BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-103

18 MARCH 1999

AIR FORCE SPACE COMMAND Supplement 1

1 SEPTEMBER 2004

Communications and Information

REQUIREMENTS DEVELOPMENT AND PROCESSING

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ AFCA/XPPD
(SMSgt Dennis L. Richards)
Supersedes AFI 33-103, 1 July 1996.

Certified by: AF/SCXX
(Lt Col G. L. Fiedler)
Pages: 33
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*; DoD 5000.2-R, *Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems*, March 15, 1996; DoD Instruction (DoDI) 5000.2, *Defense Acquisition Management Policies and Procedures*, February 23, 1991/Air Force Supplement 1 (AFSUP1); Office of Management and Budget (OMB) Circular No. A-130, *Management of Federal Information Resources*; DoD Directive 8000.1, *Defense Information Management (IM) Program*; and related aspects of the *Information Technology Management Reform Act of 1996*. It details a process to streamline the development of and response to communications and information systems requirements. It also provides an oversight procedure to maintain the integrity of the process. The communications and information systems requirements process enables users to obtain new, nondevelopmental information technology (IT) capabilities with total program cost of less than or equal to $15 million, and to sustain existing IT systems. Information technology is defined by OMB Circular A-130 as: the hardware and software used for Government information, regardless of technology involved, whether computers, communications, micrographics, or others. Those systems expected to cost more than $15 million, that involve development, or require an interface to support joint operations must follow procedures outlined in AFPD 10-6, *Mission Needs and Operational Requirements*, and AFI 10-601, *Mission Needs and Operational Requirements Guidance and Procedures*. Modifications to Air Force Materiel Command-supported Air Force systems must follow procedures in AFI 10-601. Refer recommended changes and conflicts between this and other publications to Headquarters, Air Force Communications Agency, Policy Branch, (HQ AFCA/XPXP), 203 W. Losey Street, Room 1020, Scott AFB IL 62225-5222, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to Headquarters United States Air Force, Policy Division (HQ USAF/SCXX), 1250 Air Force Pentagon, Washington DC 20330-1250. A glossary of references and supporting information is at **Attachment 1**.

(AFSPC) The OPR for this supplement is HQ AFSPC/LCXX (Connie Armstrong). This supplement supersedes AFI 33-103_AFSPCSUP 1, 1 Apr 98. This supplement implements and extends the guidance of Air Force Instruction (AFI) 33-103, ***Requirements Development and Processing***, 18 March 1999. The AFI is published word-for-word without editorial review. This supplement describes AFSPC's procedures for use in conjunction with the basic AFI. It applies to Headquarters AFSPC and subordinate units. This supplement does not apply to the Air Force Reserve Command nor Air National Guard units. Forward unit supplements to HQ AFSPC/LCXX, 150 Vandenberg Street, Suite 1105, Peterson AFB CO 80914-4340.

SUMMARY OF REVISIONS

This revision incorporates IC 99-1 and raises the cost threshold ceiling for the communications and information requirements that may be processed using AFI 33-103 procedures from $5 million to $15 million. This revision also makes several updates in terminology and publication titles. First, it replaces the term "acquisition cost" with the term "program cost" and revises the definition to match the wording cited in AFI 10-601, *Mission Needs and Operational Requirements Guidance and Procedures*, in **Attachment 1**. Definitions are also provided for full costs, information system, information technology, information system life cycle, modular contracting, national security systems, and year 2000 compliant. In addition, this revision strengthens the procedures used to program and obtain communications security (COMSEC) equipment, as outlined in paragraphs **2.5.1.**, **4.4.**, and **5.3.2.**. Pertinent references to command, control, communications, and computer (C4) systems are changed to communications and information systems. All references to Federal Information Resource Management Regulations (FIRMR) in paragraph 4 and Attachment 1 are deleted. The purpose statement, summary of revisions, paragraphs **4.**, **5.**, **7.**; and Attachment 1 are changed to allow for the incorporation of mandates under the *Information Technology Management Reform Act of 1996 (ITMRA)*. Finally, this revision changes all references to the Department of Defense (DoD) Technical Architecture Framework for Information Management (TAFIM) and Air Force Technical Reference Codes (TRC). to the DoD Joint Technical Architecture-Air Force in the purpose statement, paragraphs **2.**, **3.**, **4.**, and **5.**; and **Attachment 1**. The entire text of IC 99-1 is at **Attachment 5**. A bar (|) indicates revision from the previous edition.

(AFSPC) This document is substantially revised and must be completely reviewed.

(AFSPC) This revision replaces previous supplement in itsentirety. It prescribes policy, procedures, and responsibilities for identifying, documenting and processing requests for Command, Control, Communications and Computer (C4) systems and/or services. some required format changes have been made to allow for the conversion process into Project, Workflow, Requirement, and Resources (PWRR) Manager.

1. The Communications and Information Systems Requirements Process. 4
2. Responsibilities. 4
3. Identifying Communications and Information Systems Requirements. 5
4. The Technical Solution. 7
5. Developing the Technical Solution. 8
6. Allocating Resources. 9
7. Implementing the Requirement. 10

8. Forms Prescribed. 10

Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 11

Attachment 2— REQUEST FOR TECHNICAL SOLUTION 18

Attachment 3— LEASE VERSUS PURCHASE ANALYSIS 20

Attachment 4— INSTRUCTIONS FOR COMPLETING AF FORM 3215 22

Attachment 5— INTERIM CHANGE 99-1 TO AFI 33-103 23

1. The Communications and Information Systems Requirements Process. The communications and information systems requirements process enables requesting organizations (users) to obtain new communications and information capabilities, with the assistance of the CSO. You may also use this process to document communications and information systems sustainment requirements. The process starts when the user identifies a mission need and requests CSO assistance with defining the requirement and developing a technical solution for that need. The user may also request CSO assistance with implementing the technical solution. In some instances, the CSO must involve the Systems Telecommunications Engineering Manager (STEM), the lead command, frequency management, communications security (COMSEC) activities, and others to develop the technical solution.

1.1. (Added-AFSPC) AFSPC policy dictates that PWRR Manager is the command's official tool used to initiate, maintain, and track the lifecycle progress of requirements. It replaces the AF Form 3215, **IT/NSS Requirements Document**. The organization (user) requesting C4 equipment, services, or systems will identify their mission need by submitting a requirement on the web-based PWRR system. The requirement will automatically be routed to the appropriate office for validation. C4 capabilities cannot be purchased unless an approved requirement has been submitted and a valid technical solution has been developed.

2. Responsibilities.

2.1. The requesting organization identifies communications and information systems requirements and allocates resources to satisfy those requirements. The requester prepares an economic analysis under certain circumstances, according to AFI 65-501, *Economic Analysis*. The CSO assists the user with the economic analysis.

2.1. (AFSPC) Consult the local financial analysis office for help when assisting users to develop an economic analysis.

2.1.1. (Added-AFSPC) The requesting organization will be required to create an account in PWRR before a requirement can be submitted. Requirements can only be submitted by individual personal accounts, not organizational accounts.

2.1.2. (Added-AFSPC) The base PWRR Administrator will track and monitor all communication requirements through the system and ensure customers receive a response to their requests in a timely and effective manner. Requirements will be routed to the appropriate work center for a technical solution. Requirements outside the scope of the base's organic capabilities will be forwarded to the STEM B for technical review and blueprint updates before sending to the MAJCOM via PWRR.

2.2. The CSO helps users identify needs and develops, obtains, and implements technical solutions for user requirements. AFI 33-104, *Base-Level Planning and Implementation,* provides information about implementing solutions to user requirements.

2.2.1. (Added-AFSPC) The CSO coordinates all C4 system facility/infrastructure requirements with the civil engineer to ensure proper timing and support for C4 system installation.

2.2.2. (Added-AFSPC) DRUs follow the guidance of host base activities and this supplement when referring C4 requirements to the MAJCOM.

2.3. MAJCOMs and other involved organizations determine documentation requirements at each step of the process.

2.4. The Air Force Frequency Management Agency (AFFMA) provides frequency guidance and assistance to requesting organizations and CSOs.

2.5. Air Force Materiel Command (AFMC):

2.5.1. The Headquarters Electronic Systems Center, Cryptologic Systems Group, Security Products Division (HQ ESC/CPSG/ZSP) manages the COMSEC equipment requirements for the Air Force and evaluates all technical solutions that include information security (INFOSEC) products.

2.5.2. The 38th Engineering Installation Wing (38 EIW) helps the CSO develop technical solutions and maintains the Communications and Information Systems Blueprint. The Communications and Information Systems Blueprint documents the current communications and information systems infrastructure, identifies what's needed to satisfy present and future requirements, and provides a time-phased plan, with estimated costs, to satisfy requirements. In this sense, the Communications and Information Systems Blueprint provides a vehicle for the operational information technology planning outlined in (OMB) Circular No. A-130, *Management of Federal Information Resources.* The STEM is a part of the 38 EIW. The 38 EIW also provides program management for designated systems. See AFI 33-104 for more information about the Communications and Information Systems Blueprint.

2.5.3. The Standard Systems Group (SSG) provides software development and program management for designated systems.

2.6. HQ AFCA, Data Support Branch, Information Transfer Division, Systems and Procedures Directorate (HQ AFCA/SYND), provides technical solutions for video teleconference (VTC) requirements and provides engineering and technical support to the Air Education and Training Command (AETC) for video teletraining requirements. See AFI 33-117, Visual Information (VI) Management, for more information.

2.7. Lead Command. The lead command for a designated multi-MAJCOM C4 system is the systems advocate that responds to issues affecting system status and use. See AFI 10-901, *Lead Operating Command--Command, Control, Communications, Computers, and Intelligence (C4I) Systems Management*, for a detailed list of lead command responsibilities and the lead command assignment list.

3. Identifying Communications and Information Systems Requirements. The requesting organization identifies a mission need and determines if a nonmateriel solution will satisfy the need. Requirements arise from a deficiency in an existing operational capability, a need for a new capability, or an opportunity to replace or modernize an existing system with improved technology when operationally and economically practical. The user should determine if possible nonmateriel solutions could result from changes in doctrine, operational concepts, tactics, training, or organization. At the same time, the user must also examine affected business processes to determine if process improvement or redesign results in a nonmateriel solution. If users can't satisfy the need with a nonmateriel solution, they document their requirement and consult the CSO to help define the requirements and obtain a technical solution. Users, IT and mission planners, and support users must use strategy-to-task methodologies and the Air Force modernization planning processes to link IT investments to mission essential task improvements (see AFI 10-1401, *Modernization Planning Documentation*). The CSO integrates requirements into the base Communications and Information Systems Blueprint when the requester approves the technical solution. Prior to information technology investments, users must review opportunities to incorporate related best practices; process redesign; and competitive sourcing and privatization opportunities. Document these actions to ensure pro-

cess improvements and contracting resources are explored prior to IT investments. When processes are reengineered, process owners must ensure these processes are incorporated into the affected operational architectures.

3.1. The requesting organization provides the CSO with functional requirement information so the CSO can develop the technical solution. This includes:

3.1.1. Point of Contact. Provides sufficient information so the CSO can contact a knowledgeable individual who can provide more information about the need. The MAJCOM or wing commander defines who can submit requests.

3.1.2. Describe the Mission Deficiency or Need. In functional terms, clearly indicate the needed capability, rather than the specific equipment required (that is, provide only the technical data needed to satisfy the need). If you recommend specific equipment, state why you need that equipment. Identify systems the proposed capability must interface with, plus any standardization and interoperability requirements. In order to improve interoperability, systems fielded to satisfy the requirements for this capability will conform with applicable information technology standards and specifications. These are identified in the *DoD Joint Technical Architectur (JTA)*, the *Joint Technical Architecture-Air Force (JTA-AF)*, and the *DoD Data Dictionary System (DDDS)*. Identify security handling requirements or requirements for a secure capability. Include special requirements, when necessary, such as accommodations for individuals with disabilities, special operating conditions, manpower, training, maintenance, and mobility requirements.

3.1.3. Date Needed. Identify when the requesting organization needs the service. The requester should consider funds availability and the complexity of the requirement when identifying a service need date.

3.2. Users, communications and information planners, and STEM personnel must analyze applicable risks, benefits, and costs. Use AFP 91-215, *Operational Risk Management (ORM) Guidelines and Tools,* to help control risks. Also consider security of resources, protection of privacy, national security and emergency preparedness, energy efficiency, and year 2000 compliance. Communications and information systems life-cycle support must address initial and sustainment training, personnel acquisition and accession, logistical support, and performance measurements.

3.2.1. Requirements Authorizing Official. The MAJCOM or wing commander defines who will authorize implementation of the requirement and commitment of the resources.

3.2.2. Because of legal requirements, you must involve the base or MAJCOM Information Management function when preparing requirements that relate to information management systems, such as automated records, the reports control systems, the Privacy Act, or the Freedom of Information Act. The requester should contact the information management function before submitting the C4 systems requirement to the CSO.

3.2.3. Performance measurements. The requirement should help describe efficiency and effectiveness gaps between current and proposed IT capabilities. The requirement should also identify, in quantifiable terms, the expected improvements once the requirement is satisfied. These critical mission success factors may include changed capabilities, reduced costs, streamlined processes, enhanced performance, and other IT improvement impacts. Use Air Force Doctrine Document (AFDD) 1-1, *Air Force Task List*, the Air Force Information Technology Strategic Plan, and the Air Force Information Technology Management Plan to link IT investments to mission essential tasks and performance measures.

3.3. AF Form 3215, **C4 Systems Requirements Document**. You may use this form to submit and process requirements. **Attachment 4** contains instructions for completion of the AF Form 3215.

3.3. (AFSPC) AF Form 3215, **C4 Systems Requirements Document**: PWRR replaces the AF Form 3215. This web-based application will require the same type of information to be filled out, in addition to funding and infrastructure description. This processing includes full tracking, auditing, and reporting of both base- and command-level requirements. Integration with the existing email system provides instantaneous status updates and eliminates all paperwork while still providing a complete audit trail.

3.3.1. (Added-AFSPC) **Access PWRR Manager:** Anyone who has .mil, .gov, and certain .com addresses can create an account in PWRR; however, they will not be able to access or use it until it has been authenticated by the Base Administrator (located in the SCX office). Newly created PWRR accounts are automatically defaulted to the Base Administrator for authentication and cannot be changed by anyone but the AFSPC Program Manager. Email addresses are used to uniquely identify all users of the application.

3.3.2. (Added-AFSPC) **STEM Involvement:** Base Communications Plans Flights must work with their STEM B to ensure all short- and long-term requirements are documented in the base blueprints using C4ISR Infrastructure Planning System (CIPS)/Requirements Tracking Module (RTM).

4. The Technical Solution. The technical solution summarizes the full costs and recommended course of action to satisfy the user's need. Full costs encompass all program costs, but may include all information system life-cycle costs. The technical solution minimizes waste by improving the user's productivity, efficiency, and effectiveness of operations. It describes alternatives considered, if applicable, and includes any supporting information. It always considers compliance with applicable operational, technical, and systems architectures, as well as a review by applicable collateral activities. The technical solution provides more than the hardware and software required to satisfy the need. The CSO must provide the requester with sufficient information from which to make a decision to implement the decision and expend resources. This information may include recommendations about the acquisition and sustainment of the hardware and software. When necessary, the user compares commercial, lease**,** and purchase costs for the hardware, the need for contractual or government services to operate and maintain the system, and supplies and training for operations and maintenance. The requirement and the needs of the requester determine the methodologies the CSO uses and the level of detail. Involve contracting personnel when developing solutions that involve the procurement of equipment, software, or services to ensure the provisions of Federal Acquisition Regulations (FAR) and AFI 64-series are met. **Attachment 3** provides instructions for developing a lease versus purchase cost comparison.

4.1. The requester is required to complete an economic analysis in certain circumstances. This is a systematic examination of the costs, benefits, and risks of various alternatives. The economic analysis is required when a new project or program has a total investment cost over $1 million, or annual recurring costs over $200 thousand. If proposed changes to an on-going project push project investment costs over those levels, when no previous economic analysis was performed, an economic analysis is also required. See AFI 65-501, for more information. The requester involves the CSO when an economic analysis is required.

4.1. (AFSPC) Attach the required economic analysis to your PWRR requirements meeting these criteria. Total investment costs (life-cycle costs) include acquisition and ownership (support and O&M) resource needs over the system's useful life. See AFI 33-103, **Attachment 3**, paragraph **A3.2.2.**

4.2. There may be times when the requester alters the requirements document. If this occurs after the CSO has provided the technical solution, the requester has approved the solution, or the resources have been approved, further review is necessary. If the alteration results in an increase in the cost of the requirement by 20 percent, or it impacts architectural and interoperability standards, the requirement must be reapproved by the customer and funding activity.

4.3. All technical solution developers must ensure that communications and information systems configurations properly integrate with local, Air Force, and DoD architectures according to Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01, *Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems*; the DoD Joint Technical Architecture; the JTA-AF; and AFI 33-102, *Command, Control, Communications, Computers, and Intelligence (C4I) Systems Capabilities Planning Process*.

4.4. Technical solution developers must forward all technical solutions utilizing COMSEC/INFOSEC equipment to Headquarters Electronic Systems Center, Crytologic Systems Group, Security Products Division (HQ ESC/CPSG/ZSP), 230 Hall Blvd Ste 114, Kelly AFB, TX 78243-7056 for review, evaluation and validation.

5. Developing the Technical Solution. The CSO develops a technical solution when he or she receives a requirement, but may require outside assistance. This usually occurs when technical expertise is not locally available, to insure C4 systems integrate with base, MAJCOM and DoD architectures and standards, or when special outside activities must review the requirement due to their Air Force responsibilities.

5.1. The CSO will expedite the development of local solutions to routine requirements. Such routine requirements include telephone relocations or procurement of software that is commercially available and compatible with other locally used software. The CSO must keep review and oversight to the absolute minimum required to maintain standardization and interoperability of systems.

5.2. The CSO may contact the STEM for help in developing the technical solution. The STEM is an activity of the 38 EIW. The STEM serves the MAJCOMs, wing commanders, and CSOs as C4 engineering technical advisors. They define and clarify C4 systems requirements and assist in developing technical solutions. The STEM provides two levels of technical assistance. The first level provides a broad gauge estimate of costs associated with a solution, which is usually sufficient information for the user to decide to implement the solution. The STEM provides this estimate within 30 days. The second level contains detailed costs and requires more time and requester's funds to complete. Use **Attachment 2** as a guide to requesting any technical assistance. Contact the 38 EIW/EST, 4069 Hilltop Road, Suite 101, Tinker AFB OK 73145-6343, for more information regarding the request for technical assistance.

5.3. The CSO or the STEM must ensure other activities review certain requirements, as detailed below. The CSO and the STEM will obtain all necessary coordination when developing technical solutions. The CSO is ultimately responsible for ensuring the reviews are conducted.

5.3.1. Lead Command. AFI 10-901 defines the responsibilities of the lead command and identifies the C4 systems an activity is the lead command for.

5.3.1.1. When developing local technical solutions related to or interfacing with a system with a lead command, the CSO should contact the lead command to obtain guidance and concurrence with the proposed solution.

5.3.1.2. When developing more complex solutions, or when the lead command determines, the CSO or STEM must forward the requirements document to the lead command for coordination and concurrence with the proposed solution. The lead command concurs with the solution or provides an alternative and returns the requirements document to the CSO or STEM.

5.3.2. COMSEC. The CSO involves the unit or MAJCOM COMSEC manager and submits the requirements to HQ ESC/CPSG/ZSP. The STEM, when assisting with the proposed solution, will submit the requirement to HQ ESC/CPSG. The CPSG reviews the requirement, establishes the Mission Design Series (MDS) code, and returns it to the STEM or CSO, based on established procedures. Users and communications and information personnel will use the MDS to program and call out COMSEC/INFOSEC equipment via supply channels. Failure to identify requirements with sufficient lead-time may result in HQ ESC/CPSG's inability to provide the necessary INFOSEC equipment for that requirement.

5.3.3. Frequency Management and Host Nation Approval. If the technical solution recommends a communications and information system that involves the transmission or receipt of electromagnetic energy, the CSO must contact the unit or MAJCOM frequency manager for guidance. The CSO, with assistance from the frequency manager, will ensure recommended communications and information systems are compatible with existing equipment and will not negatively impact the frequency spectrum. See AFI 33-118, *Radio Frequency Spectrum Management*, for more information. In addition, Users must know where they will geographically deploy and use their systems. Users must incorporate communications and information support requirements into affected planning documents. Use of all systems that deploy outside of the CONUS are restricted by host countries and must receive permission to operate under host nation approval procedures employed by the CINC responsible for that area of responsibility. During peacetime and contingencies, host nations have, in the past, and will, forbid the use of systems that may interfere with their indigenous communications systems or for other reasons are not welcome. Work through the affected component MAJCOM CSO responsible for supporting the CINC (i.e., HQ United States Air Forces in Europe [HQ USAFE/SC] supports HQ European Command, HQ Pacific Air Forces [HQ PACAF/SC] supports HQ Pacific Command).

5.3.4. VTC and Video Teletraining (VTT) Requirements. The CSO reviews AFI 33-117 and the VTC Implementers Guide when processing VTC and VTT requirements. The CSO will identify any changes to the base C4 infrastructure as a result of the requirement. Keep the STEM-Base Level (STEM-B) apprised of the technical solution and impact to the C4 infrastructure.

5.3.5. The STEM coordinates applicable requirements with SSG, Maxwell AFB, Gunter Annex AL 36114-3004.

5.4. The CSO should refer to AFI 33-116, *Long-Haul Telecommunications Management*, for further assistance on acquiring, processing. and managing long-haul telecommunications.

6. Allocating Resources. The requesting organization follows established local, MAJCOM, and Air Force procedures to obtain resources to implement and sustain the technical solution. In some instances, the CSO will assist the requester to obtain the resources, especially when the CSO's communications

activity will provide manpower to operate or maintain Communications and Information systems. CSOs shall ensure user requirements are linked to the funds programming process. As a minimum, link requirements and costs by incorporating them into the Blueprint to facilitate MAJCOM and Lead Command Program Objective Memorandum submissions. See AFI 65-601, Vol 1, *Budget Guidance and Procedures*; AFI 38-201, *Determining Manpower Requirements*; and AFI 38-204, *Programming USAF Manpower*, for budget and manpower information.

6.1. (Added-AFSPC) Refer requirements to AFSPC CSS/CC for evaluation, MAJCOM Communications and Information Systems Officer (CSO) approval, or other required actions, when:

6.1.1. (Added-AFSPC) Integrated Tactical Warning/Attack Assessment (ITW/AA) service is needed within 6 months.

6.1.2. (Added-AFSPC) Initiatives cross NAF/Wing/Independent Group boundaries. The MAJCOM accomplishes cross-organization coordination and implementation authority for all upward generated requirements.

6.1.3. (Added-AFSPC) Implementation of the requirement will influence or change a configured AFSPC Lead Command C4 System (see AFI 10-901, ***Lead Operating Command—Communications and Information Systems Management***).

6.2. (Added-AFSPC) The MAJCOM CSO refers requirements with acquisition costs of more than $5M to HQ AFSPC/DRR for designation of a command-lead and development of a Mission Need Statement IAW AFI10-601, ***Mission Needs and Operational Requirements Guidance and Procedures.***

7. Implementing the Requirement. Implementation begins when the requester obtains funds and other resources. The requester may ask for CSO assistance to implement the requirement. The CSO will develop an implementation plan with the concurrence of the requester. When developing an acquisition strategy, CSOs and requesters should ensure their servicing contracting officers consider the rapidly changing nature of information technology through market research and the application of technology refreshment techniques. Reduce program risk by using modular contracting, as outlined in FAR 39. AFI 33-104 outlines base and MAJCOM implementation procedures.

8. Forms Prescribed. AF Form 3215, **C4 Systems Requirements Document**.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Information Technology Management Reform Act of 1996 (ITMRA)

(OMB) Circular No. A-130, *Management of Federal Information Resources*

FAR 39, *Acquisition of Information Technology*

CJCSI 6212.01, *Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems*

DoDD 8000.1, *Defense Information Management (IM) Program*

DoDI 5000.2, *Defense Acquisition Management Policies and Procedures,* February 23, 1991/Air Force Supplement 1

DoD 5000.2-R, *Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems,* March 15, 1996

DoD Data Dictionary System (DDDS)

JTA-AF, *Joint Technical Architecture-Air Force*

AFDD 1-1, *Air Force Task List*

AFDIR 33-121, *Compendium of Communications and Information Terminology* (will convert to AFDIR 33-303)

AFPD 10-6, *Mission Needs and Operational Requirements*

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

AFPD 33-2, *Information Protection*

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

AFI 10-901, *Lead Operating Command--Communications and Information Systems Management*

AFI 21-116, *Maintenance Management of Communications-Electronics*

AFI 23-501, *Retaining and Transferring Materiel*

AFI 33-102, *Command, Control, Communications, Computers, and Intelligence (C4I) Capabilities Planning Process*

AFI 33-104, *Base-Level Planning and Implementation*

AFI 33-116, *Long-Haul Telecommunications Management*

AFI 33-117, *Visual Information (VI) Management*

AFI 33-118, *Radio Frequency Spectrum Management*

AFI 37-131, *Freedom of Information Act Program*

AFI 37-132, *Air Force Privacy Act Program*

AFI 38-201, *Determining Manpower Requirements*

AFI 38-204, *Programming USAF Manpower*

AFI 65-501, *Economic Analysis*

AFMAN 65-506, *Economic Analysis*

AFI 65-601, Vol 1, *Budget Guidance and Procedures*

AFI 90-301, *Inspector General Complaints*

AFP 91-215, *Operational Risk Management (ORM) Guidelines And Tools*

AFMAN 23-110, *USAF Supply Manual*

Air Force Information Technology Management (ITM) Strategic Plan (ITMSP) October 1997

Abbreviations and Acronyms

AETC—Air Education and Training Command

AFI—Air Force Instruction

AFDD—Air Force Doctrine Document

AFFMA—Air Force Frequency Management Agency

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFPD—Air Force Policy Directive

C4I—Command, Control, Communications, Computers, and Intelligence

CIO—Chief Information Officer

COMSEC—Communications Security

CSO—Communications and Information Systems Officer

DDDS—DoD Data Dictionary System

DoD—Department of Defense

DoDI—Department of Defense Instruction

FAR—Federal Acquisition Regulations

FOA—Field Operating Agency

GSA—General Services Administration

HQ AFCA—Headquarters, Air Force Communications Agency

HQ 38 EIW—Headquarters, 38th Engineering Installation Wing

IT—Information Technology

ITMRA—Information Technology Management Reform Act

JTA-AF—Joint Technical Architecture-Air Force

LOC—Lines of Code

MAJCOM—Major Command

SSG—Standard Systems Group

STEM—Systems Telecommunications Engineering Manager

VTC—Video Teleconference

VTT—Video Teletraining

Y2K—Year 2000

Terms

Base-Level Communications and Information Infrastructure—Both host and tenant organizations use the base-level communications and information systems infrastructure. The infrastructure includes all aspects of Communications and Information systems (voice, data, video transmission, switching, processing, system control and network management systems, equipment and facilities).

Business Process Reengineering—A structured approach by all or part of an enterprise to improve the value of its products and services while reducing resource requirements.

Communications and Information System—An integrated combination of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control through all operational phases. It includes base visual information support systems.

Communications and Information Systems Blueprint—Document that provides the engineering plan to modernize the base-level infrastructure with cost-effective, base-wide communications and information capability to support digital transmission of voice, data, video, imagery, and telemetry needs. It documents the baseline, identifies a target base configuration to support present and future requirements, and provides a time-phased plan and estimated costs for logical transition. The Communications and Information Systems Blueprint is sometimes referred to as the "Base Blueprint" or the "Blueprint."

Communications and Information Systems Officer (CSO)—Identifies the supporting communications and information systems officer at all levels. At base-level, this is the commander of the communications unit responsible for carrying out base communications and information systems responsibilities. At MAJCOM, and other activities responsible for large quantities of communications and information systems, it is the person designated by the commander as responsible for overall management of communications and information systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol "SC" and expands it to three and four letters to identify specific functional areas. CSOs are the accountable officer for all automated data processing equipment in their inventory.

Communications and Information Systems Requirement—Identifies a communications and information systems mission shortfall or system need to the CSO. A communications and information systems requirement arises when an organization cannot accomplish its current or new mission; can increase operational efficiency or cut operational costs by using advances in technologies; or can modernize an existing communications and information system by applying modern technology to satisfy evolving communications and information systems requirements, improve mission performance, and reduce current or future operation and support costs.

Full Costs—When applied to the expenses incurred in the operation of communications and information equipment/systems, includes: all direct, indirect, general, and administrative costs incurred in the operation of the communications and information system/equipment. These costs include, but are not limited to, personnel, equipment, hardware, software, supplies, contracted services, space occupancy, and intra/inter-agency services. (OMB Circular No. A-130)

Information Resource Management—The planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information. (OMB Circular No. A-130)

Information system—A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. (OMB Circular No. A-130)

Information system life cycle—The phases, through which an information system passes, typically characterized as initiation, development, operation, and termination. (OMB Circular No. A-130)

Information Technology—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. Includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (OMB Circular No. A-130)

Information Technology Management Reform Act—A Legislative act that repealed the Brooks Act, and gave the General Services Administration exclusive authority to acquire computer resources for all of the Federal government. It assigns overall responsibility for the acquisition and management of information technology (IT), to the Director, Office of Management and Budget (OMB). Responsibilities include: Design and implement an IT management process maximizing the value and assessing and managing the risks of the IT acquisitions. Integrate the IT management process with the budget, financial and program management processes. Establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services through the effective use of IT. Prepare an annual report, to be included in the DoD budget submission to Congress, on the progress in achieving the goals. Ensure agencies establish performance measurements for IT to measure how well the IT supports agency programs. Ensure the information security policies, procedures, and practices are adequate. Appoint a Chief Information Officer (CIO). Inventory all computer equipment and maintain an inventory of any such equipment that is excess or surplus property.

Interoperability—The ability of the systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (JP 1-02).

Joint Technical Architecture—Identifies the standards and guidelines for new acquisitions or major modifications to existing DoD communications and information systems. The standards, profiles, recommended products and recommended solutions are mandatory for use in the Air Force. The domains are provided as guidance. A system is compliant with the JTA-AF if it meets, or is implementing an approved plan to meet, all applicable JTA-AF mandates.

Joint Technical Architecture-Air Force—A comprehensive set of interfaces, services, and supporting

formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles.

Lead Command—The MAJCOM or FOA assigned as the systems advocate and oversight authority.

Major Command (MAJCOM)—A major subdivision of the Air Force that is assigned a major part of the Air Force mission. MAJCOMs report directly to HQ USAF.

Modification—A temporary or permanent change to a system that is still being produced. The purpose of the modification is to correct deficiencies, improve reliability and maintainability, or to improve capabilities.

Modular contracting—Use of one or more contracts to acquire information technology systems in successive, interoperable increments. (OMB Circular No. A-130)

Nondevelopmental—Any project to procure primarily in-being products, where the total software developmental effort is realistically estimated as less than 1040 man-hours. As an alternative, use a threshold of less than 700 lines of code (LOC). If any hardware development is planned, the effort is not nondevelopmental.

Nonmaterial Solution—Includes changes in doctrine, operational concepts, tactics, training, or organization.

Operational Architecture—A description (often graphical) of the operational elements, assigned tasks, and information flows required to support the warfighter. It defines the type of information, frequency, and timeliness of the exchange, and what tasks are supported by these information exchanges. (AFDIR 33-121)

Operational Information Technology Planning—A process that links information technology to anticipated program and mission needs, reflects budget constraints, and forms the basis for budget requests. This planning should result in the preparation and maintenance of an up-to-date five-year plan which includes: a listing of existing and planned major information systems; a listing of planned information technology acquisitions; an explanation of how the listed major information systems and planned information technology acquisitions relate to each other and support the achievement of the agency's mission; and a summary of computer security planning.

Performance Measurement—The assessment of effectiveness and efficiency of IT in support of the achievement of an organization's missions, goals, and quantitative objectives through the application of outcome-based, measurable, and quantifiable criteria, compared against an established baseline, to activities, operations, and processes. (*DoD Guide for Managing IT as an Investment and Measuring Performance*, 10 February 1997)

Program Cost—The total of all expenditures, in any appropriation or fund, directly related to the automated information system definition, design, development, and deployment, and incurred from the beginning of the "Concept Exploration" phase through deployment at each separate site. For incremental and evolutionary program strategies, program cost includes all increments. Program cost does not include operations and support costs incurred at an individual site after operational cut over of any increment at that site, even though other sites may exist that have not yet completed deployment. (AFI 10-601)

Risks—Types of risk may include schedule risk, risk of technical obsolescence, cost risk, risk implicit in a particular contract type, technical feasibility, dependencies between a new project and other projects or systems, the number of simultaneous high risk projects to be monitored, funding availability, and program

management risk. (OMB Circular No. A-130)

Risk Management—1. Appropriate techniques should be applied to manage and mitigate risk during the acquisition of information technology. Techniques include, but are not limited to: prudent project management; use of modular contracting; thorough acquisition planning tied to budget planning by the program, finance and contracting offices; continuous collection and evaluation of risk-based assessment data; prototyping prior to implementation; post implementation reviews to determine actual project cost, benefits and returns; and focusing on risks and returns using quantifiable measures. (FAR 39) 2. Risk management is the process used by decision-makers to reduce or offset risk. The risk management process provides leaders and individuals a systematic mechanism to identify and choose the optimum course of action for any given situation. Risk management must become a fully integrated element of planning and executing an operation. (AFP 91-215)

Requirements Process—This three-step process identifies communications and information systems requirements, develops a technical solution, and allocates resources.

Software Development—That portion of an effort that creates new product. Developmental costs do not include the cost of in-being products that are being augmented or modified. An effort is not considered to "involve development" if the total software development involves less than 1040 man-hours of effort. (See "nondevelopmental")

Strategic Information Resources Management (IRM) Planning Processes—Processes which consist of the following components: how the management of information resources promotes the fulfillment of an agency's mission; the use of information throughout its life cycle; operational information technology planning, and links to other planning processes including strategic, human resources, and financial resources. (OMB Circular No. A-130)

Systems Architecture—A description, including graphics, of the systems and interconnections providing for or supporting a warfighting function. It defines the physical connection, location, and identification of the key nodes, circuits, networks, warfighting platforms, and so forth, associated with information exchange and specific system performance parameters. The system architecture is constructed to satisfy operational architecture requirements per the standards defined in the technical architecture. (AFDIR 33-121)

System Security—1. A condition resulting from the timely application of system security management and engineering principles throughout all phases of a system's life cycle. It can be measured in terms of relative probability; i.e., that under a known set of circumstances (vulnerability versus countermeasures), the probability that acts of illicit interference against a system could achieve a specific objective without an effective preemptive response by the operating command. (AFM 11-1, *Air Force Glossary of Standardized Terms*, will convert to Air Force Doctrine Document [AFDD] 1-2) 2. Involves applying and managing computer security, communications security, and emanations security to protect communications and information resources from denial-of-service attacks. Security ensures the integrity of communications and information resources and prevents exploitation of sensitive information.

Systems Telecommunications Engineering Manager—A communications and information systems engineer who provides technical engineering planning services in support of communications and information systems and base infrastructures. The Base-Level STEM (STEM-B) has technical responsibility for engineering management and assists the base CSO in system engineering and configuration control. The Command-Level STEM (STEM-C) provides technical assistance to the MAJCOM and coordinates with STEM-Bs on future MAJCOM mission changes, programs and efforts at

the MAJCOM-level. The Joint STEM (STEM-J) is assigned to Commander's in Chief, Joint Staff and the Defense Information Systems Agency to promote interoperability by providing an interface between those activities and the Air Force MAJCOMs and bases. The Telecommunications Manager (STEM-TM) assists the STEM-B and C.

Technical Architecture—A framework of concepts and guidance that bound a subject area, or of physical components (for example, hardware, software, and transmission media) which interrelate to perform a bounded subset of information handling, both processing and transfer. (AFDIR 33-121)

Technical Solution—This detailed description of the communications and information systems solution uses the base infrastructure and complies with downward-directed architectures and standards. It identifies recommended acquisition methods and strategies, estimates one-time and recurring costs, and identifies manpower impacts.

Video Teleconferencing (VTC)—A two-way electronic form of communications that permits two or more people in different locations to engage in face-to-face audio and visual communications for the purpose of conducting meetings, seminars, and conferences. A VTC system typically includes a telecommunications system; video compression equipment; and video, audio, and graphics components. DoD VTC equipment must conform to standards in the Corporation for Open Systems International VTC profile that incorporates international standards for VTC.

Video Teletraining (VTT)—An electronic form of communications that uses high quality video, audio, and graphics equipment for the purpose of conducting training and education programs for students that are geographically separated from the instructor. The Air Technology Network is the Air Force standard VTT network.

Waste—The extravagant, careless, or needless expenditure of Air Force funds or the consumption of Air Force property that results from deficient practices, systems controls, or decisions. The term also includes improper practices not involving prosecutable fraud. NOTE: Consider wartime and emergency operations when explaining possible waste. For example, legitimate stockpiles and reserves for wartime needs, which may appear redundant and costly, are not waste. (AFI 90-301)

Year 2000 compliant—The information technology accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it. (FAR 39)

Attachment 2

REQUEST FOR TECHNICAL SOLUTION

A2.1. Date of Request. The date the C4 systems officer submits the request.

A2.2. Control Number. The C4 systems officer assigns the control number based on the information below to track the request. The C4 systems officer must maintain the integrity of this number through the implementation phase:

Example:	**AETC**	**RANDOLPH**	**E**	**94**	**0001**
	1	2	3	4	5

1 - Requiring Command. The name of the MAJCOM that has the requirement and may implement the technical solution. For modifications to an Air Force-wide system, use "AF" instead of the MAJCOM designator.

2 - Originating Base. The name of the originating base. Use only the MAJCOM designator if more than one base.

3 - Alpha Functional Area Designator Code (*Optional*). Designators are listed in the *Air Force Data Dictionary*.

4 - Fiscal Year. The fiscal year in which an organization initiates a request.

5 - Sequence Number. A four-digit sequence number and optional alpha code designate amendments. The sequence number begins at "0001" at the beginning of each fiscal year.

A2.4. Project Title. A brief descriptive title identifying the requirement.

A2.5. Description of Mission Deficiency or Need. A description, expressed in functional terms, of what is needed. Provide sufficient information to clearly indicate what type of support you need rather than what kind of equipment you want. If the project is in support of a downward-directed program, include a statement to that effect.

A2.6. Point of Contact. The name, rank, title, office symbol, and telephone number of the individual who can provide additional information during technical solution development.

A2.7. Service Need Date. The date when the requesting organization needs to implement the solution, depending on the specific need and availability of funds.

A2.8. Date Technical Solution Needed. The CSO or requesting organization indicates the date the STEM needs to complete and deliver the technical solution.

A2.9. Processes Classified Data. Indicates whether the system processes classified information. See AFPD 33-2, *C4 Systems Security (*will change *to Information Protection)*, for more information. If the system processes classified information, identify the levels of security classification.

A2.10. Processes Sensitive Unclassified Data. Indicates whether the system processes sensitive unclassified information. Such information may be subject to the Privacy Act and Freedom of Information Act. (See AFIs 37-131, *Freedom of Information Act Program*, and 37-132, *Air Force Privacy Act Program*, for more information). If the system processes sensitive unclassified information, identify the types of information.

A2.11. Additional technical information. Include additional information needed to complete the technical solution, such as a building diagram or a listing of interfacing computers.

Attachment 3

LEASE VERSUS PURCHASE ANALYSIS

A3.1. The lease versus purchase analysis shows whether the lease or purchase of C4 equipment gives the most savings to the Air Force. The procedures below identify what information to collect and how to compute the costs associated with the lease and purchase of equipment.

A3.2. Data Required and Terms Explained. Collect the following information and use the computations in paragraph **A3.3.**

A3.2.1. Monthly Discount Factor. Get this by contacting the base or MAJCOM financial and cost analysis office. If they do not have the information, call the Director of Economics and Business Management, Economics Division, Office of the Assistant Secretary (Financial Management and Comptroller) (SAF/FMCEE), DSN 223-9346. Ask for the cumulative monthly discount factor for a lease versus purchase analysis for C4 equipment. ***Note: Know the period of the lease and purchase.***

A3.2.2. Estimated System Life. An estimate, in years, of useful life of the system. Use it when developing the lease versus purchase analysis. If an established life cycle is not provided by the manufacturer nor AFMC, use 5 years.

A3.2.3. Contract Purchase Price. The cost to purchase the equipment. Get prices from existing local, MAJCOM, or General Services Administration (GSA) contracts, or from inventories of like items. Involve your contracting office if you need to contact commercial vendors for price quotes.

A3.2.4. Purchase Option Credits. Include rental or special credits, payment discounts, etc., received when purchasing the equipment. These credits may become evident when researching the contract purchase price.

A3.2.5. Monthly Maintenance Purchase Cost. The cost to receive maintenance, on a monthly basis, when you purchase the equipment. Get these prices from existing local, MAJCOM, or GSA contracts. Involve your contracting office if you need to contact commercial vendors for price quotes.

A3.2.6. Monthly Rental Cost. The cost per month to rent the equipment. Get these prices from existing local, MAJCOM, or GSA contracts. Involve your contracting office if you need to contact commercial vendors for price quotes.

A3.2.7. Monthly Maintenance Lease Cost. The cost to receive maintenance, on a monthly basis, when leasing equipment. Get these prices from existing local, MAJCOM, or GSA contracts. Involve your contracting office if you need to contact commercial vendors for price quotes.

A3.3. Methodology. Make the following computations in the sequence listed below:

A3.3.1. Contract purchase price minus the purchase option credits equals the purchase price.

A3.3.2. Monthly maintenance purchase cost times the monthly discount factor equals the life maintenance cost.

A3.3.3. Purchase price plus the life maintenance cost equals the purchase cost.

A3.3.4. Monthly rental cost plus the monthly leased maintenance cost equals the monthly leased cost.

A3.3.5. Monthly leased cost times the cumulative monthly discount factor equals the lease cost.

A3.4. Example: You must decide to purchase or lease a facsimile machine. The contract purchase price is $4,000, but the vendor will give you a $500 discount for immediate purchase. The monthly maintenance cost is $100. You can lease the facsimile for $100 a month, and must also pay a $100 monthly for maintenance. The economic life of the machine is 5 years. Using the methodology to solve the problem is easy using the relevant facts from the example.

PURCHASE:

Contract purchase price ($4,000) minus purchase option credit ($500) equals purchase price ($3,500)

Monthly maintenance purchase cost ($100) times monthly discount factor (29.503*) equals life maintenance cost ($2,950)

Purchase price ($3500) plus life maintenance cost ($2950) equals the purchase cost ($6,450)

LEASE:

Monthly rental cost ($100) plus monthly leased maintenance cost ($100) equals monthly leased cost ($200)

Monthly leased cost ($200) times monthly discount factor (29.503*) equals lease cost ($5,901)

*The monthly discount factor may change. Do not use the factor in this example for your computations; consult your financial and cost analysis office or SAF/FMCEE.

NOTE: Compare the purchase cost option to the lease cost option. Select the lowest cost option in determining cost effectiveness. In the example above, the lease cost option is preferred.

A3.5. Format.

Equipment:

Vendor:

Location:

Date of Analysis:

Installation Date:

Projected Purchase Date:

Projected Termination Date:

Remaining System Life:

Computation Specifics:

Decision:

Attachment 4

INSTRUCTIONS FOR COMPLETING AF FORM 3215

1. Date: Enter the date the form is prepared or submitted.

2. CSO Control Number: Completed by the CSO.

3. Requirement Title: Include a title that briefly describes the requirement.

4. Date Needed: Enter the date the service is required.

5. Mission or System Supported: Identify the major C4 system or mission that the requirement relates to.

6. Requesting Agency Point of Contact: Identify who can knowledgeably discuss the requirement.

7. Requirement: State the need in functional terms. Tell what capabilities you need, don't just state what specific equipment you need. Recommend equipment if necessary. If specific equipment is recommended, state why. The focus of the requirement should be on describing the capabilities you need. Identify any security handling requirements, and indicate when a secure capability is required. When necessary, include special requirements, such as accommodations for handicapped users, special operating conditions, manpower, training, and maintenance.

8. Justification: Tell why you need it. The justification may be useful after the technical solution is provided. It can help prioritize resource allocation and project implementation.

9. CSO's Proposed Solution/Alternatives: Completed by the CSO, possibly with assistance from others, may require additional pages.

10. Technical Solution Authority: Identify who certifies the solution, meets architectural and interoperability standards, and what references were used. The CSO ensures completion, though other activities may certify.

11. Records Management Approval Authority: Involve the information management function when preparing requests that use information management systems, such as the records management and reports control systems and the Privacy and Freedom of Information Acts.

12. Requester Approval Authority: Completed after the technical solution is provided. Requester indicates what to do with the technical solution. Can approve or disapprove. User also identifies if funds are available for implementation. **NOTE:** Local or MAJCOM procedures may dictate specified dollar amount or types of requirements that require approval levels beyond that of user.

13. Host Base Approval Authority: This section is available if it is necessary to forward to another level for review or action according to local and MAJCOM guidelines.

14. MAJCOM Approval Authority: This section is available if it is necessary to forward the form to the MAJCOM for review or action according to MAJCOM guidance.

Attachment 5

INTERIM CHANGE 99-1 TO AFI 33-103

18 MARCH 1999

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*; DoD 5000.2-R, *Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems*, March 15, 1996; DoD Instruction (DoDI) 5000.2, *Defense Acquisition Management Policies and Procedures*, February 23, 1991/Air Force Supplement 1 (AFSUP1); Office of Management and Budget (OMB) Circular No. A-130, *Management of Federal Information Resources*; DoD Directive 8000.1, *Defense Information Management (IM) Program*; and related aspects of the *Information Technology Management Reform Act of 1996*. It details a process to streamline the development of and response to communications and information systems requirements. It also provides an oversight procedure to maintain the integrity of the process. The communications and information systems requirements process enables users to obtain new, nondevelopmental information technology (IT) capabilities with total program cost of less than or equal to $15 million, and to sustain existing IT systems. Information technology is defined by OMB Circular A-130 as: the hardware and software used for Government information, regardless of technology involved, whether computers, communications, micrographics, or others. Those systems expected to cost more than $15 million, that involve development, or require an interface to support joint operations must follow procedures outlined in AFPD 10-6, *Mission Needs and Operational Requirements*, and AFI 10-601, *Mission Needs and Operational Requirements Guidance and Procedures*. Modifications to Air Force Materiel Command-supported Air Force systems must follow procedures in AFI 10-601. Refer recommended changes and conflicts between this and other publications to Headquarters, Air Force Communications Agency, Policy Branch, (HQ AFCA/XPXP), 203 W. Losey Street, Room 1020, Scott AFB IL 62225-5222, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to Headquarters United States Air Force, Policy Division (HQ USAF/SCXX), 1250 Air Force Pentagon, Washington DC 20330-1250. A glossary of references and supporting information is at Attachment 1.

SUMMARY OF REVISIONS

This IC change raises the cost threshold ceiling for the communications and information requirements that may be processed using AFI 33-103 procedures from $5 million to $15 million. This IC also makes several updates in terminology and publication titles. First, it replaces the term “acquisition cost” with the term “program cost” and revises the definition to match the wording cited in AFI 10-601, *Mission Needs and Operational Requirements Guidance and Procedures*, in Attachment 1. Definitions are also provided for full costs, information system, information technology, information system life cycle, modular contracting, national security systems, and year 2000 compliant. In addition, this change strengthens the procedures used to program and obtain communications security (COMSEC) equipment, as outlined in paragraphs 2.5.1, 4.4, and 5.3.2. Pertinent references to command, control, communications, and computer (C4) systems are changed to communications and information systems. All references to Federal Information Resource Management Regulations (FIRMR) in paragraph 4 and Attachment 1 are deleted. The purpose statement, summary of revisions, paragraphs 4, 6, 7; and Attachment 1 are changed to allow for the incorporation of mandates under the *Information Technology Management Reform Act of 1996 (ITMRA)*. Finally, this IC changes all references to the Department of Defense (DoD) Technical Architecture Framework for Information Management (TAFIM) and Air Force Technical Reference Codes (TRC).

to the DoD Joint Technical Architecture-Air Force in the purpose statement, paragraphs 2, 3, 4, and 5; and Attachment 1.

1. The Communications and Information Systems Requirements Process. The communications and information systems requirements process enables requesting organizations (users) to obtain new communications and information capabilities, with the assistance of the CSO. You may also use this process to document communications and information systems sustainment requirements. The process starts when the user identifies a mission need and requests CSO assistance with defining the requirement and developing a technical solution for that need. The user may also request CSO assistance with implementing the technical solution. In some instances, the CSO must involve the Systems Telecommunications Engineering Manager (STEM), the lead command, frequency management, communications security (COMSEC) activities, and others to develop the technical solution

2.1. The requesting organization identifies communications and information systems requirements and allocates resources to satisfy those requirements. The requester prepares an economic analysis under certain circumstances, according to AFI 65-501, Economic Analysis. The CSO assists the user with the economic analysis.

2.5.1. The Headquarters Electronic Systems Center, Cryptologic Systems Group, Security Products Division (HQ ESC/CPSG/ZSP) manages the COMSEC equipment requirements for the Air Force and evaluates all technical solutions that include information security (INFOSEC) products.

2.5.2. The 38th Engineering Installation Wing (38 EIW) helps the CSO develop technical solutions and maintains the Communications and Information Systems Blueprint. The Communications and Information Systems Blueprint documents the current communications and information systems infrastructure, identifies what's needed to satisfy present and future requirements, and provides a time-phased plan, with estimated costs, to satisfy requirements. In this sense, the Communications and Information Systems Blueprint provides a vehicle for the operational information technology planning outlined in (OMB) Circular No. A-130, Management of Federal Information Resources. The STEM is a part of the 38 EIW. The 38 EIW also provides program management for designated systems. See AFI 33-104 for more information about the Communications and Information Systems Blueprint.

3. Identifying Communications and Information Systems Requirements. The requesting organization identifies a mission need and determines if a nonmateriel solution will satisfy the need. Requirements arise from a deficiency in an existing operational capability, a need for a new capability, or an opportunity to replace or modernize an existing system with improved technology when operationally and economically practical. The user should determine if possible nonmateriel solutions could result from changes in doctrine, operational concepts, tactics, training, or organization. At the same time, the user must also examine affected business processes to determine if process improvement or redesign results in a nonmateriel solution. If users can't satisfy the need with a nonmateriel solution, they document their requirement and consult the CSO to help define the requirements and obtain a technical solution. Users, IT and mission planners, and support users must use strategy-to-task methodologies and the Air Force modernization planning processes to link IT investments to mission essential task improvements (see AFI 10-1401, Modernization Planning Documentation). The CSO integrates requirements into the base Communications and Information Systems Blueprint when the requester approves the technical solution. Prior to information technology investments, users must review opportunities to incorporate related best practices; process redesign; and competitive sourcing and privatization opportunities. Document these actions to ensure process improvements and contracting resources are explored prior to IT investments. When processes are

reengineered, process owners must ensure these processes are incorporated into the affected operational architectures.

3.1.2. Describe the Mission Deficiency or Need. In functional terms, clearly indicate the needed capability, rather than the specific equipment required (that is, provide only the technical data needed to satisfy the need). If you recommend specific equipment, state why you need that equipment. Identify systems the proposed capability must interface with, plus any standardization and interoperability requirements. In order to improve interoperability, systems fielded to satisfy the requirements for this capability will conform with applicable information technology standards and specifications. These are identified in the DoD Joint Technical Architectur (JTA), the Joint Technical Architecture-Air Force (JTA-AF), and the DoD Data Dictionary System (DDDS). Identify security handling requirements or requirements for a secure capability. Include special requirements, when necessary, such as accommodations for individuals with disabilities, special operating conditions, manpower, training, maintenance, and mobility requirements.

3.2. Users, communications and information planners, and STEM personnel must analyze applicable risks, benefits, and costs. Use AFP 91-215, Operational Risk Management (ORM) Guidelines and Tools, to help control risks. Also consider security of resources, protection of privacy, national security and emergency preparedness, energy efficiency, and year 2000 compliance. Communications and information systems life-cycle support must address initial and sustainment training, personnel acquisition and accession, logistical support, and performance measurements.

3.2.3. Performance measurements. The requirement should help describe efficiency and effectiveness gaps between current and proposed IT capabilities. The requirement should also identify, in quantifiable terms, the expected improvements once the requirement is satisfied. These critical mission success factors may include changed capabilities, reduced costs, streamlined processes, enhanced performance, and other IT improvement impacts. Use Air Force Doctrine Document (AFDD) 1-1, Air Force Task List, the Air Force Information Technology Strategic Plan, and the Air Force Information Technology Management Plan to link IT investments to mission essential tasks and performance measures.

4. The Technical Solution. The technical solution summarizes the full costs and recommended course of action to satisfy the user's need. Full costs encompass all program costs, but may include all information system life-cycle costs. The technical solution minimizes waste by improving the user's productivity, efficiency, and effectiveness of operations. It describes alternatives considered, if applicable, and includes any supporting information. It always considers compliance with applicable operational, technical, and systems architectures, as well as a review by applicable collateral activities. The technical solution provides more than the hardware and software required to satisfy the need. The CSO must provide the requester with sufficient information from which to make a decision to implement the decision and expend resources. This information may include recommendations about the acquisition and sustainment of the hardware and software. When necessary, the user compares commercial, lease, and purchase costs for the hardware, the need for contractual or government services to operate and maintain the system, and supplies and training for operations and maintenance. The requirement and the needs of the requester determine the methodologies the CSO uses and the level of detail. Involve contracting personnel when developing solutions that involve the procurement of equipment, software, or services to ensure the provisions of Federal Acquisition Regulations (FAR) and AFI 64-series are met. Attachment 3 provides instructions for developing a lease versus purchase cost comparison.

4.3. All technical solution developers must ensure that communications and information systems configurations properly integrate with local, Air Force, and DoD architectures according to Chairman of the

Joint Chiefs of Staff Instruction (CJCSI) 6212.01, Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems; the DoD Joint Technical Architecture; the JTA-AF; and AFI 33-102, Command, Control, Communications, Computers, and Intelligence (C4I) Systems Capabilities Planning Process.

4.4. Technical solution developers must forward all technical solutions utilizing COMSEC/INFOSEC equipment to Headquarters Electronic Systems Center, Crytologic Systems Group, Security Products Division (HQ ESC/CPSG/ZSP), 230 Hall Blvd Ste 114, Kelly AFB, TX 78243-7056 for review, evaluation and validation.

5.3.2. COMSEC. The CSO involves the unit or MAJCOM COMSEC manager and submits the requirements to HQ ESC/CPSG/ZSP. The STEM, when assisting with the proposed solution, will submit the requirement to HQ ESC/CPSG. The CPSG reviews the requirement, establishes the Mission Design Series (MDS) code, and returns it to the STEM or CSO, based on established procedures. Users and communications and information personnel will use the MDS to program and call out COMSEC/INFOSEC equipment via supply channels. Failure to identify requirements with sufficient lead-time may result in HQ ESC/CPSG's inability to provide the necessary INFOSEC equipment for that requirement.

5.3.3. Frequency Management and Host Nation Approval. If the technical solution recommends a communications and information system that involves the transmission or receipt of electromagnetic energy, the CSO must contact the unit or MAJCOM frequency manager for guidance. The CSO, with assistance from the frequency manager, will ensure recommended communications and information systems are compatible with existing equipment and will not negatively impact the frequency spectrum. See AFI 33-118, Radio Frequency Spectrum Management, for more information. In addition, Users must know where they will geographically deploy and use their systems. Users must incorporate communications and information support requirements into affected planning documents. Use of all systems that deploy outside of the CONUS are restricted by host countries and must receive permission to operate under host nation approval procedures employed by the CINC responsible for that area of responsibility. During peacetime and contingencies, host nations have, in the past, and will, forbid the use of systems that may interfere with their indigenous communications systems or for other reasons are not welcome. Work through the affected component MAJCOM CSO responsible for supporting the CINC (i.e., HQ United States Air Forces in Europe [HQ USAFE/SC] supports HQ European Command, HQ Pacific Air Forces [HQ PACAF/SC] supports HQ Pacific Command).

6. Allocating Resources. The requesting organization follows established local, MAJCOM, and Air Force procedures to obtain resources to implement and sustain the technical solution. In some instances, the CSO will assist the requester to obtain the resources, especially when the CSO's communications activity will provide manpower to operate or maintain Communications and Information systems. CSOs shall ensure user requirements are linked to the funds programming process. As a minimum, link requirements and costs by incorporating them into the Blueprint to facilitate MAJCOM and Lead Command Program Objective Memorandum submissions. See AFI 65-601, Vol 1, Budget Guidance and Procedures; AFI 38-201, Determining Manpower Requirements; and AFI 38-204, Programming USAF Manpower, for budget and manpower information.

7. Implementing the Requirement. Implementation begins when the requester obtains funds and other resources. The requester may ask for CSO assistance to implement the requirement. The CSO will develop an implementation plan with the concurrence of the requester. When developing an acquisition strategy, CSOs and requesters should ensure their servicing contracting officers consider the rapidly changing nature of information technology through market research and the application of technology

refreshment techniques. Reduce program risk by using modular contracting, as outlined in FAR 39. AFI 33-104 outlines base and MAJCOM implementation procedures.

ATTACHMENT 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Information Technology Management Reform Act of 1996 (ITMRA)

(OMB) Circular No. A-130, Management of Federal Information Resources

FAR 39, Acquisition of Information Technology

CJCSI 6212.01, Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems

DoDD 8000.1, Defense Information Management (IM) Program

DoDI 5000.2, Defense Acquisition Management Policies and Procedures, February 23, 1991/Air Force Supplement 1

DoD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems, March 15, 1996

DoD Data Dictionary System (DDDS)

JTA-AF, Joint Technical Architecture-Air Force

AFDD 1-1, Air Force Task List

AFDIR 33-121, Compendium of Communications and Information Terminology (will convert to AFDIR 33-303)

AFPD 10-6, Mission Needs and Operational Requirements

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

AFPD 33-2, Information Protection

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

AFI 10-901, Lead Operating Command--Communications and Information Systems Management

AFI 21-116, Maintenance Management of Communications-Electronics

AFI 23-501, Retaining and Transferring Materiel

AFI 33-102, Command, Control, Communications, Computers, and Intelligence (C4I) Capabilities Planning Process

AFI 33-104, Base-Level Planning and Implementation

AFI 33-116, Long-Haul Telecommunications Management

AFI 33-117, Visual Information (VI) Management

AFI 33-118, Radio Frequency Spectrum Management

AFI 37-131, Freedom of Information Act Program

AFI 37-132, Air Force Privacy Act Program

AFI 38-201, Determining Manpower Requirements

AFI 38-204, Programming USAF Manpower

AFI 65-501, Economic Analysis

AFMAN 65-506, Economic Analysis

AFI 65-601, Vol 1, Budget Guidance and Procedures

AFI 90-301, Inspector General Complaints

AFP 91-215, Operational Risk Management (ORM) Guidelines And Tools

AFMAN 23-110, USAF Supply Manual

Air Force Information Technology Management (ITM) Strategic Plan (ITMSP) October 1997

Abbreviations and Acronyms

AETC--Air Education and Training Command

AFI--Air Force Instruction

AFDD--Air Force Doctrine Document

AFFMA--Air Force Frequency Management Agency

AFMAN--Air Force Manual

AFMC--Air Force Materiel Command

AFPD--Air Force Policy Directive

C4I--Command, Control, Communications, Computers, and Intelligence

CIO--Chief Information Officer

COMSEC--Communications Security

CSO--Communications and Information Systems Officer

DDDS--DoD Data Dictionary System

DoD--Department of Defense

DoDI--Department of Defense Instruction

FAR--Federal Acquisition Regulations

FOA--Field Operating Agency

GSA--General Services Administration

HQ AFCA--Headquarters, Air Force Communications Agency

HQ 38 EIW--Headquarters, 38th Engineering Installation Wing

IT--Information Technology

ITMRA--Information Technology Management Reform Act

JTA-AF--Joint Technical Architecture-Air Force

LOC--Lines of Code

MAJCOM--Major Command

SSG--Standard Systems Group

STEM--Systems Telecommunications Engineering Manager

VTC--Video Teleconference

VTT--Video Teletraining

Y2K--Year 2000

Terms

Base-Level Communications and Information Infrastructure--Both host and tenant organizations use the base-level communications and information systems infrastructure. The infrastructure includes all aspects of Communications and Information systems (voice, data, video transmission, switching, processing, system control and network management systems, equipment and facilities).

Business Process Reengineering--A structured approach by all or part of an enterprise to improve the value of its products and services while reducing resource requirements.

Communications and Information System--An integrated combination of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control through all operational phases. It includes base visual information support systems.

Communications and Information Systems Blueprint--Document that provides the engineering plan to modernize the base-level infrastructure with cost-effective, base-wide communications and information capability to support digital transmission of voice, data, video, imagery, and telemetry needs. It documents the baseline, identifies a target base configuration to support present and future requirements, and provides a time-phased plan and estimated costs for logical transition. The Communications and Information Systems Blueprint is sometimes referred to as the "Base Blueprint" or the "Blueprint."

Communications and Information Systems Officer (CSO)--Identifies the supporting communications and information systems officer at all levels. At base-level, this is the commander of the communications unit responsible for carrying out base communications and information systems responsibilities. At MAJCOM, and other activities responsible for large quantities of communications and information systems, it is the person designated by the commander as responsible for overall management of communications and information systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol "SC" and expands it to three and four letters to identify specific functional areas. CSOs are the accountable officer for all automated data processing equipment in their inventory.

Communications and Information Systems Requirement--Identifies a communications and information systems mission shortfall or system need to the CSO. A communications and information systems requirement arises when an organization cannot accomplish its current or new mission; can increase operational efficiency or cut operational costs by using advances in technologies; or can modernize an existing communications and information system by applying modern technology to satisfy evolving communications and information systems requirements, improve mission performance, and reduce current or future operation and support costs.

Full Costs--When applied to the expenses incurred in the operation of communications and information equipment/systems, includes: all direct, indirect, general, and administrative costs incurred in the operation of the communications and information system/equipment. These costs include, but are not limited to, personnel, equipment, hardware, software, supplies, contracted services, space occupancy, and intra/inter-agency services. (OMB Circular No. A-130)

Information Resource Management--The planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information. (OMB Circular No. A-130)

Information system--A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. (OMB Circular No. A-130)

Information system life cycle--The phases, through which an information system passes, typically characterized as initiation, development, operation, and termination. (OMB Circular No. A-130)

Information Technology--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. Includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (OMB Circular No. A-130)

Information Technology Management Reform Act--A Legislative act that repealed the Brooks Act, and gave the General Services Administration exclusive authority to acquire computer resources for all of the Federal government. It assigns overall responsibility for the acquisition and management of information technology (IT), to the Director, Office of Management and Budget (OMB). Responsibilities include: Design and implement an IT management process maximizing the value and assessing and managing the risks of the IT acquisitions. Integrate the IT management process with the budget, financial and program management processes. Establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services through the effective use of IT. Prepare an annual report, to be included in the DoD budget submission to Congress, on the progress in achieving the goals. Ensure agencies establish performance measurements for IT to measure how well the IT supports agency programs. Ensure the information security policies, procedures, and practices are adequate. Appoint a Chief Information Officer (CIO). Inventory all computer equipment and maintain an inventory of any such equipment that is excess or surplus property.

Interoperability--The ability of the systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (JP 1-02).

Joint Technical Architecture--Identifies the standards and guidelines for new acquisitions or major modifications to existing DoD communications and information systems. The standards, profiles, recommended products and recommended solutions are mandatory for use in the Air Force. The domains are provided as guidance. A system is compliant with the JTA-AF if it meets, or is implementing an approved plan to meet, all applicable JTA-AF mandates.

Joint Technical Architecture-Air Force--A comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles.

Lead Command--The MAJCOM or FOA assigned as the systems advocate and oversight authority.

Major Command (MAJCOM)--A major subdivision of the Air Force that is assigned a major part of the Air Force mission. MAJCOMs report directly to HQ USAF.

Modification--A temporary or permanent change to a system that is still being produced. The purpose of the modification is to correct deficiencies, improve reliability and maintainability, or to improve capabilities.

Modular contracting--Use of one or more contracts to acquire information technology systems in successive, interoperable increments. (OMB Circular No. A-130)

Nondevelopmental--Any project to procure primarily in-being products, where the total software developmental effort is realistically estimated as less than 1040 man-hours. As an alternative, use a threshold of less than 700 lines of code (LOC). If any hardware development is planned, the effort is not nondevelopmental.

Nonmaterial Solution--Includes changes in doctrine, operational concepts, tactics, training, or organization.

Operational Architecture--A description (often graphical) of the operational elements, assigned tasks, and information flows required to support the warfighter. It defines the type of information, frequency, and timeliness of the exchange, and what tasks are supported by these information exchanges. (AFDIR 33-121)

Operational Information Technology Planning--A process that links information technology to anticipated program and mission needs, reflects budget constraints, and forms the basis for budget requests. This planning should result in the preparation and maintenance of an up-to-date five-year plan which includes: a listing of existing and planned major information systems; a listing of planned information technology acquisitions; an explanation of how the listed major information systems and planned information technology acquisitions relate to each other and support the achievement of the agency's mission; and a summary of computer security planning.

Performance Measurement--The assessment of effectiveness and efficiency of IT in support of the achievement of an organization’s missions, goals, and quantitative objectives through the application of outcome-based, measurable, and quantifiable criteria, compared against an established baseline, to activities, operations, and processes. (DoD Guide for Managing IT as an Investment and Measuring Performance, 10 February 1997)

Program Cost--The total of all expenditures, in any appropriation or fund, directly related to the automated information system definition, design, development, and deployment, and incurred from the beginning of the “Concept Exploration” phase through deployment at each separate site. For incremental and evolutionary program strategies, program cost includes all increments. Program cost does not include operations and support costs incurred at an individual site after operational cut over of any increment at that site, even though other sites may exist that have not yet completed deployment. (AFI 10-601)

Risks--Types of risk may include schedule risk, risk of technical obsolescence, cost risk, risk implicit in a particular contract type, technical feasibility, dependencies between a new project and other projects or

systems, the number of simultaneous high risk projects to be monitored, funding availability, and program management risk. (OMB Circular No. A-130)

Risk Management--1. Appropriate techniques should be applied to manage and mitigate risk during the acquisition of information technology. Techniques include, but are not limited to: prudent project management; use of modular contracting; thorough acquisition planning tied to budget planning by the program, finance and contracting offices; continuous collection and evaluation of risk-based assessment data; prototyping prior to implementation; post implementation reviews to determine actual project cost, benefits and returns; and focusing on risks and returns using quantifiable measures. (FAR 39) 2. Risk management is the process used by decision-makers to reduce or offset risk. The risk management process provides leaders and individuals a systematic mechanism to identify and choose the optimum course of action for any given situation. Risk management must become a fully integrated element of planning and executing an operation. (AFP 91-215)

Requirements Process--This three-step process identifies communications and information systems requirements, develops a technical solution, and allocates resources.

Software Development--That portion of an effort that creates new product. Developmental costs do not include the cost of in-being products that are being augmented or modified. An effort is not considered to "involve development" if the total software development involves less than 1040 man-hours of effort. (See "nondevelopmental")

Strategic Information Resources Management (IRM) Planning Processes--Processes which consist of the following components: how the management of information resources promotes the fulfillment of an agency's mission; the use of information throughout its life cycle; operational information technology planning, and links to other planning processes including strategic, human resources, and financial resources. (OMB Circular No. A-130)

Systems Architecture--A description, including graphics, of the systems and interconnections providing for or supporting a warfighting function. It defines the physical connection, location, and identification of the key nodes, circuits, networks, warfighting platforms, and so forth, associated with information exchange and specific system performance parameters. The system architecture is constructed to satisfy operational architecture requirements per the standards defined in the technical architecture. (AFDIR 33-121)

System Security--1. A condition resulting from the timely application of system security management and engineering principles throughout all phases of a system's life cycle. It can be measured in terms of relative probability; i.e., that under a known set of circumstances (vulnerability versus countermeasures), the probability that acts of illicit interference against a system could achieve a specific objective without an effective preemptive response by the operating command. (AFM 11-1, Air Force Glossary of Standardized Terms, will convert to Air Force Doctrine Document [AFDD] 1-2) 2. Involves applying and managing computer security, communications security, and emanations security to protect communications and information resources from denial-of-service attacks. Security ensures the integrity of communications and information resources and prevents exploitation of sensitive information.

Systems Telecommunications Engineering Manager--A communications and information systems engineer who provides technical engineering planning services in support of communications and information systems and base infrastructures. The Base-Level STEM (STEM-B) has technical responsibility for engineering management and assists the base CSO in system engineering and configuration control. The Command-Level STEM (STEM-C) provides technical assistance to the MAJCOM and coordinates with

STEM-Bs on future MAJCOM mission changes, programs and efforts at the MAJCOM-level. The Joint STEM (STEM-J) is assigned to Commander's in Chief, Joint Staff and the Defense Information Systems Agency to promote interoperability by providing an interface between those activities and the Air Force MAJCOMs and bases. The Telecommunications Manager (STEM-TM) assists the STEM-B and C.

Technical Architecture--A framework of concepts and guidance that bound a subject area, or of physical components (for example, hardware, software, and transmission media) which interrelate to perform a bounded subset of information handling, both processing and transfer. (AFDIR 33-121)

Technical Solution--This detailed description of the communications and information systems solution uses the base infrastructure and complies with downward-directed architectures and standards. It identifies recommended acquisition methods and strategies, estimates one-time and recurring costs, and identifies manpower impacts.

Video Teleconferencing (VTC)--A two-way electronic form of communications that permits two or more people in different locations to engage in face-to-face audio and visual communications for the purpose of conducting meetings, seminars, and conferences. A VTC system typically includes a telecommunications system; video compression equipment; and video, audio, and graphics components. DoD VTC equipment must conform to standards in the Corporation for Open Systems International VTC profile that incorporates international standards for VTC.

Video Teletraining (VTT)--An electronic form of communications that uses high quality video, audio, and graphics equipment for the purpose of conducting training and education programs for students that are geographically separated from the instructor. The Air Technology Network is the Air Force standard VTT network.

Waste--The extravagant, careless, or needless expenditure of Air Force funds or the consumption of Air Force property that results from deficient practices, systems controls, or decisions. The term also includes improper practices not involving prosecutable fraud. NOTE: Consider wartime and emergency operations when explaining possible waste. For example, legitimate stockpiles and reserves for wartime needs, which may appear redundant and costly, are not waste. (AFI 90-301)

Year 2000 compliant--The information technology accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it. (FAR 39)