Joint Technical Architecture:
Impact on Department of Defense Programs

Judy Kerner
The Aerospace Corporation

The Department of Defense (DoD) Joint Technical Architecture (JTA) is intended to help achieve weapon systems interoperability and an open systems approach to weapons-system design. This article provides information a DoD program manager, development contractor, system architect, or other JTA stakeholder will need to know to begin applying JTA in system development. This article describes the organization and content of the JTA very briefly, and contrasts it with the Defense Information Infrastructure (DII) Common Operating Environment (COE), a related initiative with which it is often confused. Finally, it describes some of the actions DoD programs must take in order to comply with the mandate for JTA and identifies a few of the additional actions necessary to achieve system interoperability.

In today's increasingly dynamic battlespace, systems that were never intended to work together are often involved in aspects of the same mission, sometimes even deployed in the same tent. In this environment, interoperability (i.e., the ability of systems to exchange information and use common information) is at a premium, but it rarely happens by accident. The Department of Defense (DoD) has begun a number of initiatives to address aspects of this problem.

In the information technology (IT) arena, the DoD Joint Technical Architecture (JTA) [1] is intended to help achieve weapon systems interoperability and to support affordability and an open systems approach to weapon-system design. To accomplish this, the JTA specifies a set of primarily commercial specifications, standards, and guidelines in the areas of information processing, information transfer, modeling, message format, user interface, and security. DoD requires these standards and guidelines to be applied to all new and all changes to DoD information technology and national security systems.

There is a great deal to be said about the JTA, its development and context, related initiatives, and the role of interface standards and open system architectures in achieving interoperability; far too much to cover in one article. The scope of this article is limited to information a DoD program manager, development contractor, system architect, or other JTA stakeholder will need to know to become sufficiently familiar with the JTA to begin applying it in system development. This article discusses the motivation for JTA and quotes from some of the current DoD policy that mandates its use. It describes the organization and content of the JTA very briefly,

and contrasts it with the Defense Information Infrastructure (DII) Common Operating Environment (COE), a related initiative with which it is often confused. Finally, it describes some of the actions DoD program personnel must take in order to comply with the mandate for JTA, and identifies a few of the additional actions necessary to achieve system interoperability.

> ## "It is no longer possible to identify in advance all the systems with which a new system will need to interoperate even in the near term."

Motivation for JTA

The battlefield environment has changed; today, task forces are formed and dissolved in real time to meet dynamic requirements. It is no longer possible to identify in advance all the systems with which a new system will need to interoperate even in the near term. The interfaces between two or more systems have traditionally been defined in Interface Control Documents agreed to by all involved parties. But when the specific combinations of interoperating systems are not known a priori, this approach can become unworkable. The rapid pace of change in the commercial world complicates the situation still further, since increasingly many of the com-

ponents of DoD systems are of commercial origin. This dynamic environment favors systems that can evolve most easily to meet changing requirements and environments, systems whose interfaces facilitate this rapid flexibility and adaptability.

Both in industry and in DoD, interface standardization and open systems are being used to facilitate this flexibility. The concept is that if a system is implemented with a standard interface, then it should be able to interface at least with other (perhaps unspecified) systems built to use the same standard interface. This approach is well understood for hardware interfaces, as for example, with electrical sockets and plugs. The DoD is moving toward interface standardization and open systems to help achieve the necessary battlefield interoperability.

According to the DoD Open Systems Joint Task Force (OS-JTF) [2], an open system is a "system that implements sufficient open standards 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." A key characteristic of an open system is that it has standard interfaces that facilitate portability and interoperability of system components, as well as user portability. The JTA and the DII COE are two of the initiatives aimed at increasing this standardization and commonality within the DoD.

JTA Scope and Evolution

Since August 1996 when JTA Version 1.0 [3] was released, JTA's scope of applicability has broadened considerably. Corresponding to the release of JTA Version 1.0,

the Office of the Secretary of Defense (OSD) mandated the JTA for all command, control, communications, computers, and intelligence (C4I) systems and the interfaces of other key assets with C4I systems [4]. JTA Version 2.0 [5] was released in May 1998, and with its implementation memo in November 1998 [6], the scope of application broadened.

The memo said, in part: "JTA, that is the use of applicable JTA standards, is required for all emerging or changes to an existing capability that produces, uses, or exchanges information in any form electronically; crosses a functional or DoD Component[1] boundary; and gives the warfighter or DoD decision maker an operational capability." Waivers from compliance with JTA standards were possible for cost, schedule, or performance impacts, but required approval of the DoD Component Acquisition Executive (CAE) or cognizant OSD authority. Each individual DoD Component was made responsible for implementing the JTA mandate, including compliance assurance, programming and budgeting of resources, and scheduling.

JTA Version 3.0 [7] was released in November 1999; the memo implementing it [8] included the JTA Version 2.0 implementation memo as an attachment, and indicated that the key paragraphs, including those described above, continue to apply. A concern arose that the long time between releases of the JTA might not allow it to keep pace with rapidly changing technology and program needs. So it was decided to allow interim versions of the JTA to be released without new implementation memos, under the condition that the only differences involve movement of standards within the document, from "emerging" status to "mandated" status. A change of this sort precipitated the release of JTA Version 3.1 in March 2000 [9]; the only significant difference between the versions was that in Version 3.1, Gigabit Ethernet was listed as a mandated standard, while in Version 3.0 it had been classified as an emerging standard.

DoD has begun incorporating JTA compliance in major policy documents, which have further broadened its scope of applicability. For example, in May 2000, the chairman of the Joint Chiefs of Staff (CJCS) issued CJCS Instruction 6212.01B [10], which stated the following: "National Security Systems and Information Technology Systems must comply with applicable IT standards contained in the current DoD JTA Service and Agency-specific implementation." DoD Regulation
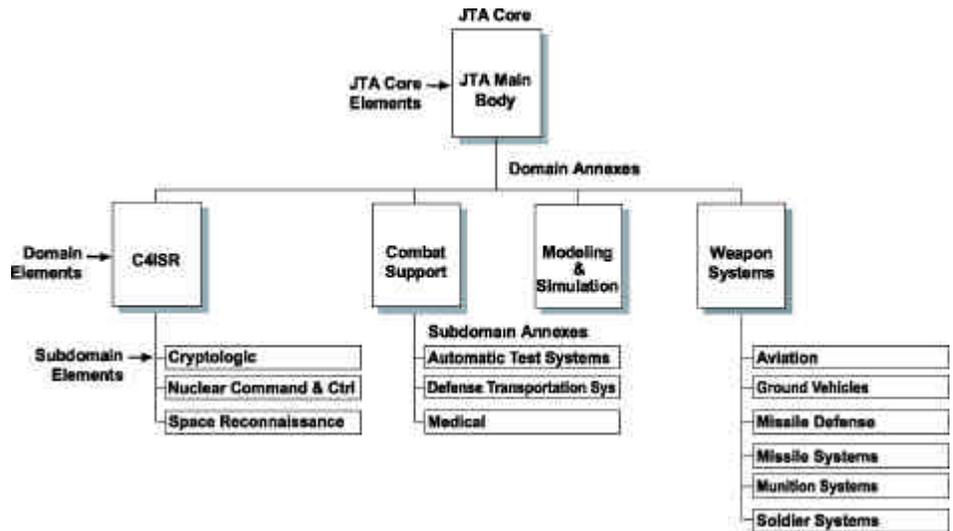

Figure 1: *Joint Technical Architecture Version 4.0 Hierarchy Model*

5000.2-R [11], dated June 2001, stated that "JTA is required for all new or changes to existing IT, including [National Security Systems] NSS," and that "if the use of a JTA mandated standard will negatively impact cost, schedule, or performance, a DoD CAE or cognizant OSD [Principal Staff Assistant] PSA may grant a waiver from use." For mission critical or mission essential programs, all granted waivers must be submitted for review to still higher levels in OSD. All waiver requests are required to detail the cost, schedule, and performance impacts if the waiver is not granted.

Policy statements such as these clearly indicate DoD's intent for JTA to be implemented; waivers are allowed if justified, but have to be approved at a very high level. JTA continues to evolve: A "final" JTA Version 4.0 became available April 2001, and the multi-phase review process for JTA Version 5.0 is already in progress.

What is JTA?

The Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework Version 2.0 [12] defines three kinds of architecture views for DoD systems. The three views defined are operational architecture (OA), systems architecture (SA), and technical architecture (TA) views. A technical architecture is defined as "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 DoD JTA is such a technical architecture; it achieves its purpose by identifying the interface standards and conventions necessary for DoD to

facilitate information technology interoperability. These standards and conventions facilitate interoperable implementation of the system capabilities described in the SA view, within the operational context described in the OA view.

The structure of the JTA document includes a *core*, four *domain* annexes, and a number of *subdomain* annexes. Figure 1, taken from DoD JTA Version 4.0 [1], shows the hierarchical structure of the JTA and identifies the JTA core, domains, and subdomains.

The JTA core contains common interfaces and standards considered to be applicable to all DoD systems to support interoperability. Domains are intended to identify families of systems. To further support interoperability among the systems of each JTA domain, the corresponding JTA domain annex contains domain-specific JTA standards that are applicable (in addition to those in the JTA core) to the systems of the domain. Similarly, subdomains identify smaller groupings of similar or related systems within a domain; systems within a subdomain must comply with all relevant standards in the JTA core, in the annex for the parent domain, and in the relevant subdomain.

JTA Version 4.0 Structure

The JTA core is divided into sections that contain different kinds of IT standards and guidelines. All of the specifications that are cited as "mandated" in the JTA must enhance interoperability, be technically mature, implementable, and publicly available. The JTA also lists additional standards as "emerging;" their criteria for inclusion are less strict, and they are considered either for elevation to mandated status or for deletion each time the JTA is revised.
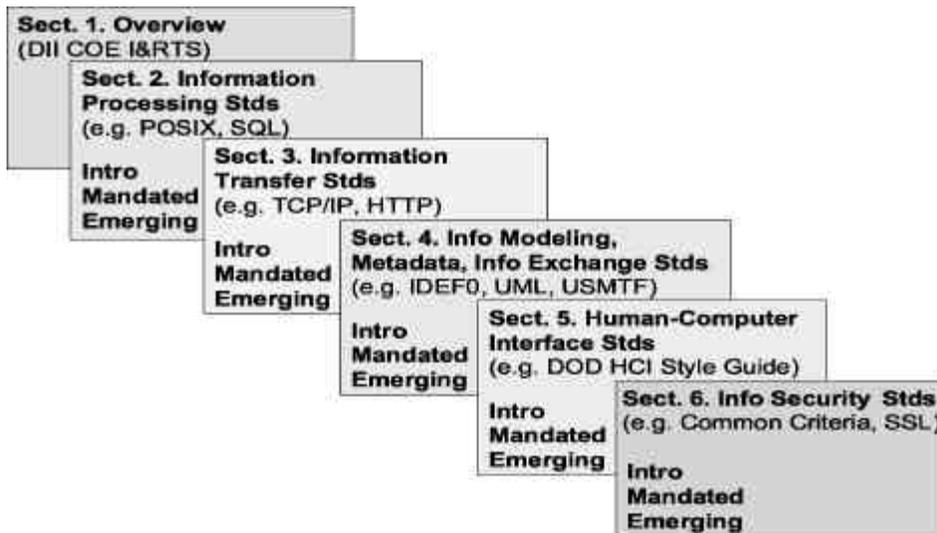
Figure 2: *Structure of the Joint Technical Architecture Core*

Figure 2 shows graphically the structure of the JTA core, with examples of the kinds of standards in each section.

JTA Version 4.0 Section 1 contains an overview of the document and describes a number of related initiatives, including the C4ISR Architecture Framework [12] referred to earlier and the DoD Technical Reference Model (TRM) [13]. It also contains the only policy statements in the JTA itself. In JTA Version 4.0, a new subsection called Policy was introduced into Section 1. One subsection under Policy identifies four key documents[2] applicable for Combined and Coalition Standardization and/or Interoperability, and another subsection mandates use of the DII COE. The remainder of the JTA specifies mandated and emerging information technology standards that are to be complied with whenever applicable.

Compliance with the DII COE is mandated in JTA Section 1 for Command and Control (C2), Combat Support (CS), and Intelligence Systems supporting the Joint Task Forces (JTFs) and Combatant Commands. DII COE is implemented by a set of modular software that provides generic functions or services that are accessed by other software through standard application program interfaces (APIs). DII COE and the levels of DII COE compliance are defined in the DII COE Integration and Runtime Specification (I&RTS) [14], which is identified as one of the mandated standards in the JTA. The JTA further requires that all applications of a system that must be integrated into a DII platform be at least DII COE I&RTS Level 5 compliant with a goal of achieving Level 8. The levels of DII COE compliance are beyond the scope of this article, but as a quick reference, for Level 5 compliance, the system's software would need to be segmented, use the DII COE Kernel, and be installed via COE tools. A brief comparison of JTA and DII COE is presented later in this article. Additional information about DII COE is available in the I&RTS and on the DII COE Web site[3].

JTA core Sections 2 through 6, and the domain and subdomain annexes, contain mandated and emerging information technology standards with brief descriptions and some guidance on when each would apply. Following is an abbreviated discussion of the kinds of standards in each core section, and a very few examples of the standards in the domain annexes. The JTA is available on the Web[4], and the reader is encouraged to browse through the JTA for more information and to look for standards of interest. The standards in these sections of JTA are organized loosely according to the service areas and services defined in the DoD TRM [13].

JTA Section 2 contains standards in a category called Information Processing. These are common software and information technology interface standards such as Portable Operating System Interface (POSIX), Motif, Structured Query Language (SQL), and Common Object Request Broker Architecture (CORBA); some data interchange standards, such as Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and National Imagery Transmission Format (NITF); as well as some of the more widely used *markup language* standards, such as Hypertext Markup Language (HTML) and eXtensible Markup Language (XML). Many of the standards in this section are so prevalent it is hard to find a commercial product to which one of these standards applies that does not comply with that standard.

JTA Section 3 standards are categorized as Information Transfer Standards. These standards include Internet protocols, e-mail, and networking standards. The standards in this section include Simple Mail Transfer Protocol (SMTP), Multipurpose Internet Mail Extension (MIME), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Uniform Resource Locator (URL), and Transmission Control Protocol (TCP)/Internet Protocol (IP). Again, many of these standards are virtually ubiquitous, especially among commercial products. Also in this section are a small number of military standards for which there is no commercial alternative, such as Global Positioning System (GPS) and Military Satellite Communications (MILSATCOM) standards. But as for all of the mandated standards in JTA, these are included only if they are publicly available and widely implemented.

JTA Section 4 is titled Information Modeling, Metadata, and Information Exchange Standards. It includes standards in all three categories. There are modeling

	JTA	DII COE
Contents	Industry and some military specifications and standards	Middleware and infrastructure software and utilities
Features	Interface specifications	Mostly open system products
Software	No software is identified except DII COE	Implemented using DISA-approved COTS and GOTS software
Implementation Context	Compliance with any standard required only if corresponding service is in system; JTA has additional applicability guidance for each standard	I&RTS defines DII COE compliance levels and segmentation, provides rules for interaction among software components
Mandate	Mandated in DoD and DoD Component policies	Mandated in JTA, only for C2, combat support, and intelligence systems

Table 1: *Joint Technical Architecture and Defense Information Infrastructure Common Operating Environment Compared*

standards like Integration Definition (IDEF0), IDEF1X, and Unified Modeling Language (UML); data definition standards such as Defense Data Dictionary System (DDDS); and message formats for information exchange, like Tactical Digital Information Link (TADIL-J) and United States Message Text Format (USMTF).

JTA Section 5 contains Human-Computer Interface (HCI) Standards, including DoD, Motif, and Windows style guides; human-centered design processes; and military symbology standards.

The final section in the JTA core is Section 6, which contains Information Security Standards for various means of protecting confidentiality and integrity of information. Examples include the FORTEZZA Cryptologic Standard; Secure Sockets Layer (SSL) protocol; secure versions of standards that appear in other sections, such as Secure MIME (S/MIME) for encrypted e-mail; and the Common Criteria for evaluation of the strength and functional correctness of Information Assurance products.

The domain and subdomain annexes contain standards that are considered to apply only to specific families of systems so that, for example, the C4ISR Domain includes NITF Extensions, the Modeling & Simulation Domain includes High-Level Architecture (HLA), and the Combat Support domain includes Continuous Acquisition and Life Cycle Support (CALS).

High-Level Comparison of JTA and DII COE

Confusion about the relationship between JTA and DII COE often provokes questions: Is JTA a superset or a subset of DII COE? Can the mandated compliance with JTA be achieved by implementing a system using DII COE? Is selecting a platform that does not support DII COE sufficient grounds for a JTA waiver? To respond simply, the answer to all these questions is "No." JTA mandates the use of DII COE

for certain systems, but complying with JTA means complying with all applicable JTA standards; DII COE implementation does not imply JTA compliance (although it may help, since most DII COE products are also JTA-compliant). Table 1 above contrasts JTA and DII COE.

Program personnel must understand the difference between requirements for JTA compliance and for DII COE compliance. Here are some important points to remember:

- JTA and DII COE compliance are not the same. If a program is required to comply with JTA, then implementing DII COE may also be necessary (i.e., for command and control, combat support, and intelligence systems). However, the relevant JTA standards must still be identified, and the system assessed for compliance with them.
- The scope and application are broader for JTA. DoD policy mandates JTA for all national security systems and IT systems. JTA mandates DII COE compliance only for command and control, combat support, and intelligence systems.
- The impact on program architecture may be greater for DII COE, because it contains software that must be incorporated into the system architecture. But JTA standards may also drive some aspects of the system architecture – it is important to develop a JTA profile while the architectural impact can be minimized.

Complying with JTA

OSD mandates that compliance with all applicable JTA standards must be considered for all new programs and changes to existing programs. What does this mean for a program? JTA contains many industry standards that will be implemented regardless of the mandate, so for those parts of a system, there will be no impact at all. For many other parts of the system, if the JTA standards are kept in mind during the ini-

tial design of the system, then when there are architectural decisions to be made that could make JTA compliance either trivial or difficult to accomplish, the decision can be made to go towards JTA compliance without additional cost. As was mentioned earlier, it is important to remember that DII COE compliance at any level is not sufficient to ensure JTA compliance, even though DII COE compliance is also required for many programs.

The applicable mandated standards in the JTA are expected to be used as the starting set of standards for a system. In a JTA-compliant system, a mandated standard in JTA is intended to be implemented only by systems that have a need for the information technology services specified by that standard. This means both that the service area is one that is required by the program and also that the guidance in the JTA for applicability of the specific standard indicates that it is appropriate for the program's needs. Additional standards (outside of JTA) may be used to meet requirements, but only if they are not in conflict with mandated standards in the JTA.

Implementing JTA on a Program

To implement JTA on a program, the first step is to develop a JTA profile for the system. This will provide the information that is needed either to assess JTA compliance of an existing program or to plan for JTA compliance in a developing program. A simple process for developing a JTA profile is suggested here, but other approaches could be followed:

1. Create a table from the List of Mandated and Emerging Standards (LMES) (called Appendix B in earlier versions of JTA). Include all standards from the JTA core sections, and all standards from any relevant service areas in domain and subdomain annexes. It is important to check all annexes for relevant service areas, even in domains to which the system does not belong.

JTA Section	Currently Mandated Standard	Applicable?	Comply?	Alternate Standard	Comments
2.2.2.1.4.1 Document Interchange	ISO 8879:1986, SGML (with Amendment 1 and Technical Corrigenda 1 and 2)	Y	Y		
	HTML 4.01 Specification	Y	Y		
	XML 1.0	Y	N	Proprietary format	Transitioning to XML in upgrade
2.2.2.1.4.2 Graphics Data Interchange	JPEG File Interchange Format (JFIF), Version 1.02	N			
	PNG Specification, Version 1.0	N			
	GIF, Version 89a	N			

Table 2: *Example Joint Technical Architecture Standards Profile Entries*

2. For each service area, determine whether the service area is applicable to the system.
3. For each applicable service area, identify the standards that are appropriate to the system's needs, using the standard-specific guidance in the JTA. (Note that a standard classified as emerging should not be used if an appropriate mandated standard is available.) Then determine whether the system is/will be compliant with the standards identified.
4. If not, then determine migration plans or justification for non-compliance.

An excerpt from a JTA profile is shown in Table 2 .

The JTA standards profile can be used as a starting point in cases such as these:
• To familiarize designers of a system with relevant standards before design decisions are made.
• To use JTA standards as references for implementers as the system is being developed.
• To develop compliance criteria for testing to ensure that the relevant JTA standards are implemented on the program.
• To establish customers' acceptance criteria.

• To generate migration plans showing JTA standards that will be implemented in later releases of a system, or creating waiver requests if a particular standard cannot be implemented on a system even in the future.

For new programs and changes to existing programs, JTA compliance, and DII COE compliance if applicable, must be in Requests for Proposal and in all relevant contractual documents. The DoD JTA User Guide and Component JTA Management Plan [15] should provide some help with contractual language.

Conclusions

Each DoD Component is responsible for JTA implementation within the Component. Each has unique policies, and additional funding for JTA compliance is often not provided. The OSD direction is clear – JTA is essential to meeting the future requirements for interoperable systems. Getting to this vision of interoperability will be a long-term effort, since JTA compliance is only mandated for new systems and those being upgraded. It is important to realize also that compliance with JTA by

itself will not guarantee interoperability between systems. Common data, selection of common options, and sometimes common software, such as the DII COE, will also be necessary to achieve true interoperability. There are likely to be growing pains in the interim, but the overall goal is vital for the future of our military. ◆

References

1. Joint Technical Architecture Version 4.0, Department of Defense, 2 April 2001.
2. Terms and Definitions, DoD Open Systems Joint Task Force (OS-JTF), <www.acq.osd.mil/osjtf/html/approach_terms.html>, 23 April 1999.
3. Joint Technical Architecture Version 1.0, Department of Defense, 22 Aug. 1996.
4. Kaminski, Paul G. and Emmett Paige. Implementation of the DoD Joint Technical Architecture, 22 Aug. 1996.
5. Joint Technical Architecture Version 2.0, Department of Defense, 26 May 1998.
6. Buchholz, Douglas D., Jacques S. Gansler, and Arthur L. Money. DoD Joint Technical Architecture (JTA) Version 2.0, 30 Nov. 1998.
7. Joint Technical Architecture Version 3.0, Department of Defense, 15 Nov. 1999.
8. Gansler, Jacques S., Arthur L. Money, and John L. Woodward Jr. DoD Joint Technical Architecture (JTA) Version 3.0, 29 Nov. 1999.
9. Joint Technical Architecture Version 3.1, Department of Defense, 31 March 2000.
10. CJCSI 6212.01B: Interoperability and Supportability of National Security Systems, and Information Technology Systems, Chairman of the Joint Chiefs

of Staff, 8 May 2000.

11. DoD Regulation 5000.2-R: Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information System Acquisition Programs, Department of Defense, June 2001.

12. Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework Version 2.0, Department of Defense, 18 Dec. 1997.

13. DoD Technical Reference Model Version 2.0, Department of Defense, 9 April 2001.

14. Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS) Version 4.1, Department of Defense, 3 Oct. 2000.

15. JTA User Guide and Component JTA Management Plan Version 1.0, Draft, Department of Defense, 2001.

Notes

1. The term "DoD Components," as defined in DoD Regulation 5000.2-R [11], refers collectively to "the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Defense Agencies, and DoD Field Activities."

2. The documents identified in JTA Version 4.0 Section 1.6.2 Combined and Coalition Standardization and/or Interoperability are the following:
   • Department of Defense, Directive 2010.6: *Standardization and Interoperability of Weapons Systems and Equipment Within the North Atlantic Treaty Organization*, 5 March1980.
   • Chairman of the Joint Chiefs of Staff, CJCSI 2700.01: *International Military Rationaslization, Standardization, and Interoperability Between the United States and Its Allies and Other Friendly Nations,* 30 Jan. 1995.
   • North Atlantic Treaty Organization (NATO), *Consultation, Command and Control (C3) Technical Architecture (TA) (NC3TA),* 15 Dec. 2000.
   • Allied Communications Publication (ACP) 140, *Combined Interoperability Technical Architecture (CITA)*, 3 May 1999.

3. The DII COE Web site contains such information about DII COE as current implementation status, requirements for changes, future plans, meeting dates for the oversight group and working groups, and links to other relevant Web sites.

Information about DII COE changes regularly, since it involves releases of software that may be updated. For current information, check the DII COE Web site: <http://diicoe.disa.mil/coe>.

4. The DoD JTA Web site contains a great deal of information about JTA, including previous and current versions of the JTA document, recent news regarding JTA, and information on how to participate in the JTA development process. The Web site also contains a list of all the organizations participating in the JTA Development Group, with contact info for the representatives from each DoD Component. Following are URLs for the DoD JTA Web site and the JTA Web sites of the Military Services:
   • DoD JTA:
     <www.jta.itsi.disa.mil>.
   • USAF JTA:
     <www.afca.scott.af.mil/jta-af>.
   • USA JTA:
     <http://arch-odisc4.army.mil>.
   • USN JTA:
     <www.acq-ref.navy.mil>.

About the Author

Judy Kerner is a senior project leader at The Aerospace Corporation in El Segundo, Calif., where she leads activities for the Department of Defense Joint Technical Architecture and related initiatives. Kerner has more than 25 years of experience in software architecture, software engineering, standards, and open systems. She has worked for TRW, Norden Systems, and previously for several commercial organizations. Her assignments have included project management and responsibilities in all phases of the software life cycle, as well as research. Kerner holds a master's degree in computer science from the Polytechnic Institute of New York.

The Aerospace Corporation
P.O. Box 92957
Los Angeles, CA 90009
Phone: (310) 336-6555
Fax: (310) 336-8266
E-mail: judy.kerner@aero.org