

1 JULY 2000



**AIR EDUCATION AND TRAINING COMMAND
Supplement 1**

26 SEPTEMBER 2001

Communications and Information

**JOINT TECHNICAL ARCHITECTURE – AIR
FORCE**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://afpubs.hq.af.mil>.

OPR: HQ AFCA/ITLD (Mr. Douglas W. Gray)

Certified by: HQ USAF/SCXX
(Lt Col Terry G. Pricer, Sr.)

Pages: 19

Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*. It mandates the Joint Technical Architecture – Air Force (JTA-AF) and describes implementation details, roles, and responsibilities. This instruction applies to all Air Force organizations and personnel involved in planning, designing, engineering, and managing the acquisition, installation and modification of Air Force information technology (IT) systems. In addition, it also applies to Air National Guard units when stationed on active duty bases and connected to the base infrastructure. This instruction supports the Department of Defense (DoD) 5000-series acquisition procurement publications. Address technical questions on this instruction to Headquarters Air Force Communications Agency (HQ AFCA/ITLD), 203 W. Losey Street, Room 1065, Scott AFB IL 62225-5222. Send recommended changes or comments to HQ AFCA/ITPP, 203 W. Losey Street, Room 1065, Scott AFB IL 62225-5222, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCIC/ITAT. Refer to **Attachment 1** for a glossary of references and supporting information. Maintain and dispose of all records created as a result of prescribed processes in accordance with Air Force Manual (AFMAN) 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-322V4).

(AETC) AFI 33-133, 1 July 2000, is supplemented as follows:

Maintain and dispose of records created as a result of processes prescribed in this publication in accordance with AFMAN 37-139, *Records Disposition Schedule* (will become AFMAN 33-322, Volume 4). This supplement does not apply to the Air National Guard or the Air Force Reserve Command.

This supplement contains requirements and detailed guidance for implementing the use of the Joint Technical Architecture—Air Force (JTA-AF) and AETC enterprise information technology (IT) architecture technical profiles for planning, developing, and acquiring IT systems and associated components in AETC. This supplement provides guidance to measure technical architectural compliance. It also pro-

vides general guidance for requesting a noncompliance waiver and recommending changes to AETC IT architectural baselines and the JTA-AF through the AETC IT Enterprise Configuration Control Board (CCB). Submit recommendations to change or improve this supplement to HQ AETC/SCXI, 61 Main Circle, Suite B, Randolph AFB TX 78150-4545.

1. Purpose . The JTA-AF is the IT technical architecture for the Air Force. It assists the Air Force in meeting the requirements of Title 40 U.S.C., Chapter 25, 1401 et seq., Public Law 104-208, 30 Sep 96, *Clinger-Cohen Act, 1996* (formally the *Information Technology Management Reform Act*) to achieve an interoperable IT infrastructure and reduces costs of ownership. While the DoD Joint Technical Architecture (DoD JTA) mandates a core set of standards, the JTA-AF tailors and refines them for Air Force use. The JTA-AF also provides additional standards, standards profiles, recommended products, IT infrastructure architectures, and guidance not included in the DoD JTA. The JTA-AF encompasses the DoD JTA and, as such, is the single Air Force source for IT standards and products guidance. The JTA-AF and associated implementation plan, compliance procedures, configuration control processes, compliance database, and tools are available on the JTA-AF Web page,

<http://www.afca.scott.af.mil/jta-af/index.html>.

1.1. The JTA-AF Implementation Plan documents the Air Force approach to implementing the DoD JTA. The plan contains detailed implementation processes for the configuration management of JTA-AF, including Configuration Control Board (CCB) Charter/structure/management, Request For Change (RFC) submittal format/content/process, detailed process relationships between: JTA-AF, *Defense Information Infrastructure Common Operating Environment (DII COE)*, *JTA-AF Recommended Products*, and *DoD JTA*. The *JTA-AF Implementation Plan* will also contain the database requirements/maintenance to be provided by AFCA to support the status reports to be made available to the Air Force Chief Information Officer (AF-CIO), Air Force Acquisition Executive (AFAE), Office of the Secretary of Defense (OSD) and associated staffs, as required in the *Air Force Implementation Plan for the DoD Joint Technical Architecture (JTA)*, 1 December 1998.

1.2. (Added-AETC) The guidance of the JTA-AF is a critical source for developing the AETC Enterprise IT Architecture technical profiles. The use of these technical profiles:

1.2.1. (AETC) Provides guidance on minimum configurations and recommended products to expedite the development of common user IT solutions and acquisitions for the command.

1.2.2. (AETC) Provides practical technical architecture guidelines for integrating IT systems and components into the AETC IT Enterprise.

1.2.3. (AETC) Ensures emerging IT systems properly integrate with AETC, Air Force, and DoD IT architectures. **NOTE:** AETC technical profiles and associated web pages are available on the AETC IT Architecture web site (<https://www.aetc.af.mil/cio/architecture/index.html>).

1.2.4. (AETC) Is required by the AETC Chief Information Officer (CIO). These profiles reflect the technical architecture view of the AETC Enterprise IT Architecture and are intended to complement the JTA-AF guidance and IT goals of the command.

2. Policy . The use of JTA-AF standards and standards profiles are mandated for all Air Force IT acquisitions. Air Force users must use JTA-AF recommended products and IT infrastructure architectures whenever feasible to foster interoperability, assure mission success, commonality, and reduce cost of

ownership. Competitively awarded contracts will include a list of recommended JTA-AF products. The JTA-AF recommended products list is posted on the JTA-AF Web page.

2.1. Applicability. Air Force IT refers to all information processing and information transmission systems in the Air Force inventory. This includes command and control (C2) (composed of all mission areas including combat support), global networks, data processing facilities, communications systems, wireless systems, modeling and simulation tools, and common office automation systems (e.g., desktop computers, word-processing software, electronic mail [E-mail] software, etc.). The JTA-AF also specifies the interface standards of those systems with other key assets (e.g., weapon systems and sensors) to support critical warfighter interoperability. The JTA-AF does not apply to the internal design of airborne weapons systems areas (requirements) dealing with avionics/weapons/electronics (AWE) needed to maintain safety of flight, combat air maneuvers, ordinance delivery, or operational flight as their primary mission functions. The JTA-AF does apply to those airborne weapon systems that provide as their primary mission function: C2 or intelligence information, and external communications interfaces to other weapons systems and systems supporting the JTFs and CINCs. Exclusions other than as noted above must have a waiver (see paragraph 2.2.).

2.1.1. The JTA-AF compliance is mandatory for all new systems and for upgrades to existing systems. JTA-AF implementation is required for:

- 2.1.1.1. All DoD acquisition categories (ACAT).
- 2.1.1.2. Spiral development acquisitions.
- 2.1.1.3. *Advanced concept technology demonstrations (ACTD).
- 2.1.1.4. *Advanced technology demonstrations (ATD).
- 2.1.1.5. *Joint warrior interoperability demonstrations (JWID).
- 2.1.1.6. *Joint expeditionary force experiments (JEFX).
- 2.1.1.7. *Battle laboratory projects and similar programs.

* These programs must use the JTA-AF for guidance in developing interfaces. It is not the intention of the JTA-AF to stifle new and emerging technology--program advocates must comply with JTA-AF compliance requirements. If additional units are needed beyond the residual capability, the additional buys shall constitute an acquisition program.

2.2. Implementation. The essential components of implementation are compliance, compliance assessment, migration plan, and waiver. Compliance refers to a particular IT system. A compliant system is designed and built in accordance with all of the applicable standards and guidance in the JTA-AF. Compliance assessment is the process to determine if a system is compliant and/or what additional criteria you must meet to achieve compliance. A migration plan is a schedule of intermediate steps that, when completed, result in a JTA-AF compliant system, and a waiver is a one-time exemption for a JTA-AF mandated standard. A waiver, once granted, is valid until the next major system upgrade, block change and/or other engineering change proposal (ECP) that changes the production baseline. The *Air Force Implementation Plan for the DoD Joint Technical Architecture (JTA)*, 1 December 1998, available on the JTA-AF Web page (<http://www.afca.scott.af.mil/jta-af/index.html>), details how and when each of these components are accomplished.

2.2.1. (Added-AETC) AETC Approach to JTA-AF Implementation:

2.2.1.1. (AETC) Together, the JTA-AF and the AETC IT technical profiles will be used by all AETC organizations and personnel involved in planning, developing, and acquiring IT systems and associated hardware and software. In the event of inconsistency between the JTA-AF and the AETC technical profiles, the JTA-AF will take precedence. Applicable AETC IT systems will be JTA-AF compliant.

2.2.1.2. (AETC) Actions described in this supplement are required for projects and programs (non-DoD 5000-series programs) implemented in accordance with 33-series AFIs. Education and Training Technology Application Program (ETTAP) proposals and prototypes for IT systems are considered advanced concept technology demonstrations (ACTD) as defined in the basic AFI. To ensure innovative ETTAP ideas and projects are not stifled, IT systems developed through ETTAP must use applicable JTA-AF and AETC IT technical profiles guidance only when developing interfaces with other Air Force or AETC IT systems.

2.2.2. (Added-AETC) JTA-AF Compliance Assessment:

2.2.2.1. (AETC) In all emerging AETC IT systems, the project or program manager will conduct a JTA-AF compliance assessment of the system. In addition, a JTA-AF compliance assessment will be incorporated in the system's command, control, communications, computer, and intelligence support plan (C4ISP). The documented JTA-AF compliance assessment is considered the technical architecture view (TV-1) for a C4ISP.

2.2.2.2. (AETC) The compliance assessment will identify the applicable JTA-AF standards, recommended products required for the implementation of the IT system, and determine if the system is in compliance. For Air Force downward-directed IT systems, the system program office (SPO) is required to conduct the compliance assessment and incorporate it into the C4ISP. For MAJCOM-unique or base-level systems, the program or project manager for the system is required to conduct and document the compliance assessment.

2.2.2.3. (AETC) This compliance assessment is an integral part of the interoperability certification of a system to verify its compliance with DoD and Air Force standards. An example of a technical architecture compliance matrix is shown in **Attachment 2 (Added)**, this supplement.

2.2.2.4. (AETC) For an existing IT system with no plans for upgrade or replacement, a compliance assessment may be conducted to document noncompliance, to include the projected date when the system may be retired. No further action is required.

2.2.2.5. (AETC) For an existing IT system that will undergo an upgrade or replacement or for a system under development, a compliance assessment is required. If a system has specific service areas that are noncompliant with the JTA-AF and/or AETC technical profiles, a compliance waiver request will be submitted to HQ AETC/SCXI (per paragraph **2.2.4. (Added)**[AETC], this supplement) or a compliance migration plan will be developed (per paragraph **2.2.3. (Added)**[AETC]), this supplement).

2.2.3. (Added-AETC) Compliance Migration Plan:

2.2.3.1. (AETC) If an emerging or existing IT system is noncompliant with the applicable standards and products, a compliance migration plan will be developed or a compliance waiver request will be submitted to HQ AETC/SCXI (per paragraph **2.2.4. (Added)**[AETC]), this supplement). A migration plan or an approved waiver request is also a requirement of the

system's C4ISP. **NOTE:** If a compliance waiver request is disapproved, a compliance migration plan is still required to be developed and documented in the C4ISP.

2.2.3.2. (AETC) As a minimum, a compliance migration plan will address the following:

2.2.3.2.1. (AETC) System Information. This will include the name or type of system, name of higher level systems that will be supported or have an interface, noncompliant technical standards and system components (hardware and software), and current level of defense information infrastructure-common operating environment (DII-COE) compliance, if applicable.

2.2.3.2.2. (AETC) Migration Data. This will include the schedule of corrective actions or impacts required to achieve compliance, estimated cost (annually, one-time) to achieve compliance, estimated timeline to achieve compliance, and estimated change of annual maintenance or operational cost as a result of achieving compliance, if any.

2.2.3.3. (AETC) If a system under development requires data element standardization, the compliance migration plan must also comply with guidance prescribed in the AETC Sup 1 to AFI 33-110, *Data Administration Program*.

2.2.4. (Added-AETC) Compliance Waiver Request:

2.2.4.1. (AETC) A waiver may be requested if the use of a JTA-AF standard, AETC standard, and/or recommended product does not result in sufficient improvement in system functionality or does not meet a unique user requirement. The waiver documentation must contain fair, accurate, and objective descriptions of the cost (if applicable), benefits, and/or impact if the waiver is not granted. The format for a waiver request is shown in **Attachment 3 (Added)**, this supplement. **NOTE:** A waiver may not be requested for data standardization compliance. See the AETC Sup 1 to AFI 33-110 for data standardization guidance.

2.2.4.2. (AETC) The process for requesting a waiver is as follows:

2.2.4.2.1. (AETC) The waiver request will be prepared by the project manager or organization responsible for the system and forwarded to HQ AETC/SCXI for final processing through the AETC IT Enterprise CCB. If the requesting organization (base tenant) is not a headquarters organization, the base-level communications and information systems officer (CSO) must formally coordinate and concur with waiver request before the process can be continued.

2.2.4.2.2. (AETC) If the base-level CSO concurs with the waiver request, he or she will indorse and forward the waiver to HQ AETC/SCXI for final processing. If the waiver request concerns a standard mandated by the JTA-AF, the AETC IT Enterprise CCB will review and endorse the request and submit it to HQ USAF/SC for final approval. All other waiver requests will be evaluated by the AETC IT Enterprise CCB to form a final recommendation to the AETC Chief Information Officer (CIO) for approval or disapproval. HQ AETC/SCXI will provide the requesting organization with the final decision on waiver approval or disapproval within 30 workdays of receipt. Submit request for waivers to HQ AETC/SCXI via e-mail (<mailto:hqaetcsxi@randolph.af.mil>) or to 61 Main Circle, Suite 2, Randolph AFB TX 78150-4545.

2.2.5. (Added-AETC) Request For Change (RFC) Process:

2.2.5.1. (AETC) An RFC is the required documentation for proposing a change to JTA-AF and AETC IT architectural baselines. It is the mechanism for proposing a standard IT technical solution for use throughout the Air Force.

2.2.5.2. (AETC) Each RFC will be prepared by the project manager or primary organization responsible for the change proposal. AETC RFCs will be developed in accordance with the format specified in **Attachment 4 (Added)**, this supplement, and submitted to the AETC IT Enterprise CCB for evaluation and processing. Submit RFCs to HQ AETC/SCXI via e-mail (<mailto:hqaetcscxi@randolph.af.mil>) or to 61 Main Circle, Suite 2, Randolph AFB TX 78150-4545.

2.3. Data Collection and Reporting. The mechanism for collecting and maintaining information on the implementation components is the JTA-AF Compliance Database Management System (CDBMS), accessible via the JTA-AF Web page (<http://www.afca.scott.af.mil/jta-af/index.html>). HQ USAF Report Control Symbol (RCS) HAF-SC (A) 0001 applies. The JTA-AF CDBMS is used for all compliance assessments and will facilitate the development of migration plans and waivers by providing templates with instructions for their completion and processing. The reporting capability of the system is a beneficial tool for managers/leaders interested in tracking the status of JTA-AF compliance in the Air Force and making planning decisions. Refer to the JTA-AF Implementation Guide for specific information on reporting requirements and instructions.

2.4. Configuration Control Board (CCB). The JTA-AF CCB, in support of the CIO, works to achieve Air Force consensus on JTA-AF related issues. The CCB is the governing body for considering and approving changes to the JTA-AF and the *Joint Technical Architecture - Air Force Configuration Control Board Organizational Charter*, 20 March 1998 (which governs the CCB). The RFC is the mechanism for submitting changes for consideration by the CCB. The RFC format and on-line submission instructions are provided on the JTA-AF Web page (<http://www.afca.scott.af.mil/jta-af/index.html>).

2.4.1. The CCB will represent the Air Force on issues relating to the DoD JTA and the ESC/DI on issues relating to *Defense Information Infrastructure Common Operating Environment (DII COE)*.

2.4.2. (Added-AETC) AETC IT Enterprise Configuration Control Board (CCB):

2.4.2.1. (AETC) The AETC IT Enterprise CCB is the key element for configuration control of the AETC IT Enterprise. In support of the AETC CIO, the AETC IT Enterprise CCB is the management forum for (1) establishing and documenting command positions on RFC proposals to the JTA-AF, (2) approving or disapproving applicable waiver requests, and (3) approving or disapproving RFCs to existing AETC IT architectural baselines.

2.4.2.2. (AETC) The AETC IT Enterprise CCB Charter, available on the AETC IT Architecture web page (<https://www.aetc.af.mil/cio/architecture/index.html>), details the CCB's objectives, review criteria, membership, and general process. The charter supports AFI 33-101, *Communications and Information Management Guidance and Responsibilities*, which makes AETC's communications and information staff element (HQ AETC/SC) responsible for ensuring the integrity and interoperability of systems by employing configuration management.

2.5. JTA-AF Implementation Roles and Responsibilities.

- 2.5.1. AF-CIO. Acts as approval authority for *JTA-AF Implementation Plan*.
- 2.5.2. CIO Management Board:
 - 2.5.2.1. For 5000-series programs, reviews and recommends approval of waiver requests.
- 2.5.3. SAF/AQ:
 - 2.5.3.1. Supports HQ AFCIC/IT in developing the *Air Force Implementation Plan for the DoD JTA*.
 - 2.5.3.2. Supports AFCA in developing the *JTA-AF Implementation Plan*.
 - 2.5.3.3. As AFAE, approves waivers for acquisition programs.
- 2.5.4. HQ USAF/SC:
 - 2.5.4.1. Recommends approval of waiver request packages prior to submission to the CIO Management Board.
- 2.5.5. HQ AFCIC/IT:
 - 2.5.5.1. Manages the JTA-AF.
 - 2.5.5.2. Chairs the CCB.
 - 2.5.5.3. Develops and maintains the *Air Force Implementation Plan for the DoD JTA*.
 - 2.5.5.4. Reviews waiver request packages prior to submission to the HQ USAF/SC and CIO Management Board.
 - 2.5.5.5. Sends copies of the approved waiver request package to HQ AFCA/IT for tracking.
 - 2.5.5.6. Separates and forwards required waiver packages to Under Secretary of Defense (USD[AL&T]) and ASD (C3I).
- 2.5.6. Air Staff Functionals and Major Commands (MAJCOM):
 - 2.5.6.1. Incorporate the requirement for JTA-AF compliance into mission area plans (MAP) and mission support plans (MSP) according to AFI 10-1401, *Modernization Planning Documentation*.
 - 2.5.6.2. Include the requirement for JTA-AF compliance in mission need statements (MNS), operational requirements documents (ORD), and program objective memorandums (POM) according to AFI 10-601, *Mission Needs and Operational Requirements Guidance and Procedures*, and AFI 65-601V1, *Budget Guidance and Procedures*.
 - 2.5.6.3. Include JTA-AF compliance requirement in mission area assessment (MAA) and mission need analysis (MNA) according to AFI 10-601.
 - 2.5.6.4. Concur with migration plans, as appropriate.
 - 2.5.6.5. Concur with waiver requests, as appropriate.
- 2.5.7. Program Executive Officer (PEO)/Designated Acquisition Commander (DAC):
 - 2.5.7.1. Require Air Force-level project managers (AF PM) to report, during existing reviews for 5000-series programs, their efforts toward meeting JTA-AF requirements.
 - 2.5.7.2. Process and concur with waiver request packages, as appropriate, for 5000-series pro-

grams prior to milestone decision authority (MDA) review.

2.5.8. AF PM:

2.5.8.1. Ensure JTA-AF compliance in programs/projects.

2.5.8.2. Complete a compliance assessment for programs/projects.

2.5.8.3. Develop a migration plan for remedying deficiencies or securing an appropriate waiver.

2.5.8.4. Enter implementation data (compliance assessment, waiver data, and migration plan data) into the CDBMS and update the data when there is a change such as system upgrade, new system, or JTA-AF revision. Review JTA-AF for revisions at least annually.

2.5.9. MAJCOM/Base-Level Project Manager/Base Level Program Manager:

2.5.9.1. Provide technical solutions using JTA-AF compliant products and/or JTA-AF recommended products.

2.5.9.2. Provide JTA-AF requirements to base contracting for inclusion in new contracting documents.

2.5.9.3. Assist AF PM in unit-level migration plan or waiver procedures.

2.5.10. MDA or Equivalent:

2.5.10.1. Certify compliance assessments during program reviews for 5000-series programs.

2.5.10.2. Approve migration plans during program reviews for 5000-series programs.

2.5.10.3. Review and recommend approval of waiver requests for 5000-series programs prior to submission to the CIO Management Board.

2.5.11. HQ AFCA:

2.5.11.1. Develops and maintains JTA-AF.

2.5.11.2. Provides training and tools to facilitate JTA-AF compliance

2.5.11.3. Serves as Secretariat of the CCB.

2.5.11.4. Develops and maintains the CCB Charter.

2.5.11.5. Supports HQ AFCIC/IT in developing the *Air Force Implementation Plan for the DoD JTA*.

2.5.11.6. Develops and maintains the Technical Architecture Smart Assistant (TSA).

2.5.11.7. Develops and maintains the JTA-AF CDBMS.

2.5.11.8. Develops and maintains the *JTA-AF Implementation Plan*.

JOHN L. WOODWARD, JR., Lt General, USAF
Director, Communications and Information

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

Title 40 U.S.C., Chapter 25, 1401 et seq., Public Law 104-208, 30 Sep 96, *Clinger-Cohen Act, 1996* (formally the *Information Technology Management Reform Act*)

OSD JTA Policy Memorandum, *Implementation of the DoD Joint Technical Architecture*, August 22, 1996

DoDD 4630.5, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems*, November 12, 1992

DoDI 4630.8, *Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems*, November 18, 1992

DoD Joint Technical Architecture (DoD JTA)

C4ISR Architecture Framework Version 2.0, 18 December 1997

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3500.04A, *Universal Joint Task List*, 13 September 1996

Air Force Implementation Plan for the DoD Joint Technical Architecture (JTA), 1 December 1998

AFI 10-601, *Mission Needs and Operational Requirements Guidance and Procedures*

AFI 10-1401, *Modernization Planning Documentation*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-322V4)

AFI 65-601V1, *Budget Guidance and Procedures*

Defense Information Infrastructure Common Operating Environment (DII COE)

Joint Technical Architecture - Air Force (JTA-AF)

Joint Technical Architecture - Air Force Configuration Control Board (CCB) Organizational Charter, 20 March 1998

References (Added-AETC)

AFI 33-101, *Communications and Information Management Guidance and Responsibilities*

AFI 33-110, *Data Administration Program* (and its AETC Sup 1)

Abbreviations and Acronyms

ACAT—Acquisition Category

ACTD—Advanced Concept Technology Demonstration

AFAE—Air Force Acquisition Executive

AFCA—Air Force Communications Agency

AF-CIO—Air Force Chief Information Officer

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AF PM—Air Force Program Manager

AIS—Automated Information System

ASD—Assistant Secretary of Defense

ATD—Advanced Technology Demonstration

AWE—Avionics/Weapons/Electronics

C2—Command and Control

C4ISR—Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

CCB—Configuration Control Board

CDBMS—Compliance Database Management System

CIO—Chief Information Officer

DAC—Designated Acquisition Commander

DII COE—Defense Information Infrastructure Common Operating Environment

DoD—Department of Defense

DoD JTA—DoD Joint Technical Architecture

E-mail—Electronic Mail

IT—Information Technology

JEFX—Joint Expeditionary Force Experiment

JTA—Joint Technical Architecture

JTA-AF—Joint Technical Architecture – Air Force

JWID—Joint Warrior Interoperability Demonstration

MAA—Mission Area Assessment

MAJCOM—Major Command

MAP—Mission Area Plan

MDA—Milestone Decision Authority

MNA—Mission Need Analysis

MNS—Mission Need Statement

MSP—Mission Support Plan

ORD—Operational Requirements Document

OSD—Office of the Secretary of Defense
PEO—Program Executive Officer
PM—Program Manager
POM—Program Objective Memorandum
RCS—Report Control Symbol
RFC—Request for Change
SIGINT—Signal Intelligence
TSA—Technical Architecture Smart Assistant
USD—Under Secretary of Defense

Abbreviations and Acronyms (Added-AETC)

C4ISP—command, control, communications, computer, and intelligence support plan
CIO—chief information officer
CSO—communications and information system officer
ETTAP—Education and Training Application Program
IT/NSS—information technology/National Security System
POC—point of contact
SPO—system program office
TV-1—technical architecture view

Terms

Advanced Concept Technology Demonstrations (ACTD)—ACTDs are a means of demonstrating the use of emerging or mature technology to address critical military needs. They are not acquisition programs, although they are designed to provide a residual, usable capability upon completion.

Information Technology (IT)—1. With respect to an executive agency, means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. It includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. IT does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.
2. Any planned modification to an operational capability which produces, uses, or exchanges information in any form electronically; which crosses a functional boundary or boundaries among Component, Allied, or Combined Forces; and which produces an operational capability for the warfighter or other DoD decision maker. This technology includes: automated information systems (AIS), communications/computers interface to and among weapon systems communications/computer interfaces and among tactical signal intelligence (SIGINT) systems, and the DoD communications and information technology infrastructure.

Information Technology Architecture—An integrated framework for evolving or maintaining existing

information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals. **NOTE:** The *Clinger-Cohen Act* defines "Information Technology Architecture" with respect to Executive Branch agencies.

Joint Warrior Interoperability Demonstration (JWID) and Similar Programs JWIDs are Joint Staff-sponsored demonstrations of evolving command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) technologies and joint/combined interoperability solutions. The capabilities and C4ISR processes are presented to the CINCs, military services, and agencies in a joint operational environment that allows the warfighters of all services to assess their value in solving current warfighting and interoperability deficiencies, and recommend them for implementation or further refinement.

Technical Architecture View—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. (*C4ISR Architecture Framework Version 2.0*, 18 December 1997)

Key World Wide Web Information Sources

ASD C3I: http://www.c3i.osd.mil/org/cio/i3/AWG_Digital_Library/pdffdocs/fw.pdf

SAF AQ: <http://www.safaq.hq.af.mil/>

CJCSM 3500.04A, Universal Joint Task List, 13 September 1996:

<http://www.dtic.mil/doctrine/jel/cjcsd/cjcsm.htm>

DoD JTA: <http://www-jta.itsi.disa.mil>

DoDD 4630.5, Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems: <http://jite-emh.army.mil/ciidocs.htm#4630.5>

DODI 4630.8, Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems, November 18, 1992:

<http://jite-emh.army.mil/ciidocs.htm#4630.8>

OSD JTA Policy Memorandum, Implementation of the DoD Joint Technical Architecture, August 22, 1996: <http://www-jta.itsi.disa.mil/jta/jtamemo.html>

JTA-AF Web page: <http://www.afca.scott.af.mil/jta-af/index.html>

Air Force Implementation Plan for the DoD JTA: <http://www.afca.scott.af.mil/jta-af>

AF-CIO Management Board Web Page: <http://www.cio.hq.af.mil/ciomb.htm>

ATTACHMENT 2 (ADDED-AETC)

TECHNICAL ARCHITECTURE COMPLIANCE MATRIX (SAMPLE)

(Program Title)

Information Processing Mandated Standards

A	B	C
JTA-AF Section and Service Area	Mandated Standard, Title, and Date	Program Title Status
2.2.2.1.2. User Interface Services	FIPS Pub 158-1: 1993. User Interface Component of the Application Portability Profile X-Windows Version 11, Release 5.	Compliant
	X/Open c323, Common Desktop Environment (CDE) Version 1.0, April 1995.	Compliant
2.2.2.1.3. Data Management Services	FIPS Pub 127-2: 1993. Database Language for Relational DBMS.	Compliant
2.4.2.2. Data Model	DoD 8320.1-M-1, Data Standardization Procedures, April 1998	Compliant

Information Transfer Mandated Standards

A	B	C
JTA-AF Section and Service Area	Mandated Standard, Title, and Date	Program X Status
Domain Name System (DNS)	IAB Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987	Compliant
3.2.1.1.1.3. File Transfer	IAB Standard 9/RFC-959, File Transfer Protocol, October 1985	Compliant
3.2.1.1.1.4. Remote Terminal	IAB Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983.	Not Used
3.2.1.1.1.5 Network Management	IAB Standard 15/RFC-1157, Simple Network Management Protocol (SNMP), May 1990	Compliant

Human-Computer Interfaces Mandated Standards

A	B	C
JTA-AF Section and Service Area	Mandated Standard, Title, and Date	Program X Status
5.2.1. General	DoD HCI Style Guide, TAFIM Version 2.0, Volume 8, 30 September, 1994.	Compliant
5.2.2.1. Commercial Style Guides	Open Software Foundation (OSF)/Motif™ Style Guide, Revision 1.2 (OSF 1992)	Compliant
5.2.2.2. DoD HCI Style Guide	DoD HCI Style Guide, TAFIM Version 2.0, Volume 8, 30 September, 1994.	Compliant

Information Systems Security Mandated Standards

A	B	C
JTA-AF Section and Service Area	Mandated Standard, Title, and Date	Program X Status
6.2.2.1. Application Software Entity Security Standards	DoD 5200.28-STD, The Department of Defense Trusted Computer System Evaluation Criteria, December 1985	Compliant
	NCSC-TG-021, Version 1, Trusted Database Management System Interpretation, April 1991	Compliant
6.2.2.2.1. Operating System Services Security	DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985	Compliant
6.2.3.1.1.1. Security Algorithms	FIBS PUB 180-1, Secure Hash Standard, NIST, April 1995	NA
	FIPS PUB 186, Digital Signature Standard, NIST, May 1994	NA
6.2.3.1.1.2 Security Protocols	MIL-STD-2045-48501, Common Security Label	Compliant

Recommended Products

A	B	C
JTA-AF Section and Service Area	Recommended Product	Program X Status
Section 5; Network Operating System	Windows NT Server 5.0	Compliant
Sections 5; Desktop Operating System	Windows NT Workstation	Compliant
Section 5; Internal Router	Cisco 7507	Not Used
Section 5; Internal Switch	Cisco Catalyst 2900	Compliant

ATTACHMENT 3 (ADDED-AETC)**FORMAT FOR A COMPLIANCE WAIVER REQUEST**

MEMORANDUM FOR HQ AETC/SCXI

FROM: _____

SUBJECT: Request for a Compliance Waiver

- 1. System, Equipment, and Product Background Information.** *Describe the background information that initiated the waiver request.*
- 2. Justification.** *Describe the justification for the waiver request.*
- 3. Impact to Interoperability if Waiver Is Approved.** *Describe the negative impacts, if any, that would result from noncompliance with the JTA-AF and/or AETC IT Architecture.*
- 4. Impact if Waiver Is Not Approved.** *Describe the negative impacts, if any, that would result if the waiver is not approved.*

Signature (see note)

NOTE: This should be the signature of the requestor approval authority or base-level CSO. If the requesting organization (base tenant) is not a headquarters organization, the base-level CSO must endorse the request for waiver.

ATTACHMENT 4 (ADDED-AETC)

FORMAT FOR A REQUEST FOR CHANGE (RFC) FOR IT ARCHITECTURE

INSTRUCTIONS: Using the format below, send the initial RFC for IT architecture to HQ AETC/SCXI as an attachment to a memorandum. The package may be submitted in one of the following ways: (1) by mail (HQ AETC/SCXI, 61 Main Circle, Suite 2, Randolph AFB TX 78150-4545); (2) by e-mail (<mailto:hqaetcsxci@randolph.af.mil>); or (3) by fax (DSN 487-4469 or Comm 210-652-4469). Ensure each initial RFC contains as much of the following information as possible and limit each RFC to one recommended product, issue, or change. HQ AETC/SCXI will provide assistance as required and will forward the RFC to the AETC IT Enterprise CCB.

1. Recommended Change:

1.1. Target Document. *Identify the areas the change will affect; for example, JTA-AF, AETC IT Enterprise CCB charter, or AETC IT Architecture, including technical profiles, minimum configurations, etc. Also identify the specific section or component to which the initial RFC refers; for example, AETC IT architecture technical view or profile, server minimum hardware configuration, etc.*

1.2. Summary. *Provide a short executive summary of the initial RFC, indicating what is being proposed, who the RFC impacts, why the change is needed, how it will be implemented, and what benefit will be provided.*

2. Scope. *Identify the proposed range of applicability for the recommended change as determined by the sponsoring RFC point of contract (POC). Indicate whether the RFC is for a specific IT domain (for example, e-mail, network management, voice network) or a functional group (for example, civil engineering, communications and information) and whether it applies AETC wide or Air Force wide.*

3. Requirements. *Identify the requirements the RFC will satisfy. Define the goals of each recommendation, including operational or user requirements, critical characteristics, logistics and readiness, performance, training, interoperability, or other requirements, as required. If possible, reference a requirements document such as an information technology/National Security System (IT/NSS) requirements document, mission need statement (MNS), or operational requirements document (ORD).*

4. Alternatives. *Consider the proposed change and leading alternatives (that is, the current approach and competing approaches). If there are multiple alternatives, limit the number identified to the top two or three. Include the following items for the proposed change and alternatives being considered:*

4.1. Short Overview and Description. *Provide a short overview and description of each alternative.*

4.2. Requirements Correlation Matrix. *For each requirement listed in paragraph 3 of this RFC, identify whether the alternative satisfies the requirement. Also identify how the alternative satisfies the requirement or why it does not. The following table is an example of a requirements correlation matrix:*

Requirement	Product 1	Product 2	Product 3
1	Yes	Yes	No
2	Yes	Yes	Yes
3	Yes	No	Yes
4	Yes	Yes	No

4.3. Cost Data. *The cost data is an integral part of the alternative analysis which deals with real economical rationale for deciding whether to pursue one alternative over another. The cost data lists all costs incurred by AETC or Air Force for adopting a standard or recommended product. The incurred costs should be directly related to the implementation of the chosen alternative at the time the implementation is performed. Consider the questions below for the recommended product and all alternate products. Take discounts for quantity purchases into account and describe them.*

4.3.1. *What hardware and software applications make up this product?*

4.3.2. *What hardware and software systems or subsystems make up this product?*

4.3.3. *For all systems and applications:*

4.3.3.1. *What quantities are to be purchased?*

4.3.3.2. *How many locations are involved and where are they?*

4.3.3.3. *What are the costs of these applications and systems?*

4.3.3.4. *What are the licensing fees and terms associated with the product?*

4.3.3.5. *What are the costs of publications, manuals, and technical data revision not included in purchase costs?*

4.3.3.6. *How many different government publications (for example, AFIs, technical manuals) will require preparation or revision, if any? What will it cost to prepare or revise these publications?*

4.3.3.7. *What are the integration or interface costs, if any?*

4.3.3.8. *Will any testing be required for this product and are there any costs?*

4.3.3.9. *What are the manpower costs of operations or maintenance personnel for the product?*

4.3.3.10. *What are the training costs of operations or maintenance personnel for the product?*

4.3.3.11. *What are the support equipment costs?*

4.3.3.12. *What are the site installation costs?*

4.3.3.13. *What are the costs for initial spares and repair parts?*

4.4. Known Deficiencies. *Address known problems within the standards or product, such as missing features.*

4.5. Acquisition Strategy. *Identify existing contracts for the product (for example, Desktop V, ULANA II, DMS, DISA, and GSA Schedule).*

5. Justification. *Provide other supporting rationale for the recommendations.*

6. Point of Contact (POC). *Identify an RFC POC. Provide his or her name, organization, mailing address, telephone number, fax number, and e-mail address.*

7. Other Relevant Documentation. *Include any other documentation relevant to the RFC. Include informative references, business case analyses, test data, and/or supporting documentation.*