DRAFT - NOT FOR IMPLEMENTATION OR COMPLIANCE

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE PAMPHLET 32-1003, VOLUME 5
AUGUST 1998

Civil Engineering

WORKING IN THE RESOURCES FLIGHT INFORMATION SYSTEMS MANAGEMENT

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCESA/CEOM (Capt T. Wahl) Certified by: AFCESA/CC (Col H. Dean Bartel)
Pages: 22
Distribution: F.

This volume in this pamphlet series describes the Air Force Engineer's role in activities required to develop, prepare, submit, and maintain a financial plan, budget estimates, and the Base Civil Engineer (BCE) financial management system; manage all manpower and personnel issues; operate and maintain automation systems and support; and all activities related to real property accountability and reporting. The 32 series of Air Force publications contains USAF policy and procedural guidance for the Resources Flight. This volume provides detailed information for performing the Information Systems Management mission. The information systems management function is responsible for development, management, and execution of the civil engineer financial programs. This volume in this pamphlet also supports policy and guidance from HQ USAF/SC, HQ AFCIC and the 33 series of Air Force publications.

Chapter 1 Overview 3
1.1 Information Systems Basics 3
1.2 Planning 4
1.3 Operations 4
1.4 Maintenance 4
1.5 Inventory 4
1.6 Training 4
Chapter 2 Information System Basics 6
2.1 Different Types of Systems 6
2.2 Computer Basics 7
2.2.1 I/O Devices 8
2.2.2 Memory 8
2.2.3 Central Processing Unit 8
2.2.4 Operating System 8
2.2.5 Files 9

Chapter 3 Planning for Information Systems 10
3.1 Establishing an IS Plan 10
3.1.1 Setting Objectives 10
3.1.2 Conducting an External Analysis 11
3.1.3 Conducting Internal Analysis 11
3.1.4 Identifying Strategic Initiatives 11
3.2 Request Process 11
Chapter 4 System Operation 14
4.1 Organization and Accessibility of System 14
4.2 Security and Protection of Software/ Hardware 14
4.3 Controlling Data/System Quality and Integrity 15
4.4 Recovering/ Restoring and Upgrading Software 15
4.5 Controlling Communications and System Connectivity 16
4.6 A Network 16
Chapter 5 Maintenance 19
Chapter 6 Inventory 20
Chapter 7 Training 21

List of Figures and Tables

Figure 1. CE Information System Operating Environment 7

Table 1. Security Protection Classes 15

List of Attachments

Attachment 1: List of Acronyms 22

Chapter 1 Overview

Information Systems (IS) management is a primary function in Resources Flight. The major responsibilities of this function are planning, operation, maintenance, inventory, and training. This is a set of responsibilities that are in transition as civil engineering moves from the Wang computer platform to open computer systems. The new systems integrate with not only Air Force engineers, but with military and civilians everywhere around the world.

The current role of the system administrator is very different from the days of managing civil engineer information requirements with the Wang system. Communications, data management, e-mail and word processing were all managed through a world-wide network of civil engineer Wang computers. The direction is now for most hardware and system requirements to be managed by local base computer-communications personnel. Civil engineer information system management is evolving into a function of user advocacy rather than primary technical support.

This pamphlet provides an overview of the responsibilities that system administrators face on a daily basis. Certain basics are discussed for systems, hardware and software. For those civil engineer organizations that are still operating their own networks and systems, this volume will barely scratch the surface of executing the technical functions. Regardless of who executes the specific technical support, the civil engineer system administrator will continue to be responsible for assuring that the proper planning, operation, maintenance, inventory, and training supports the information system needs of the local civil engineer organization.

1.1 Information Systems Basics

This pamphlet takes the time to explain the basics of information systems before delving into responsibilities of Information Systems Management. Chapter 2 looks at types of systems and system components.

Basics include system types, network basics, and computer basics.

1.2 Planning

The primary part of planning responsibility is to provide managers with an information system that enhances their ability to successfully complete their mission. Planning considerations include infrastructure, operating system, hardware, software, reliability, funding, and support.

IS also manages the interfaces with each CE Flight, Communications Squadron, computer maintenance contractors, the SSG, AFCESA, other computer operators, base ops, and internal systems.

1.3 Operations

Under operations, the IS manager makes sure the system is both accessible and secure, maintains software, ensures the integrity of data, and controls communications via computer with the worldwide CE community. The manager also ensures network, computers, and devices are operating correctly so users can accomplish computer-based tasks as required. The IS manager is responsible for PC connectivity to Regional Processing Centers for access to the Work Information Management System (WIMS).

System operation includes security, user utilities, user rights, fileshare server utilities, file utilities, file protection, functional menus, and file transfers.

1.4 Maintenance

In maintaining the systems, the IS manager ensures service and maintenance contracts are in place and all hardware and software are covered. The IS manager is responsible for system maintenance, but does not perform all of the actual maintenance.

1.5 Inventory

The IS manager is responsible for maintaining the system inventory, including software and hardware. The manager identifies what needs to be replaced, when it needs to be replaced, and what equipment is no longer needed.

1.6 Training

Training is a key responsibility of the Resources Flight. Time and training should be included in the planning process. Formal training, not within the unit's capability, is identified to the base communications unit as a training requirement.

When new systems are acquired, users must be educated on their functions and utility. The IS manager may perform periodic classes on the uses of new hardware or software. The IS managers are not applications specialists, but they

are responsible for assuring that proper training is available for the effective utilization of all applications and programs.

Chapter 2 Information System Basics

2.1 Different Types of Systems

There are several types of computer systems, including micro-computers, mini-computers, and mainframes.

Micro-computers are fully-functional workstations. Historically, they have been classified as personal computers (PCs). These devices contain five basic components:

(1) devices,
(2) memory,
(3) central processing unit (CPU),
(4) operating system, and
(5) files.

Mini-computers consist of a central computer with physical connections to multiple I/O devices. Typically, the I/O devices are considered to be dumb workstations. These dumb terminals can not function without the connection to the mini-computer.

Mainframes are computers set apart, basically, because of their cost or capacity.

The CE community, along with the rest of the AF, is moving to a local area network (LAN) configuration. The typical LAN connects personal computers to the CE LAN; will run commercial, off-the-shelf software, and has forward processing, graphics, and spreadsheet capabilities. The CE LAN will access regional Defense Megacenters (DMC) managed by the Deputy Chief of Staff, Command, Control, Communications and Computers, SC, via telecommunication. The CE information system is shown in Figure 1.

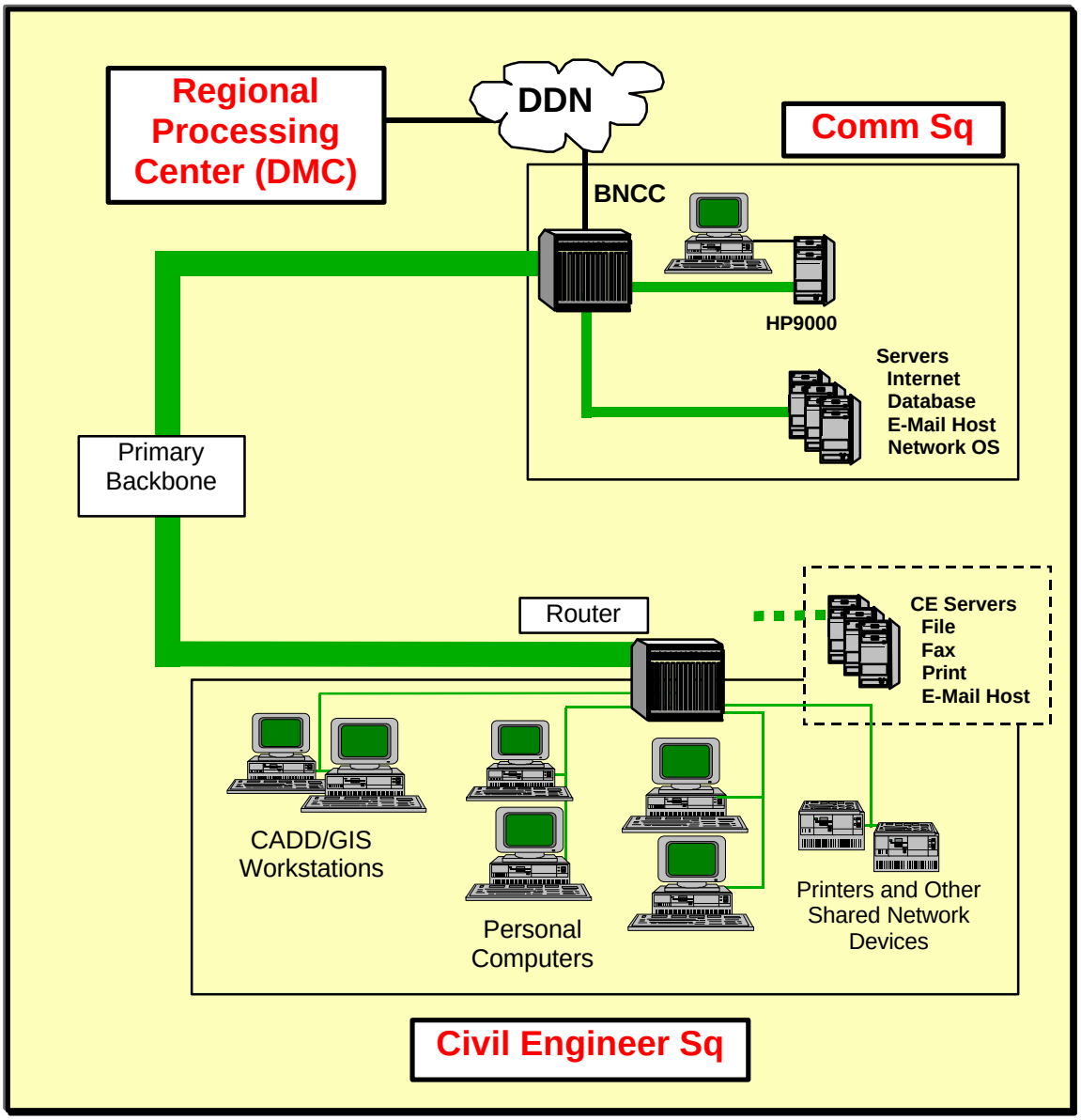

Figure 1. CE Information System Operating Environment

2.2 Computer Basics

To understand the responsibilities of the IS manager, the building blocks of an information system must first be understood.

This section outlines the components basic to any computer. A brief explanation of input/output devices (I/O), short- and long-term memory, the central processing unit (CPU), the operating system, files, and different computer system follows.

2.2.1 I/O Devices

I/O devices are used to get data in and out of computers. Input devices include keyboards, scanners, and light pens. Output devices include printers, monitors, tapes and disks.

2.2.2 Memory

All data flows are to and from memory. Data from input devices always goes into memory. Output devices always receive their data from memory. Two-way data flows exist between files and memory and between the arithmetic/logic unit and memory. Data flows from the memory to the control unit, telling the control unit what to do next.

The two types of memory are short- and long-term. Short-term memory provides temporary storage for programs and data. It exists on the main system board or on add-in memory boards. All programs must be loaded into memory in order to run. Long-term memory is used as secondary data storage for vast quantities of data. It exists on peripheral devices such as removable disk drives and tape drives.

2.2.3 Central Processing Unit

The CPU carries out addition, subtraction, multiplication, and division. It also performs certain logical operations; such as, comparing two numbers for equality or finding out which number is larger.

The CPU is composed of the control unit and arithmetic logic unit. The control unit controls the components of the system. It provides the control that enables the computer to take advantage of the speed and capacity of its other components. The arithmetic logic unit carries out the actual addition, subtraction, multiplication, and division functions.

2.2.4 Operating System

The operating system establishes the parameter by which the computer will run. Is basic functions are managing the flow of information to and from the various parts of the computer and establishing the operation parameters of the system, such as usable memory, file formats, etc.

2.2.5 Files

Program and data files make up the final component of the computer.

Program files are a list of operations stored in memory that tell the control unit what to do. They are expressed in a precise format (close to machine language) the computer has been designed to understand. Examples include word processing programs, spreadsheet programs, and database programs.

Data files contain data in a format suitable for processing by an application on the computer.

Chapter 3 Planning for Information Systems

Planning for information systems requires a coordinated effort among the IS manager, the base Civil Engineer users, the Communication Squadron, the major command (MAJCOM), and the Air Force Civil Engineer Support Agency (AFCESA).

The coordinated planning effort ensures that the IS will be able to grow with and support the needs of the BCE unit.

A few of the benefits of formal planning follow.

(1) The unit acquires a system that will integrate with existing and future systems.
(2) Formal planning prevents the risk funds will be wasted on ill-fated technology or items that are considered neat, versus items that meet a need.
(3) It helps the IS manager evaluate progress and make needed adjustments.
(4) Including the user in the planning phase greatly increases the likelihood the fielded resource will actually do what the user needs.

One of the primary objectives of the planning effort should be development of an information system that can assist the BCE unit in adding value. Examples would include systems that offer assistance in constructing budgets or in compiling information on facility assessments.

3.1 Establishing an IS Plan

The four steps used in establishing the IS plan are:

Step 1: set objectives,

Step 2: conduct an external analysis,

Step 3: conduct an internal analysis, and

Step 4: identify strategic initiatives.

3.1.1 Setting Objectives

The IS plan objectives must match the organizational objectives and provide some clear benchmark to measure any progress. For example, the objective set for system reliability might be 99 percent up time.

Factors to consider when planning include:

- support requirements for operations and contingencies,
- access to resources for handicapped personnel,
- security,
- the need to share information or other resources,
- management of records, and
- the operating environment; such as, location, power and power conditioning, temperature and humidity, and dust and dirt in the air.

3.1.2 Conducting an External Analysis

No information system is isolated; therefore, the external environment must be considered. The CE community, has moved to a local area network (LAN) configuration. The CE LAN will run commercial, off-the-shelf software with graphics and spreadsheet capabilities. The CE LAN will access regional Defense Megacenters (DMC) managed by the Deputy Chief of Staff, Command, Control, Communications and Computers, SC, via telecommunication.

For planning purposes, it is important to know what happens at the DMCs, as well as what resources are, or will be, available at the base. For the resources information, the IS manager will contact the base SC.

3.1.3 Conducting Internal Analysis

The fourth step of the planning process includes a review of internal requirements, as well as, current IS resources. During this internal analysis, the customer's software and hardware requirements are reviewed and capacity planning performed. The plan for short-term and long-term loss of system hardware and software is undertaken; as well as a contingency plan in case of the absence of the IS manager.

3.1.4 Identifying Strategic Initiatives

Strategic initiatives can be determined, resulting in significantly improve IS and IS management. Some of these initiatives may require significant investment. Others may be relatively easy to acquire or accomplish.

3.2 Request Process

There is a formal process in place for requesting computer technology. Requirements are identified to SC using an AF Form 3215, Computer Systems Requirements Document (CSRD) (see Figure 2). SC evaluates the request for validity, as well as, identifying possible alternatives.

If the CSRD is valid and costs less than $50,000, the BCE may purchase the item with 3400 funds. If funds are not available within the organization, the CSRD may be reviewed by a Wing Computer Systems Requirements Board (CSRB). The Board consists of wing IS managers. The CSRB will prioritize the requirement with other wing automated data processing equipment (ADPE).

The following are some notes on the computer system requirement document, AF Form 3215:

On AF Form 3215, block 5 (ROD/POD) is used for the required operational date (ROD) or the planned operational date (POD). If the items sought are not needed by a firm, fixed date, the POD would be more appropriate

Block 9 (Requirement), should state the capabilities needed to accomplish specific tasks. For example: A valid requirement would be “a fully functional workstation, capable of running geographic information system (GIS) applications software.” An invalid (inadequate) requirement is “ a dual processor is required.”

Block 10 (Justification) is used to justify each unique aspect of the requirement. For example: if block 10 requested a portable, fully-functional workstation . . ., then the fact that it needs to be “portable” must be justified.

Block 11 (impact if disapproved). This block is used to explain the adverse impact to the mission if the request is refused. For example, explaining what the impact would be if software used to transfer mail to remote systems is disapproved.

Block 18 (Proposed Solution/Alternatives) can be used to propose solutions; however, it is not mandatory.

C4 SYSTEMS REQUIREMENTS DOCUMENT	DATE:	CSO CONTROL NUMBER:

REQUIREMENT TITLE:		REQUESTING AGENCY POINT OF CONTACT *(Organization, Office, Name, Grade, Telephone Number)*
DATE NEEDED:	MISSION OR SYSTEM SUPPORTED:	

REQUIREMENT:

JUSTIFICATION:

TECHNICAL SOLUTION AND COSTING

CSO'S PROPOSED SOLUTION/ALTERNATIVES:

TECHNICAL SOLUTION AUTHORITY

THIS SOLUTION MEETS ARCHITECTURAL AND INTEROPERABILITY REQUIREMENTS *(Name, Organization, Telephone Number):*	TECHNICAL REFERENCES USED:

APPROVAL AUTHORITY

RECORDS MANAGEMENT APPROVAL AUTHORITY *(Name, Title, Organization):*		APPROVED
		DISAPPROVED
REQUESTER APPROVAL AUTHORITY *(Name, Title, Organization):*		FUNDS AVAILABLE
		UNFUNDED
		APPROVED
		DISAPPROVED
HOST BASE APPROVAL AUTHORITY *(Name, Title, Organization):*		APPROVED/FUNDED
		APPROVED/UNFUNDED
		DISAPPROVED
MAJCOM APPROVAL AUTHORITY *(Name, Title, Organization):*		APPROVE
		VALIDATE

AF FORM 3215, AUG 95 *(EF-V5)* *(PerFORM PRO)* PREVIOUS EDITIONS ARE OBSOLETE.

Figure 2. AF Form 3215, Computer Systems Requirements Document

Chapter 4 System Operation

One of the major responsibilities of the IS manager is system operation. The manager is responsible for the organization and accessibility of the system, ensuring the system hardware and data are protected and secure; controlling data/system quality and integrity; recovering/restoring and upgrading software; and controlling communications, connectivity, and data exchange with the worldwide CE community.

4.1 Organization and Accessibility of System

The IS manager must configure the operating system to meet users' needs by defining printers, modem access, and user restrictions; then, arrange the system based on standard naming conventions.

4.2 Security and Protection of Software/ Hardware

The IS manager certifies required security safeguards have been implemented on each mainframe, LAN, and personal computer prior to operating the system. The system security must be documented by the manager in the form of a risk analysis.

The manager is responsible for physical security of the system, as well as, ensuring system (or data) access is secure.

To ensure the physical security of the system, the IS manager takes actions to prevent the theft of the system.

To ensure the security of access to data in the system, the IS manager must define the ownership of applications and determine who has permission to read, write, and execute applications. For the Wang, the three controlled levels of system security are

1. the system access level,
2. the file access level, and
3. the actual data record level.

System access is limited by assigning a unique user identification and password. Passwords can be encrypted for an added level of security. A file protection class can be assigned to files which limits access by certain users. These four protection classes are shown in Table 3.

Two programs used to limit individual file or program options are IRGTUD and IUSRUD. IRGTUD in the I1XXOBJ library allows the IS manager to add updater titles to control access to program options; such as, ADD, MODIFY, and DELETE. IUSRUD allows the manager to add/modify a user's rights.

Table 1. Security Protection Classes

#	Only the owner and the system administrator (IS manager) can access
@	Any user can only EXECUTE
$	Any user can READ, EXECUTE, or COPY
BLANK	Any user can do anything to a file with a blank protection class. Blank means nothing is entered in the protection class field

4.3 Controlling Data/System Quality and Integrity

The Resources Flight is responsible for operation of the computer system and the data integrity; however, all members of the organization are responsible for ensuring the quality of the data and each flight is responsible for the quality of the data being input. The IS manager periodically checks on the data by running reports to retrieve information that should be in the system. If the reports show information that is wrong, the owner of the data must correct these problems.

4.4 Recovering/ Restoring and Upgrading Software

When hardware and/or software malfunction and a database is damaged, procedures must be in place to restore the database to its original condition. The IS manager is responsible for periodically backing up data to prevent complete loss of data in case of a system crash. The frequency of the backups depends on the frequency with which the data changes.

As new releases or new versions of software are made available, the IS manager is responsible for loading the new versions in a timely fashion. This ensures the system software is consistent with the rest of the Air Force.

4.5 Controlling Communications and System Connectivity

Change is everywhere in the computer system domain. The change is most evident and dramatic in telecommunications and networking. Basic reasons for networking are sharing of resources and data, distributed data processing, and enhanced communication.

On the squadron level, a variety of resources such as laser printers, software stored on a file server, a compact disk storage device, or even a single facsimile (FAX) machine are shared resources. On the AF level, supercomputer processing capability may need to be shared, such as in the case of the Defense Megacenters.

Sharing of data allows users at the base to share/pass data to MAJCOM or other interested agencies.

Enhanced communications via electronic mail over computer networks has become a mainstay of communication in most Air Force organizations.

4.6 A Network

Networks consist of a physical media, arranged according to some topology or configuration, in a particular type of network (Wang, LAN, WAN, etc.). Communication throughout the network is permitted through the use of particular protocols. Protocols are agreed upon set of rules or conventions governing communication among elements of a network or levels of a network.

The IS manager is responsible for ensuring that the system can communicate with all configured devices, as well as, other computer systems. The minicomputer (Wang) is configured to connect to the AF concentrator. The AF concentrator has a Defense Data Network port, enabling the computer to pass mail and data files to remote systems. The concentrator connection, or transport, is configured with the Wang System Networking Tools (WSN) provided by Wang, WSNEDIT.

The following programs are important not only to the Wang system networking, but, other system networks.

WSNEDIT is applicable directly to Wang system and defines both network and system level configurations. The network level describes system and area information. The system level is stored in a local view file and represents data link, service, and routing definitions

A **data link** includes protocol parameters and names of connected systems and service information includes file transfer and logon parameters. Routing includes parameters for message routing to any destination in the WSN.

Transmission control protocol/Internet protocol (TCP/IP) are communications protocols developed under contract from the U.S. Department of Defense to inter-network dissimilar systems. It is a de facto UNIX standard, supported on almost all systems, and used by many corporations and most universities and federal agencies. TCP controls data transfer. IP provides the routing.

A **router** is a computer system that routes messages from one LAN to another. Used to internetwork similar and dissimilar networks, it can select the most expedient route based on traffic load, line speeds and costs, and network failures. Routers maintain address tables for all nodes in the network.

File Transfer Protocol (FTP) and **Simple Mail Transfer Protocol (SMTP)** provide file transfer and e-mail. Multipurpose Internet Mail Extensions (MIME) are extensions to the SMTP format that allow it to carry multiple types of data (binary, audio, video, etc.). TELNET protocol provides terminal emulation for all types of computers in the network.

Internet Packet Exchange (IPX) is netware communications protocol used to route messages from one node to another. IPX packets include network addresses and can be routed from one network to another. An IPX packet can occasionally get lost when crossing networks, thus IPX does not guarantee delivery of a complete message.

A **gateway** is typically referred to as a node on a network that connects two otherwise incompatible networks. For example, PC users on a local area network may need a gateway to gain access to the Wang mainframe computer because the mainframe does not speak the same language (protocols) as the PCs on the LAN. Gateways on data networks often perform code and protocol conversion processes.

Gateways also eliminates duplicate wiring by giving all users on the network access to the mainframe without having a direct, hard-wired connection.

Chapter 5 Maintenance

The IS manager is responsible for system maintenance, but does not actually perform all of the maintenance. Systems maintenance ensures all equipment and software is covered by some form of a maintenance contract. The IS manager must notify the computer system officer (CSO) of all equipment to be covered by the base's maintenance contract. The CSO will ensure that a contract is in place. There are alternative contract avenues available. Depending on the situation, a monthly maintenance contract may be established or the manager may determine that a per-call contract should be established.

In some cases, a monthly contract including parts and labor is established for core mainframe equipment. This is usually done because of the high cost of parts for the mainframe. For non-core equipment, a per-call contract is established. With the per-call contract, the unit is billed for any replacement parts used and any labor costs. The base CSO will ensure that the most cost-effective avenue is chosen.

All maintenance is requested using an AF Form 597.

There are two types of software maintenance, primary and secondary support.

The major command may be the only one that can call the maintenance contractor for primary software support. Others who require contract support, and are not identified on the contract, may have to go through MAJCOM. Secondary software support allows the unit to call the maintenance contractor directly.

Chapter 6 Inventory

The IS manager is responsible for maintaining the system inventory, including software and hardware, and the identifying computer equipment no longer needed. Identification of outdated equipment should be done at least 120 days before the equipment goes off-line. This allows completion of the screening cycle while the equipment is still in use and eliminates the need to store excess equipment. This equipment will be redistributed across the AF or DoD through the Defense Automation Resources Information Center. If there are no other parties interested in the equipment, the manager is required to turn the equipment into the Defense Reutilization Materiel Office (DRMO).

The IS manager's responsibility for maintaining the software on the computer systems includes:

- identifying all excess software for reutilization;
- destroying software that is more than two versions behind the most current version;
- ensuring users do not use shareware or public domain software until the CSO certifies it to be free of viruses, hidden defects, and obvious copyright infringements; and
- ensuring shareware users pay any necessary fees.

Chapter 7 Training

Training is an extremely important responsibility of the Resources Flight. This responsibility is identified in the manpower standard and credit is given for this activity. Time and training should be included in the planning process. Formal training, not within the unit's capability, is identified to the base communications unit as a training requirement.

When new systems are acquired, users must be educated on their functions and utility. The IS manager may perform periodic classes on the uses of new hardware or software. The following alternative training methods may be used.

Individuals from different flights are trained by the IS manager. These students then train their flight personnel. Training can be acquired from the base communications unit. Training can be acquired from a commercial provider. If the resources are available, the TDY expenses are paid for someone from another base to come and conduct training.

Attachment 1 List of Acronyms

ACK	acknowledgment
ADPE	automated data processing equipment
AFCESA	Air Force Civil Engineer Support Agency
BCE	base civil engineer
CPU	central processing unit
CSO	computer system officer
CSRB	Computer Systems Requirement Board
CSRD	Computer Systems Requirement Document
DARPA	Defense Advanced Research Projects Agency
DMC	Defense Megacenters
DRMO	Defense Reutilization Material Office
FTP	file transfer protocol
I/O	computer input/output devices
ICP	Internet protocol
ID	identifier
IEEE	TBD
IS	information system
LAN	local area network
OSI	TBD
PC	personal computer
POD	planned operational date
ROD	required operational date
SC	TBD
SMTP	simple mail transfer protocol
TCP	transmission control protocol
WIMS	Work Information Management Agency
WSN	Wang System Network