

**BY ORDER OF THE COMMANDER
AIR EDUCATION AND TRAINING
COMMAND**



AIR FORCE INSTRUCTION 33-133

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 AETC/SCXI (Mr A. Cephas)

Certified by: HQ AETC/SCX (Lt Col Taglieri)

Pages: 12

Distribution: F

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 provides 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.

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

1.2.3. 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. 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.

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

2.2.1.1. 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. 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) JTA-AF Compliance Assessment:

2.2.2.1. 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. 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. 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. 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. 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) Compliance Migration Plan:

2.2.3.1. 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. As a minimum, a compliance migration plan will address the following:

2.2.3.2.1. 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. 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. 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) Compliance Waiver Request:

2.2.4.1. 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. The process for requesting a waiver is as follows:

2.2.4.2.1. 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. 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) Request For Change (RFC) Process:

2.2.5.1. 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. 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:hqaetcsxci@randolph.af.mil>) or to 61 Main Circle, Suite 2, Randolph AFB TX 78150-4545.

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

2.4.2.1. 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. 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.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

NOTE: The following are added:

References

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

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

Abbreviations and Acronyms

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

Attachment 2 (Added)**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)**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)**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.*

PAUL F. CAPASSO, Colonel, USAF
Director of Communications and Information