in any form electronically; cross a functional or DoD Component boundary; and give the warfighter or DoD decision-maker an operational capability.”*

It should be noted that the Version 1 promulgation memo, dated 22 August 1996, and Version 2 promulgation memo, dated 30 November 1998, of the JTA *requested* Services and Agencies to provide a JTA implementation plan (Component JTA Management Plan). The promulgation memo for Version 3, dated 29 November 1999, goes further by stating that, “Each DoD Component and cognizant OSD authority is *required* to have on file a current or new implementation plan with the USD (AT&L) and the ASD (C3I) [DoD Chief Information Officer (CIO)]. If an implementation plan needs revision, it is due within 60 days while a new plan is due within 90 days from the date of this memorandum.”

#### 9.5. User Selection Standards and Specifications

Any service-specific guidance provided by appropriate command authorities may be used as a last resort if there are no appropriate standards in a given base service area.

### 10. Contract Language

This section contains examples of general information items and text that can be used in procurements or solicitations in specifying the requirement to use the Joint Technical Architecture. The text is offered as examples, is to be used to illustrate the concept, and can be modified to suit user needs. It provides a systems acquisition template for the Systems Engineer for specifying and establishing criteria for JTA compliance.

#### 10.1. Statement of Work Language

The following list of requirements contains example wording that could be used in a Statement of Work (SOW). Portions or all of the following text could be used as appropriate:

- This Statement of Work (SOW) describes the requirements for a technical architecture consisting of components defined by the DoD Joint Technical Architecture (JTA). The use of standards and products from the referenced documents are described as follows:
  - a. DoD has developed a Joint Technical Architecture that is directed at supporting a broad range of applications and system implementations.
  - b. The JTA describes the component interfaces, protocols, and supporting data formats standards necessary to provide the services required by applications. A list of mandated

and emerging standards has been identified by DoD to be used in this procurement by the contractor.

- A general requirement for an open system and interoperability environment:
  - a. All information technology (IT) products and services offered in response to this solicitation shall operate in and execute upon platforms that provide the necessary degree of interoperability specified in the accompanying specifications and as modified by this solicitation. The contractor shall provide evidence to show that these products and services conform to and are in compliance with the Joint Technical Architecture.
  - b. For each standard, product, or service defined for use in this solicitation the contractor shall provide the following information:
    1. Contract Line Item Number (CLIN)
    2. Name and identification of each item, including version or release number that identifies the implementation explicitly from all other versions or configurations.
    3. Description of the component, especially where a part of or volume of a standard is referenced.
    4. Reference document identifiers that support contractor or vendor product claims are required, along with cross-references to section numbers as described in specifications or the contract.
- Unless otherwise specified, all standards-based validation testing and compliance issues shall be conducted or approved by the DoD Contracting Officers Representative (COR) as the sole validation authority for specific standards, or by organizations named specifically by the Contracting Officer. Derived validations shall be acceptable where the same product and end interface points are the same as previously implemented and tested in a similar DoD implementation.
- Interoperability among implements shall be proven through current registration of offered products and test results with an accredited or recognized Government source or professional organization, where such service or proof exists.
- Where DoD interoperability proof of compliance does exist, the contractor shall demonstrate interoperability by executing demonstration tests on the proposed platforms with the identified standard required by this contract for each individual specification affected.
- A DoD-provided application program in source code form shall be compiled and executed on one or more the proposed platforms selected at random. The application program shall be moved to another platform that is not of the same model, and the program shall be compiled with and executed on this platform. A detailed report of the modifications made to the source code to achieve successful compilation and execution shall be submitted. These compliance tests may be executed with contractor-provided application programs that have been approved by the Government.
- Proof of compliance shall be acceptable where two or more certificates from industry-recognized trademarking or branding organizations shall indicate that the same implementation of the proposed component (i.e., same standard, same hardware or software version and release) has been validated on at least two different contractors' platforms. Contractor-provided applications that have been approved by the Government shall also be acceptable.
- In cases where a capability demonstration is the required from of compliance testing, the following instructions shall apply:

- a. Where a proposed standard has not been declared as a mandate or emerging standard, the contractor shall demonstrate the implementation in a manner that exhibits the implementation's interoperability, portability, and scalability characteristics.
  - b. A DoD-provided application shall be installed and executed on two of the proposed platforms selected at random. If only one platform is proposed, that a second platform of different model supplied by the Government or contractor shall be temporarily used for the execution of this test.
  - c. A data file of DoD-provided information shall be transmitted through network communications directly from one platform to the other. A null modem or other similar connection can be employed where a network is not available. Both applications shall be executed and a report printed on the file's contents on external storage (e.g., floppy disk or magnetic tape).
  - d. These compliance tests may be executed, at the Government's discretion, with contractor-provided data files that have approved by the Government.
  - e. In the event that an identified standard changes from emerging to mandated status, compliance testing or assurance shall be required within 12 months of the change in status of the standard.
- In the event an interpretation of standard is required that will invoke any waiver procedure, such a request for interpretation shall be made within 30 calendar days after contract award, or the event triggering the need for such occurs. Any corrections required as a result of decisions made under the interpretation activities shall be completed within 12 months of the date of the formal notification to the contractor of the decision made or approved by the Government.
  - As standards and other specifications required in this contract evolve or are transitioned from emerging to mandated, the contractor shall provide upgrades for implementation based on the current standards within 12 months of the publication and release of the standards.
  - Technologies based on emerging standards not specifically referenced in this contract may be proposed by the contractor only when such specifications achieve a high degree of stability, and the benefit to the Government can be clearly documented when compared to older technologies and their cost basis.
  - Contractors shall use service and interface definitions derived from the DoD Technical Reference Model document.
  - All service and interface definitions used to identify, associate, or describe a standard in this procurement, solicitation, specification, or deliverable shall be derived using the DoD TRM. Further elaboration of a particular service or interface definition (i.e., subservice definition) shall be traced to or identified as their related DoD TRM service or interface category or group. Where new technologies are introduced and identified as impacting interoperability, the respective service/interface category associated with this technology shall be identified or defined where an existing category is deemed not applicable.
  - Service and interface definitions derived from other sources or standards shall be reviewed to ensure that they are consistent with DoD TRM service and interface definitions.
  - After contract award, the contractor shall provide transition plans for accomplishing the move from the current standards environment to the JTA-compliant environment in an orderly and controlled manner. In particular where noncompliant standards are referenced (i.e., draft standards and other public specifications), the contractor shall provide a method and plan for transitioning from the proposed implementation to a future JTA-compliant implementation and shall certify that the transition shall be implemented and completed within 12 months from the

date of acceptance of such, unless otherwise specified in the contract. The transition plan shall include problem areas, enhancements to legacy and migration components, redundancy, new components introduced relative to the standards being used, and those that are being proposed for use in support of interoperability.

- If a standard is not yet supported by implemented products, intermediate targets shall be identified that provide this incremental functionality and help to transition to the objective and compliant environment. These intermediate targets shall be defined by the contractor and fully described including changes from the baseline. Detailed plans for managing and implementing the intermediate targets shall be included. Each intermediate target shall include a description of the intermediate target environment, major changes from the baseline, and identification of schedules, deliverables, milestones, and organizational resource requirements, as a minimum.

### **10.2. System Requirements Specification Language**

The following sample guidance can be used in System Requirements Specifications. Portions or all of the following text could be used as appropriate.

- The system design approach shall comply with the applicable portions of the Joint Technical Architecture. Any proposed technical designs that deviate from the standards and practices delineated in the Joint Technical Architecture, either during the evaluation and/or subsequent execution of this contract, shall be approved through the Program Manager, prior to implementation. The Joint Technical Architecture document is located on the Web at URL: <http://www-jta.itsi.disa.mil>.

### **10.3. Request for Proposal Language**

Portions of all of the following text could be used as appropriate on Request for Proposal Submissions.

- System Design Section – Technical Volume  
The offeror shall provide a written discussion of the extent to which his proposal complies with the applicable sections of the DoD Joint Technical Architecture.
- Software Development/Design Section – Technical Volume  
The offeror shall describe how the proposed software design approach and software development environment are compliant with the applicable portions of the DoD Joint Technical Architecture.
- Evaluation Approach Section  
The use of Understanding of Requirements and Completeness as elements of the Technical Evaluation Approach will ensure that compliance with the Joint Technical Architecture as required in the system requirements section is evaluated as a critical element.

Note: The applicable documents section of the RFP should list the specific version number of the Joint Technical Architecture document and the date of that version.

Page intentionally left blank.



## Appendix A: Component JTA Management Plan

This appendix is a recommended template for use by DoD Services/Agencies in documenting their JTA Implementation Plans.

### 1. Purpose

State the purpose of this document, i.e., to comply with the DoD Joint Technical Architecture memo. Provide Agency policy for the use of the JTA. Additional information may include reference to current agency programs, philosophies, or background.

Include a concise summary of JTA program management in your Agency. Include a summary of major work activities during the cycle, major milestones, required resources, and budget. Indicate the status of this Component JTA Management Plan, that is, is it a new plan, a major revision, or periodic update.

Rationale: To provide background information concerning Agency and current JTA efforts.

### 2. Applicability and Scope

State of the applicability of the JTA to the Agency; list of all organizations covered under the management plan.

### 3. Organization

#### 3.1. Organizational Responsibilities

List each Agency office involved in the JTA compliance process in your organization and the offices' general responsibility in the JTA process, i.e. configuration management, waiver process, reviewing documents.

Rationale: To document the structure of JTA responsibility, along with areas of responsibility.

#### 3.2. Organizational Priority.

Describe how the JTA Program supports Agency specific missions and goals. Describe how effective JTA management will impact Agency performance measures.

Detail the level of priority in the context of Agency objectives given JTA compliance in your organization. Describe the degree of emphasis the Agency places (on programs and systems under their cognizance) for verification of current JTA compliance status, and for ensuring JTA compliance in programs and systems currently under development. Justification/rationale for setting priorities, such as funding, should be included in this section.

Rationale: To demonstrate Agency commitment to JTA compliance, and external impacts that effect management.

### 4. Procedures

#### 4.1. Management/Oversight Structure and Processes.

Describe the project management methodologies used to administer the JTA process in your Agency. Identify the different offices and organizations responsible for oversight, as well as for reviewing planning documents for JTA compliance. Identify the different management documents to be used in the oversight process.

Explain the processes for periodic requests for component conformity with JTA requirements, as well as for receipt, tracking, evaluating, or providing feedback on JTA compliance within applicable programs.

Rationale: To identify the roles and responsibilities for management.

#### **4.2. Schedule.**

Provide a timeline for major milestones and events. These should include milestones such as time frame for establishing new user support programs and training associated with JTA compliance, and other major events. Schedules should be expressed in terms of calendar dates.

Rationale: To show overall JTA milestones.

#### **4.3. Change Control and Configuration Management.**

Change Control and Configuration Management. Describe your Agency's approach to change control configuration management. Document the internal change control and configuration management process.

List the office(s) responsible for these responsibilities. Explain how these offices will maintain control of this process. Show how program/system managers use the Agency's process for recommending changes in both the Agency's configuration management and the JTA.

Rationale: To document the internal change control and configuration process and associated controls for the JTA.

#### **4.4. Assessment of Progress.**

Document the Agency strategy for assessing progress for JTA compliance and interoperability. Describe the Agency's internal, ongoing review process. Specify and provide a sample of reports that will be produced for management to use to monitor the project. Explain how and at what stage(s) the executive management is involved in the review process.

Provide description of your Agency's process for identifying the development and acquisition of new systems and migrating systems and at what points they are reviewed for verification of JTA compliance. Provide a description of the process that will be used to track the costs and benefits attributable to this project.

Rationale: To describe the Agency's verification and assessment process.

#### **4.5. Review Procedures.**

##### **4.5.1. Implementation Procedures.**

Identify offices and/or organizations responsible for reviewing planning documents for JTA compliance. Show how program milestone decision authorities utilize JTA compliance as exit criteria for acquisition program milestone reviews. Define language that program managers should include in mission-needs statements, operational requirements documents, and systems specifications documents.

Detail your organization's process for JTA compliance. Identify the approach in specific functional domains, organizational elements, or systems, as well as the criteria for migration.

The program schedule should integrate all activities into a single comprehensive plan that represents a "road map" for JTA program implementation from the investment decision through the in-service

phase. Show major program milestones and critical interrelationships between work activities in the integrated program schedule. Developing a compliance assessment template is recommended.

Rationale: To list the JTA related milestones.

#### **4.5.2. Criteria for Migration to JTA Compliance.**

There are two aspects to consider when developing migration compliance procedures. The first is the migration of legacy non-compliance systems undergoing major upgrades, and the second includes systems that are currently under development.

Indicate the process for migrating non-compliant legacy systems undergoing major upgrades to JTA compliance. List the criteria that these systems need to consider, such as cost, scheduling, and standards evaluation.

##### **4.5.2.1. Migration of Legacy, Non-compliant Systems.**

Indicate the process for migrating non-compliant legacy systems undergoing major upgrades to JTA compliance. List the criteria that these systems need to consider, such as cost, scheduling, and standards evaluation.

##### **4.5.2.2. JTA Compliance, New and Developmental Systems.**

Provide a comprehensive listing of the steps that will be taken to review all developmental systems for migration to JA compliance.

##### **4.5.2.3. Waivers.**

Describe the procedures for determining if a waiver can be requested and the process within the Agency to obtain such a waiver. Document the approval process for obtaining waivers. Document the process for coordinating waivers with the appropriate organizations that design, review, implement, and acquire IT systems. For describing systems that may be subject to a waiver based on cost, compare costs associated with a JTA-compliant system against the cost of a non-compliant system.

Include factors such as interoperability with other systems, urgency for delivery, existing JTA standards, and applicability of JTA standards for new emerging systems.

Rationale: To document factors affecting migration to JTA compliance.

#### **4.5.3. Estimated Cost for JTA Management.**

Describe the overall program costs for management/oversight requirements, and additional funding requirements for user support and training associated with JTA compliance. Identify any funding constraints.

Rationale: To gauge the overall cost for JTA compliance for a specific Agency.

#### **4.6. Integration with Other Initiatives.**

Provide any plans to integrate with other ongoing component initiatives (e.g., other technical architectures). State how the Agency will coordinate with other agencies acquiring systems or capabilities under its acquisition purview, as well as how the Agency will coordinate the acquisition of systems or capabilities under the purview of other agency acquisition responsibilities. For those agencies that have their own technical architecture, or prescribed set of standards, describe how their system(s) will integrate with the JTA.

Rationale: To show how the JTA relates to Agency technical architecture initiatives.

## **5. Support**

### **5.1. User Support.**

Describe user support functions for JTA within the Agency. The description should contain the points of contact for any questions regarding the JTA, including office, mailing address, phone and fax numbers, and e-mail address. Describe the level and type of support such as help desk, e-mail, or telephone support. Include outreach efforts such as briefings or meetings in response to concerns or questions.

Rationale: To list the efforts made to support users.

### **5.2. Training and Education.**

Describe the type of course(s) or instruction, the frequency, type of personnel focus, and the scope of training. List types of training and materials provided by the Agencies (i.e. briefings, booklets/handouts).

Describe follow-up procedures for ensuring that employees and contractor personnel have been provided adequate training. Describe any JTA awareness programs existing in the Agency.

Rationale: To list and describe the type of training provided on the JTA.

## **APPENDICES**

**References.** Provide a list of all documents, correspondence, and other sources of information cited in the plan. Reference documents and policy specific to your organization that supports the JTA. For each reference, include the title, date, author, and publishing organization.

**Definitions.** Define or provide references to the definition of all terms, used in the plan. Terms used should be defined in this section if the meanings are not well known or require special explanation.

**Acronyms.** Define abbreviations and/or acronyms in the plan.

**Key WWW Information Sources.** URLs for Web pages to assist program managers in complying with the JTA, i.e., the JTA Web site, JTA Users Guide Web page, agency-specific technical architecture Web pages, and Web sites for other referenced guidance/directives.

**Compliance Assessment Template.** A tool to be developed for a system to use in assessing compliance with the standards contained in the JTA

**Milestone Chart.** This is a chart listing the agency's major JTA milestones.

## **Appendix B: Frequently Asked Questions (FAQ) about the DoD JTA**

### **1. What is a technical architecture?**

Recent discussions within DoD have defined three types of architectures: operational, technical, and system. A technical architecture is a set of rules, or “building codes,” that are used when a system engineer begins to design/specify a system. These rules consist primarily of a common set of standards/protocols to be used for sending and receiving information (information transfer standards such as Internet Protocol suite), for understanding the information (information content and format standards such as data elements, or image interpretation standards) and for processing that information. It also includes a common human-computer interface and “rules” for protecting the information (i.e., information system security standards)

### **2. What is the Joint Technical Architecture?**

The JTA is a document that mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. DoD’s policy is that the JTA shall be used by anyone involved in the management, development, or acquisition of new or improved systems within DoD.

### **3. Why is a JTA needed?**

The need for interoperability and improved information flow across DoD in support of the joint operations has been widely recognized. In order for systems to “interoperate” in a joint environment, new systems need to be “born Joint,” and legacy systems need to be upgraded to achieve joint interoperability. The JTA is a key element of DoD’s overall architectural strategy to achieve that goal.

### **4. What is the Scope of the JTA?**

The scope of the JTA includes information technology and information technology-related standards in DoD systems that may exchange information or services across a joint, functional, or organization boundary.

### **5. What was done to ensure that the JTA would be useful to its stakeholders?**

The JTA development process emphasized the participation of “users” such as Program Managers and developers, as well as the technical standards experts from all of the DoD user communities. Each DoD Component established continuous communication with its development community and involved them in the standards selection process throughout JTA’s development cycle. Key DoD senior-level stakeholders such as leaders of DoD’s acquisition community have been kept current about the process and progress of JTA’s development.

### **6. Does the JTA Apply to lease services?**

Yes, at a minimum the JTA standards apply at the interfaces to these services.

### **7. Why does the JTA need to address so many standards?**

DoD owns, uses, and continues to develop a very wide range of information systems with many possible interfaces services and technologies. JTA focuses on the concerns about interoperability by identifying the minimum set of standards for the various service areas, emphasizing one standard per function, where possible. Generally, a given system will only implement a subset of the functionality defined and therefore need only a subset of the standards from the JTA. Standards in the JTA are “mandatory” in the sense that if a service is going to be implemented, then it must be implemented in

accordance with the JTA standards. For example, if your system is not using SATCOM, there is no need to implement any of the SATCOM standards.

**8. Doesn't the use of standards conflict with DoD's acquisition reform efforts, particularly the use of military standards?**

No, the standardization documents identified in the JTA are consistent with Acquisition Reform policy initiatives that take precedence over the JTA when there are conflicts.

**9. When a new version of a standard identified in the JTA has been published, should we assume that the new version is automatically mandated by the JTA?**

No, a newly revised standard may not necessarily be "backward compatible" with the requirements that it has replaced. If the revised standard is "backward compatible" then it will be evaluated for its interoperable requirements, and mandated in a future JTA version. As a general rule, newer versions of standards will be mandated in the JTA when they mature by demonstrating sufficient product support and a continuing impact upon DoD's need for interoperability. Thus, a clear migration path from the older version of the standard will be identified to continue the interoperability requirements.

**10. What do I do when I need standards not listed in the JTA to interface with non-U.S. systems?**

In some cases, the citation of JTA standards, for example those of ISDN and SONET, does not ensure interoperability in regions outside North America where standards for these services differ. The JTA recognizes that this is a critical area affecting interoperability, but this version does not recommend a specific solution. In these cases, the system acquisition agency is responsible for analyzing the requirements and choosing appropriate solutions.

**11. As a user, can I submit a proposal for a standard to be added, changed, or deleted to the JTA?**

Yes. Interested parties can request a userid and password to the JTA's Change Request Web pages. Information about this capability can be found on the JTA Web site at <http://www-jta.itsi.disa.mil>. Use the following as a checklist in submitting proposed changes:

1. State the recommended change.
2. Write out the precise title (including punctuation and spelling), version number, status (draft, final, or approved), part, and date of the proposed standard.
3. Specify the standards body/forum that developed the standard.
4. Specify that the standard support the component's objectives of improved system interoperability and/or affordability.
5. State whether the standard is proprietary or open.
6. List a minimum of three commercial products that implement the standard.
7. State where your proposed standard should be placed in the JTA (Core mandate, emerging standard, or as an addition to a specific domain or subdomain), include the paragraph number.
8. Provide support that the proposed standard does not create any conflicts with existing component mandates.
9. Specify implications to a component deployment.
10. Specify that this standard be consistent with authoritative sources: law, regulation, policy, and guidance documents. If not, provide a rationale supporting the deviation from authoritative sources.

**12. Why are some required standards such as TADILs A, B, and C not in the JTA?**

The JTA is a forward-looking document that defines standards for new systems. The intent is to clearly indicate a migration direction. Standards such as TADILs were viewed as legacy standards and therefore not included.

**13. Why aren't specific programming languages or Web Browsers identified in the JTA?**

The JTA does not identify specific programming language standards so as to avoid subjecting users to a multiple waiver process for both programming mandates and JTA standards. In the case of Web Browsers, the JTA mandates standards and specifications, such as HTML and HTTP, which govern the format of World Wide Web information. The JTA maintains independence from specific products whenever possible.

**14. Do the standards cited in the JTA preclude the use of plug-ins, such as those that support RealAudio and QuickTime video?**

RealAudio is a de facto standard that has not been approved by a standards body. Systems may use RealAudio under the general umbrella of VISP VSM-1 system descriptions, but interoperability is not guaranteed.

**15. How does one go about getting the certification? I have been granted access to the JTA Compliance Database, but whom do we contact to actually obtain the certification? What about waivers?**

According to CJCSI 6212.01B, Defense Information Systems Agency (DISA) Center for Standards (CFS) is supposed to certify your Information Technology Standards Profile prior to milestone III. The system's standards profile is the set of one or more base standards and, where applicable, the identification of chosen classes, subsets, options, and parameters of those base standards necessary for the system to accomplish its function. The Center for Standards can assist the system developer in selecting the appropriate standards (i.e., developing the profile) to meet the interoperability requirements of your system. To complete this process, however, the profile that DISA CFS develops for the system developer must be certified as representing the actual requirements of the developer. In other words, once the profile is developed, it must be validated that the standards selected actually represent what the system is going to be based on. This means that all costs, legacy requirements, interfaces, and other issues have been addressed. Once this is done, the profile can then be sent back to DISA CFS for evaluation and/or certification.

According to DoD 5000.2-R, in developing the DSPTS standards profile the standards must come from the DoD Joint Technical Architecture (latest version). This document, and the implementation memorandum, can also be found on the JTA Web site <http://www-jta.itsi.disa.mil>.

**16. Does the JTA have a form for requesting a waiver for granting permission to operate a non-DII COE-certified operating system (i.e., LINUX) on an Air Force base network?**

If the question concerns the mandate for DII COE level 5 compliance, the matter needs to be resolved through the Service's acquisition review process. The DII COE only releases DII COE Kernels that are deemed compliant by DISA and its Kernel Platform Compliance (KPC) Program. The JTA does not mandate any specific operating system; rather, it mandates only the standards for interfacing with the one selected (UNIX or Windows). A waiver is required if these standards are applicable to systems using LINUX OS. If not applicable, a waiver is not required.

A waiver must be approved by the cognizant Acquisition Executive and forwarded for concurrence by USD(A&T) and ASK(C31)/DoD CIO. The memo forwarding the waiver must contain sufficient details in terms of the impact to cost, schedule, or performance to allow us to make recommendation our respect principal.